Conditions d’utilisation des contenus du Conservatoire numérique

1- Le Conservatoire numérique communément appelé le Cnum constitue une base de données, produite par le Conservatoire national des arts et métiers et protégée au sens des articles L341-1 et suivants du code de la propriété intellectuelle. La conception graphique du présent site a été réalisée par Eclydre (www.eclydre.fr).

2- Les contenus accessibles sur le site du Cnum sont majoritairement des reproductions numériques d’œuvres tombées dans le domaine public, provenant des collections patrimoniales imprimées du Cnam.

Leur réutilisation s’inscrit dans le cadre de la loi nº 78-753 du 17 juillet 1978 :

- **la réutilisation non commerciale de ces contenus est libre et gratuite dans le respect de la législation en vigueur ; la mention de source doit être maintenue (Cnum - Conservatoire numérique des Arts et Métiers - https://cnum.cnam.fr)**
- **la réutilisation commerciale de ces contenus doit faire l’objet d’une licence. Est entendue par réutilisation commerciale la revente de contenus sous forme de produits élaborés ou de fourniture de service.**

3- Certains documents sont soumis à un régime de réutilisation particulier :

- **les reproductions de documents protégés par le droit d’auteur, uniquement consultables dans l’enceinte de la bibliothèque centrale du Cnam. Ces reproductions ne peuvent être réutilisées, sauf dans le cadre de la copie privée, sans l’autorisation préalable du titulaire des droits.**

4- Pour obtenir la reproduction numérique d’un document du Cnum en haute définition, contacter cnum(at)cnam.fr

5- L’utilisateur s’engage à respecter les présentes conditions d’utilisation ainsi que la législation en vigueur. En cas de non respect de ces dispositions, il est notamment passible d’une amende prévue par la loi du 17 juillet 1978.

6- Les présentes conditions d’utilisation des contenus du Cnum sont régies par la loi française. En cas de réutilisation prévue dans un autre pays, il appartient à chaque utilisateur de vérifier la conformité de son projet avec le droit de ce pays.

NOTICE BIBLIOGRAPHIQUE

Auteur(s)	**Givierge, Marcel (1871-1931)**
Titre	**Cours de cryptographie**
Adresse	**Paris : Berger-Levrault, éditeurs, 1925**
Collation	**1 vol. (IX-304 p.) ; 22 cm**
Nombre de vues	**315**
Cote	**CNAM-BIB 8 Y 88**
Sujet(s)	**Cryptographie** **Machines à chiffrer**
Thématique(s)	**Technologies de l'information et de la communication**
Typologie	**Ouvrage**
Langue	**Français**
Date de mise en ligne	**21/01/2021**
Date de génération du PDF	**06/02/2026**
Recherche plein texte	**Disponible**
Notice complète	https://www.sudoc.fr/094130906
Permalien	https://cnum.cnam.fr/redir?8Y88

COLONEL M. [illegible]IERGE

COURS

DE

CRYPTOGRAPHIE

BERGER-LEVRAULT, ÉDITEURS

NANCY-PARIS-STRASBOURG

1925

COURS DE CRYPTOGRAPHIE

COLONEL M. GIVIERGE

COURS

DE

CRYPTOGRAPHIE

PARIS
BERGER-LEVRAULT, ÉDITEURS
136, BOULEVARD SAINT-GERMAIN (VI^e^)
1925

AVANT-PROPOS

Les résultats des travaux des décrypteurs, et même l'objet de ces travaux et l'existence des services de décryptement, étaient jadis laissés dans l'ombre par les Gouvernements ou les particuliers qui en profitaient. Ceux-ci, en effet, s'efforçaient de ne pas tarir la source des renseignements qui leur étaient fournis par ce canal et évitaient d'effaroucher leurs indicateurs inconscients en révélant la possibilité d'un danger pour le secret dont on avait voulu entourer la correspondance. A notre époque de « diplomatie au grand jour », on a laissé filtrer des renseignements assez précis sur les services qu'ont pu rendre les organes chargés des études de cryptographie. C'est ainsi qu'au cours de la guerre et dans la suite, des allusions fréquentes, parfois dissimulées, parfois d'une clarté complète, ont été faites, touchant les traductions des télégrammes chiffrés des puissances belligérantes. On peut lire dans la *Revue Militaire française* du 1er juillet 1921 que la manœuvre de Tannenberg a été singulièrement facilitée à Ludendorff par la connaissance du chiffre russe, qui permettait de traduire tous les ordres des armées que ce général combattait. Les communications de ces armées se faisaient exclusivement par T. S. F. et les radiotélégrammes étaient captés et traduits en temps utile pour permettre à Ludendorff de rédiger ses ordres en tenant compte des ordres ennemis (*Revue Militaire française*, Librairie Chapelot à Paris. N° 1, p. 14 et 15). *L'Intransigeant* du 5 septembre 1920 contient un article : « La bataille de la Marne

contée par les radios du commandement ennemi », où figurent les textes d'un certain nombre de traductions de ces radiotélégrammes chiffrés (1).

On peut ajouter que pendant la guerre le secret de nos déchiffrements fut assez mal gardé. La censure, mal informée des questions à tenir secrètes, permit à la presse, tant chez nous que chez nos alliés, de donner des renseignements qui tirèrent nos ennemis de leur quiétude initiale. Ces derniers réduisirent en conséquence leur correspondance radiotélégraphique militaire et la rendirent plus difficile à traduire. Une polémique entre l'*Œuvre* et l'*Action Française*, en novembre 1919, fait d'autre part allusion à des traductions de correspondance chiffrée diplomatique, dont certains textes parurent dans un journal du même mois (*La Voix Nationale*, presse de Paris). Déjà, d'ailleurs, au cours même de la guerre, la question des traductions de dépêches diplomatiques chiffrées a été traitée par la presse mondiale, au sujet des télégrammes adressés aux représentants allemands en Amérique, Bernsdorf et Luxburg, et l'on peut regarder les révélations relatives aux agissements de ces diplomates dans des pays encore neutres comme un des facteurs de la déclaration de guerre des États-Unis et du Brésil.

On ne peut pas espérer que les Gouvernements dont la correspondance a été traduite aient ignoré la publication de renseignements relatifs à cette traduction. Le secret dont on entourait jadis les services de cryptographie a donc été trahi. On peut déplorer par contre que les censeurs, partageant l'ignorance générale du public, en dehors de rares spécialistes, sur les questions de chiffre, aient laissé

(1) Cet article contient d'ailleurs une inexactitude historique; il laisse croire que ces radios furent traduits au moment de la bataille de la Marne et purent alors venir en aide à notre commandement. Or, ils ne furent traduits que par la suite, et ce n'est que quelques semaines après cette bataille que nos généraux purent se trouver dans la situation rapportée plus haut pour Ludendorff.

passer des notes utilisables par l'adversaire. Trop de secret est quelquefois néfaste; à force de cacher les notions de cryptographie, on manque de personnel averti, alors que les connaissances d'ordre général répandues sur certaines questions, celle des transports par exemple, n'empêchent pas les états-majors de garder secrets les détails dont la connaissance intéresserait l'ennemi. On en a trop dit pour que l'existence des services de déchiffrement soit ignorée. Les journaux de polémique, tels que *Aux Écoutes*, le *Cri de Paris*, le *Journal* lui-même, ont donné des détails, qui, pour un homme averti, permettent de se rendre compte de notre organisation. Dans ces conditions, il vaut mieux multiplier le nombre des personnes ayant des notions saines sur ce sujet.

Sans avoir besoin de remonter aux exemples historiques (Voir Josse et Bazeries) et de rappeler l'importance que les ministres attachaient aux recherches de Viète sous Henri IV et de Rossignol sous Louis XIII, nous pouvons dire, en nous appuyant sur les considérations qui précèdent, qu'à toute époque les études cryptographiques sont utiles aux États, et que ceux-ci ont besoin de cryptologues exercés.

Il nous semble alors d'un intérêt national de chercher à éveiller les vocations cryptographiques. Plusieurs se sont révélées au cours de la dernière guerre, grâce aux hasards heureux qui ont fait entrer dans les services du Chiffre des personnes ignorantes auparavant de ce genre d'études, où pourtant, bien douées comme elles l'étaient, elles ont remporté les plus brillants succès. Mais il est prudent de ne pas compter uniquement sur une telle improvisation pour renforcer à la mobilisation les services qui fonctionnent dès le temps de paix.

Nous croirons alors avoir rempli une partie de la tâche que nous nous sommes proposée, si l'exposé que nous donnons plus loin peut intéresser, malgré son aridité, quelques personnes jusque-là étrangères aux problèmes cryp-

tographiques et désireuses de se délasser à l'étude d'une science aussi intéressante que la géométrie, avec l'assaisonnement de curiosité que peut y introduire la connaissance du contenu de communications désirées secrètes par leurs auteurs.

Tandis qu'à la fin du dernier siècle, il eût fallu des circonstances extraordinaires pour permettre à des particuliers de se trouver en possession de cryptogrammes authentiques, tels que ceux qui passaient par les lignes télégraphiques, et qui étaient protégés contre toute indiscrétion par le secret qu'entourait ce genre de communications, la diffusion de la télégraphie sans fil permet à l'heure actuelle de recueillir des cryptogrammes de toute nature, les uns chiffrés avec des systèmes relativement simples, les autres avec les procédés les plus compliqués de la diplomatie.

L'autre but que nous avons visé est de faciliter aux élèves cryptologues les recherches de procédés plus ou moins classiques, décrits, parfois avec des longueurs qui nous semblent inutiles à la compréhension du principe, dans certains recueils aujourd'hui presque introuvables, les éditions en étant épuisées. Nous ne prétendons pas, par conséquent, avoir fait œuvre originale. Nous avons composé un manuel permettant à nos élèves de traiter ici les exercices que nous leur proposerons d'autre part. Nous avons laissé de côté certains procédés classiques, parce que leur importance actuelle au point de vue pratique nous a semblé négligeable, d'après les documents qui nous sont tombés sous les yeux, et qu'ils ne nous paraissaient pas comporter d'enseignements intéressants.

Nous avons donc butiné à droite et à gauche, nous efforçant de ne pas oublier de citer nos auteurs. Bazeries regrette de ne point connaître de noms de cryptologues après l'époque de Louis XIV; on trouvera, dans cette compilation, les noms de quelques-uns de ceux qui, parmi bien d'autres, ont travaillé sur des questions de Chiffre aux

environs de 1920. Nous tenons à y ajouter avec un sentiment d'affection tout spécial ceux de MM. Ancel et Haverna, cryptologues aussi savants que modestes, qui voulurent bien guider, en 1907, nos premiers pas dans la carrière cryptographique. Nous y ajouterons aussi ceux des colonels d'artillerie Thévenin et Olivari. Malgré les intéressantes études de ces deux remarquables cryptologues, leurs noms en effet ne sont pas venus sous notre plume au cours des pages qui vont suivre, à côté de ceux des autres officiers, qui, au cours de la guerre, soit dans un bureau d'état-major, soit pendant les heures de loisirs que leur laissait l'exercice du commandement au front, s'efforçaient, et souvent avec succès, de pénétrer les grimoires des transmissions ennemies pour y découvrir la révélation des attaques contre la patrie et permettre de les parer en temps utile.

COURS DE CRYPTOGRAPHIE

CHAPITRE I

GÉNÉRALITÉS

Chiffrer un document, c'est transformer un texte *clair*, c'est-à-dire écrit de manière que tout lecteur qui en connaît la langue soit capable d'en comprendre le sens, en un texte *chiffré* dont le sens n'est compréhensible qu'à ceux qui peuvent le *déchiffrer*, qui en connaissent la clef.

Si l'on emploie un *langage convenu*, le texte peut présenter un sens, mais ce n'est pas le sens que lui donnera le destinataire. Ainsi l'on peut concevoir que le télégramme : je vous envoie trois tonnes d'arachide par le vapeur Cap Vert, voudra dire : trois contre-torpilleurs allemands sont arrivés aux Iles du Cap Vert.

Certains langages convenus sont fort compliqués, nous en donnons ci-après un exemple :

On adopte un certain nombre d'expressions donnant des renseignements importants, et on les numérote. Supposons que dans la série de ces expressions, celles qui représentent des nombres soient numérotées de 1 à 10, celles qui signifient arrivées et départs de 11 à 20, celles qui spécifient la nature des bateaux de 20 à 30 et supposons aussi que, dans ces catégories, l'expression 11 signifie = part ce matin; l'expression 23 = cuirassés.

Il s'agit d'envoyer au correspondant, sous une forme qui n'inspire aucun soupçon, les nombres 11, 7, 23, qui signifieront : partent ce matin 7 cuirassés.

Nous lui télégraphierons :

« Cours du café au Havre cent douze soixante quinze »

ou « cotons filés Roubaix quatre vingt quatre trente » et notre télégramme sera lu en trois parties, l'une : début jusqu'au nom de denrée de 11 lettres; l'autre, nom de lieu, de 7; la troisième, prix de denrée, de 23.

Des dispositions de timbres sur une enveloppe peuvent constituer aussi une numération fort étendue, correspondant à un catalogue de phrases, et c'est une sorte de langage convenu, où le texte à tournure innocente est en quelque sorte formé par l'enveloppe et son adresse.

On appelle aussi, fréquemment, langage convenu, en particulier dans les relations avec le service télégraphique, des textes écrits dans une langue avec des mots appartenant à cette langue, mais ne présentant aucun sens au lecteur ignorant de la clef, parce que les mots du télégramme représentent d'autres mots de la langue. Exemple : envoyez à l'ours cinq monuments délivrés vaches jolis à noirs (envoyez à la maison Fox et C° cinq costumes complets drap noir 115 à 135 francs). On étend même parfois le terme de langage convenu au texte où des mots du télégramme intercalés dans un texte vaguement français appartiennent à des langues étrangères ou à des langages forgés. A notre avis, il vaut mieux garder le mot de langage convenu pour les textes qui se lisent couramment avec un sens apparent, et traiter les autres documents, qui se révèlent à première vue comme ayant subi une déformation pour en cacher le sens, de documents chiffrés ou cryptogrammes.

Nous n'entreprendrons pas l'étude des documents en langage convenu. Avant de passer à l'étude des cryptogrammes, et surtout des différents systèmes classiques de cryptographie, nous écarterons également, mais en en mentionnant l'existence, une série assez importante de documents d'une nature assez spéciale. Ce sont ceux qui ne peuvent être étudiés que sur le texte écrit par leur auteur, ou sur des photographies de ce texte, et qui peuvent à la rigueur se rattacher à l'emploi du langage convenu.

Des inventeurs en effet proposent d'appeler l'attention du destinataire d'une missive sur certaines lettres choisies dans un document dont le sens se suffit à lui-même. On

peut ainsi, comme le raconte About dans son roman : *Trente et Quarante*, souligner certaines lettres d'un journal ou d'une affiche de manière que ces lettres donnent des mots et des phrases. Mais, si l'on souligne, on risque d'attirer l'attention de tiers intéressés à connaître la communication. On peut alors employer des signes moins visibles : déliés supprimés entre la lettre et ses voisines, lettre dépassant la ligne, etc... ou, dans des textes imprimés, en particulier dans des tracts édités pour certaines propagandes et devant passer comme insignifiants, caractères d'imprimerie spéciaux présentant une forme particulière, comme lacunes dans le corps de la lettre, fautes d'impression systématiques, etc...

Nous ne ferons que mentionner les documents de cette nature, tout en faisant remarquer que la suite des lettres ainsi signalées au destinataire peut ne pas donner un texte clair, mais un cryptogramme, dont l'étude rentrera dans le sujet traité plus loin.

Ayant écarté de nos études ultérieures ce qui se rapporte au langage convenu, nous allons commencer l'étude des cryptogrammes, c'est-à-dire des documents qui, par leur seul aspect, révèlent qu'il ne sont pas destinés à être lus sans la connaissance par le destinataire d'une convention ou clef.

Pour la facilité du langage, nous admettrons que « chiffrer » veut dire : transformer un texte clair en texte chiffré, « déchiffrer » s'appliquera à la besogne du destinataire qui, ayant fait avec l'expéditeur la convention qui constitue la clef, transformera le cryptogramme en texte clair. Quant à l'opération du tiers indiscret, cryptologue (1) d'occasion ou de profession (et non cryptographe, les cryptographes sont des instruments à faire des cryptogrammes, des machines à chiffrer), qui cherche à découvrir la clef et à traduire un document qui ne lui est pas

(1) Les personnes qui trouveraient que cryptologue, par sa construction, n'indique pas assez qu'il s'agit d'*écriture* secrète pourraient employer le vocable cryptographiste.

destiné, nous l'appelerons décryptement. (Certains auteurs l'appellent perlustration.) Dans l'établissement d'un système cryptographique, on s'attachera généralement à rendre le chiffrement et le déchiffrement aussi simples et rapides que possible, tout en opposant au décryptement le maximum de difficultés.

Pendant que nous sommes sur le sujet des conditions à chercher dans l'établissement d'un système cryptographique, nous attirerons l'attention du lecteur sur le point suivant : l'usage que l'on veut faire de ce système est un des éléments à considérer tout d'abord dans le choix des procédés. On n'aura pas les mêmes dangers à craindre, ni les mêmes précautions à prendre, si l'on veut faire correspondre deux cryptologues exercés travaillant dans leur bureau, que si l'on doit mettre en relations par T. S. F. les unités d'un front de combat avec les organes de commandement en arrière. C'est un point que bien des inventeurs perdent de vue, et ils en profitent pour critiquer les méthodes officielles et s'indigner que le Gouvernement n'ait pas adopté leurs inventions. Certains rasoirs excellents sont pourtant tout à fait dangereux dans les mains d'un singe, et certains compte-tours délicats fonctionneraient mal sur la roue d'une brouette de tourbière. Il en est de même des systèmes cryptographiques à faire employer par des milliers d'officiers et de sous-officiers qui ne sont pas le moins du monde cryptologues, qui doivent chiffrer dans des abris obscurs avec les nerfs plus ou moins tendus, et qui risquent d'oublier des détails pourtant pleins d'ingéniosité. On ne peut espérer non plus garder secret le principe du système qu'on leur fera appliquer et les éléments secrets doivent se réduire à quelques indications ou clefs.

Le chiffrement dans des postes diplomatiques, lorsque la besogne s'accroît par trop et oblige à prendre du personnel mal exercé, donne lieu lui-même, malgré la qualité et l'intelligence des exécutants, à des malfaçons que la théorie ne peut faire prévoir, mais dont l'expérience permet d'affirmer l'existence, pour la plus grande joie des décrypteurs.

Un système excellent en théorie peut aussi, lorsqu'on

l'exploite intensivement et qu'on le met dans les mains de trop nombreux correspondants, donner lieu à des décryptements beaucoup plus faciles que des procédés méprisés par les auteurs qui n'ont du service du chiffre qu'une connaissance trop limitée ou trop théorique.

En dehors de cet élément d'appréciation pour le choix des systèmes, il faut tenir compte des conditions de transmission. L'emploi du télégraphe impose des règles, dont on peut s'affranchir dans les lettres ou dans les messages téléphonés. L'Administration taxe les cryptogrammes, en dehors des mots de toute langue appartenant à un répertoire publié par les soins de la Conférence de Berne, en en comptant les lettres. Si le cryptogramme peut être coupé en tranches de dix lettres donnant des mots prononçables, même n'appartenant à aucune langue, chaque tranche est taxée pour un mot. Quand les lettres ne donnent qu'un mélange confus de consonnes et de voyelles, on compte un mot pour cinq caractères. Il en est de même pour les nombres, les groupes comptant pour un mot doivent compter au maximum cinq chiffres. Enfin l'on n'admet pas dans un même mot de cinq lettres le mélange de lettres et de chiffres. Ce sont là des éléments qu'on ne peut négliger quand on prépare un système pour chiffrer les télégrammes, tant pour le prix des transmissions que pour les facilités de service qui évitent les erreurs.

Nous n'insisterons pas sur les qualités à rechercher pour un système dans chaque cas particulier, et, abandonnant ces questions préliminaires, nous allons aborder les définitions techniques des systèmes cryptographiques.

Classement des systèmes cryptographiques.

On peut ramener les systèmes cryptographiques à deux genres : les systèmes de substitution et les systèmes de transposition.

On distingue quelquefois aussi les systèmes syllabiques et alphabétiques d'une part, et d'autre part les dictionnaires ou codes.

Les systèmes de substitution donnent des cryptogrammes où les éléments du texte clair, lettres, syllabes, mots, membres de phrases même, sont remplacés par une représentation différente de l'élément clair, mais où l'ordre de ces représentations est conforme à l'ordre des éléments du clair, si bien que si, par exemple, une même syllabe se trouve en tête et en queue du clair, l'élément de tête et l'élément de queue du cryptogramme représentent la même syllabe du clair. On les appelle quelquefois systèmes d'interversion (1).

Les systèmes de transposition sont ceux où les éléments du clair conservent leur représentation, mais où l'ordre en est modifié, si bien que si un texte clair contient par exemple dix fois la lettre a dont une fois en tête et une fois en queue, le cryptogramme contiendra 10 a, mais ces a pourront être groupés par exemple les uns à côté des autres, et la première et la dernière lettre du cryptogramme pourront n'avoir rien de commun avec a.

Ces deux systèmes peuvent d'ailleurs se superposer, de manière qu'à la fois on change les éléments du clair en les remplaçant par des représentations, et on mélange ces représentations pour en troubler la succession.

Les procédés syllabiques ou alphabétiques ne portent que sur les éléments des mots. Certains procédés où les mots du clair sont remplacés soit par des groupes de chiffres, soit par des groupes de lettres, soit par des mots français ou étrangers, et où le nombre des mots ou expressions ayant des représentations de cette nature est tellement grand que les listes de correspondances entre les mots et leurs représentations forment la matière d'un volume, donnent naissance aux dictionnaires ou codes, mais ce ne sont que des procédés de substitution.

---

(1) Valerio a adopté ce nom. On emploie des alphabets où les lettres sont interverties. D'autres auteurs appellent systèmes d'interversion ceux où l'on intervertit les lettres du clair; nous appelons ces procédés systèmes de transposition. Pour éviter toute ambiguité, il y aurait lieu de n'employer le mot interversion ni dans un cas ni dans l'autre.

CHAPITRE II

SUBSTITUTIONS SIMPLES A REPRÉSENTATION UNIQUE

Nous ferons rentrer dans la catégorie des substitutions tous les cryptogrammes où les caractères du clair sont remplacés par des signes différents de ceux ordinairement employés dans la langue du document et où ces signes se succèdent dans l'ordre des caractères qu'ils représentent.

L'écriture d'un texte en signaux Morse, en écriture Braille des aveugles, est une substitution. Il en est de même de la transcription d'un texte en caractères d'une autre langue, et, lorsque ces caractères sont peu connus, les décrypteurs les traitent souvent comme ils traiteraient une écriture forgée de toutes pièces. A la fin de la guerre, les services du chiffre ont reçu pour étude beaucoup de lettres écrites en allemand à l'aide de l'écriture hébraïque cursive, qui se trouva être ignorée des services de contrôle français. Les ouvrages d'Edgar Poë, de Conan Doyle font allusion à des écritures forgées, où par exemple de petits bonshommes remplacent les 24 lettres de l'alphabet, leurs bras et leurs jambes occupant 24 positions différentes. On a fait des alphabets de substitution avec des notes de musique en employant, avec la position dans la gamme, les rondes, blanches, noires, etc..., et les cryptogrammes prennent alors l'aspect innocent de romances ou de fox-trott. Il y a dans les ouvrages de cryptographie de nombreux exemples d'écritures forgées pour être employées entre les membres d'associations secrètes, l'écriture maçonnique par exemple. Nous n'insisterons

pas sur ces curiosités plutôt historiques, et nous en viendrons aux substitutions qui peuvent donner lieu à des transmissions télégraphiques, c'est-à-dire où l'on emploie des lettres et des chiffres, appartenant par exemple à l'écriture française. Les systèmes de cette nature sont parfois qualifiés de systèmes littéraux ou systèmes numériques, ceux où les signes conventionnels ne sont ni lettres ni chiffres étant appelés systèmes stéganographiques.

Pour faire un cryptogramme par substitution, on peut remplacer les lettres du clair par d'autres lettres, dont la succession n'aura aucun sens apparent. A chaque lettre du clair, dans le cas le plus simple, correspondra une lettre et une seule du cryptogramme. Si l'on écrit les lettres du clair sur une liste dans l'ordre alphabétique normal, et qu'en face de chaque lettre on écrive celle qui lui correspond dans le cryptogramme et dont l'ensemble constitue l'alphabet de substitution, on aura le système des deux alphabets : alphabet clair et alphabet de substitution, qui se correspondent, ou ce qu'on appelle le tableau de correspondance relatif au cryptogramme. On applique aux alphabets de substitution pour la facilité du langage un certain nombre de dénominations que nous allons indiquer ci-après.

On appelle alphabet *normal*, ou normalement ordonné, celui où les lettres se succèdent A B C D... Z, en commençant par A. Si l'on considère un alphabet où les lettres se succèdent dans ce même ordre, mais en ne commençant pas par A, nous dirons que l'alphabet est *régulièrement ordonné*. Quand l'alphabet n'est pas régulièrement ordonné il est *interverti*, mais il peut exister certaines relations entre les lettres. S'il n'en existe aucune, que le hasard seul ait déterminé la correspondance des lettres du clair et de celles du cryptogramme, l'alphabet est dit *incohérent*. On l'appelle *réciproque*, lorsque les lettres du clair et celles du cryptogramme sont groupées par deux, de sorte que si M du clair se traduit par X du cryptogramme, X du clair se traduira par M du cryptogramme. On écrit souvent le tableau de correspondance des alpha-

bets réciproques sur deux lignes, les lettres d'une ligne correspondant à celles de l'autre.

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z

A = N, N = A, B = O, O = B, etc.

Si la dernière lettre d'un des alphabets correspond à la première de l'autre, on emploie parfois la dénomination d'alphabets *inverses*.

A B C D E F G H I J K L M
Z Y X W V U T S R Q P O N

Dans certains ouvrages, on applique le nom d'alphabets *complémentaires* à ceux où le total du rang alphabétique de la lettre du clair et de la lettre du cryptogramme est constant, comme dans l'exemple d'alphabet inverse ordonné ci-dessus (A, 1° lettre + Z 26e lettre = 27, B, 2e lettre + Y 25e lettre = 27, etc...).

Enfin, on traite d'alphabets *parallèles* ceux qui sont tels que la différence entre le rang alphabétique d'une lettre de l'un d'eux et celui de la lettre du cryptogramme qui correspond à cette dernière dans l'autre soit constant. On emploie souvent l'expression, à propos d'alphabets parallèles, de *décalage* de l'un par rapport à l'autre de *n* lettres. L'alphabet M N O P Q... est décalé de 2 lettres par rapport à K L M N O..., c'est-à-dire qu'une lettre du premier correspond à celle du second qui la précède de deux rangs dans l'ordre de ces alphabets.

Nous n'avons donné ces définitions qu'afin de permettre au lecteur de suivre certains ouvrages ou les descriptions de certains procédés. En elles-mêmes, elles n'ont pas un intérêt primordial. Ce qui est intéressant, c'est l'établissement d'un alphabet de substitution et la manière de donner la clef du système.

Quand on emploie seulement des alphabets réguliè-

rement ordonnés, on aura un tableau de substitution du genre du suivant :

Clair :	A	B	C	D	E	F	G	H	I	J	K	L	M
Crypto :	C	D	E	F	G	H	I	J	K	L	M	N	O
Clair :	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Crypto :	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

et le mot clair « ennemi » sera chiffré : gppgok.

La clef pourra être indiquée, soit par la différence d'ordre alphabétique entre la lettre du cryptogramme et celle du clair = + 2, soit par l'énoncé de la lettre du cryptogramme qui correspond à A du clair = C.

La méthode de substitution, où l'alphabet du cryptogramme est un alphabet ordonné comme l'alphabet du clair, décalé seulement d'un certain nombre de lettres, est dite méthode de Jules César.

Elle donne lieu à la remarque suivante : si, sous chacune des lettres du cryptogramme, nous écrivons l'alphabet dans l'ordre, en reprenant à A après Z, nous reproduisons le clair quand toutes les lettres ont été modifiées un même nombre de fois.

g	p	p	g	o	k
h	q	q	h	p	l
.	.	.	.	.	.
d	m	m	d	l	h
e	n	n	e	m	i

Le déchiffrement des cryptogrammes chiffrés par ce moyen est donc des plus simples. Il est bon, quand on a affaire à un document qui semble une substitution (nous verrons plus loin comment on se fait une opinion sur ce point) et qui peut émaner de personnes peu cryptologues, comme des prisonniers ou des hommes de troupe, d'essayer ce procédé sur le début du cryptogramme. On s'évite souvent des travaux assez longs et des tâtonnements inutiles.

Si l'on emploie des alphabets incohérents, la clef est constituée par le tableau de concordance. Or, s'il est facile

de se souvenir d'un des termes de ce tableau, à savoir l'alphabet du clair ordonné, il peut être difficile de se rappeler l'autre, et l'on peut avoir des raisons de ne pas le conserver par écrit et de tenir à la reconstituer seulement au moment du besoin.

Il existe plusieurs moyens de rétablir des alphabets incohérents au moyen de clefs faciles à retenir. Nous allons en indiquer quelques-unes.

Soit le mot clef : infanterie.

Écrivons sur une première ligne, dans leur ordre, les lettres de la clef en ne faisant figurer chacune d'elles que la première fois qu'elle apparaît :

i n f a t e r

et écrivons au-dessous, en lignes de même longueur (sauf la dernière) les autres lettres de l'alphabet dans l'ordre normal

i	n	f	a	t	e	r
b	c	d	g	h	j	k
l	m	o	p	q	s	u
v	w	x	y	z		

En relevant ce tableau par colonnes, nous aurons un alphabet interverti donnant lieu au tableau de concordance suivant

Clair :	a	b	c	d	e	f	g	h	i	j	k	l	m
Crypto :	i	b	l	v	n	c	m	w	f	d	o	x	a
Clair :	n	o	p	q	r	s	t	u	v	w	x	y	z
Crypto :	g	p	y	t	h	q	z	e	j	s	r	k	u

et le mot ennemi sera chiffré nggnaf.

Soit le mot clef : commission de délimitation.

Écrivons sur une ligne les lettres du mot clef sans répétitions

c o m i s n d e l t a

et sur une autre ligne au-dessous le reste de l'alphabet, dans l'ordre normal

c o m i s n d e l t a
b f g h j k p q r u v w x y z

Nous considérerons ces deux lignes comme constituant un alphabet réciproque, où les dernières lettres w x y z, n'ayant pas de remplaçantes ne seront pas modifiées par le chiffrement (si l'on emploie des alphabets de ce genre, il sera bon d'écrire par exemple la deuxième ligne à l'envers pour que ce ne soient pas toujours les dernières lettres de l'alphabet qui restent inchangées).

Le mot chameaux sera chiffré bivgqvtx.

Comme nous l'avons dit, au lieu de remplacer les lettres du clair dans les substitutions par d'autres lettres, on peut les remplacer par des groupes de chiffres ou de lettres, ou même par des signes quelconques. Quand on représente les 26 lettres de l'alphabet français par les 26 lettres d'un alphabet, incohérent ou non, tiré de ce même alphabet français, on n'a généralement qu'une représentation pour chaque lettre. Si on employait pour représenter les lettres de l'alphabet normal des *groupes* de lettres ou de chiffres, comme on peut former plus de 26 groupes de cette nature, on pourrait faire correspondre à chaque lettre de l'alphabet normal plusieurs de ces groupes. Il en est de même si l'on invente des signes.

Nous réserverons le nom de substitutions simples, sans addition à cette dénomination (on dit parfois substitution simple à représentation unique), aux substitutions où chaque lettre ou signe du clair n'a qu'une seule représentation dans le tableau de correspondance, cette représentation pouvant être soit un caractère unique, soit un groupe de caractères.

Nous allons continuer l'étude des substitutions simples à représentation unique sans envisager encore les substitutions où une seule lettre du clair peut avoir plusieurs représentations. Nous passerons maintenant des systèmes où une lettre est représentée par une lettre à ceux où elle est représentée par un groupe.

Quand on emploie des groupes de lettres ou de chiffres, pour représenter les lettres du clair, on a un tableau de substitution qui peut être compliqué, et, si l'on ne veut pas le conserver par écrit, il faut avoir recours à des artifices dans le genre de ceux dont nous avons parlé plus haut pour la formation au moment du besoin des alphabets incohérents.

Un artifice fréquemment employé est la formation d'un tableau de 25 cases, où l'on écrit dans un ordre quelconque, mais connu des deux correspondants (soit par lignes, soit par colonnes, en ordre naturel ou en ordre incohérent découlant d'un mot clef) l'alphabet diminué d'une lettre (ordinairement w que l'on remplace par 2 v).

On fait correspondre à chaque ligne et à chaque colonne du tableau une lettre ou un chiffre. On convient de représenter chaque case par un groupe de 2 lettres : par exemple, la lettre de la ligne suivie de celle de la colonne (ou l'inverse, mais il faut choisir une convention qui ne donne qu'une représentation pour chaque case et non deux). On peut employer la clef pour fixer les lettres représentatives des lignes et des colonnes.

Exemple : Soit la clef : infanterie.
J'écris dans le carré un alphabet incohérent composé de infater suivi du reste de l'alphabet. Au-dessus des colonnes, j'écris les 5 premières lettres de infater, à côté des lignes les 5 dernières :

	i	*n*	*f*	*a*	*t*
f	i	n	f	a	t
a	e	r	b	c	d
t	g	h	j	k	l
e	m	o	p	q	s
r	u	v	x	y	z

et je conviens de représenter une lettre du clair par la lettre de la ligne suivie de celle de la colonne.

ennemi se chiffre aifnfnaieifi.

En désignant les lignes et les colonnes par des chiffres, tous différents, convenant de placer toujours en tête du

groupe de 2 chiffres le plus élevé de ces deux chiffres, et formant le tableau de 25 par ordre alphabétique parallèle à une diagonale, on aura, avec le tableau ci-dessous :

	0	2	4	6	8
1	a	c	f	j	o
3	b	e	i	n	s
5	d	h	m	r	v
7	g	l	q	u	y
9	k	p	t	x	z

la représentation suivante du mot ennemi = 326363325443.

On inventera à l'infini des systèmes de ce genre, mais ils impliquent toujours une loi, afin de construire le tableau à l'aide de la clef. On peut trouver avantage à ne se fixer aucune loi, à choisir au hasard les représentations de chaque lettre; la suite des nombres de deux chiffres par exemple employés pour représenter les lettres n'étant en aucun manière ordonnée. Quand on lira le tableau de correspondance, on trouvera facilement à sa place alphabétique, au chiffrement, la lettre du clair et on lira en face le nombre qui doit la représenter dans le cryptogramme, mais au déchiffrement il faudra chercher dans la liste des nombres, sans aucun guide, celui dont on désire le sens. Pour simplifier cette recherche, on pourra alors faire deux tableaux de correspondance, l'un, dit *chiffrant*, où les lettres du clair sont en ordre alphabétique et où les nombres à substituer forment une liste incohérente, l'autre, dit *déchiffrant*, où les nombres, qu'on lit dans le cryptogramme, sont en ordre numérique, et peuvent se retrouver par suite facilement à la lecture, chacun ayant en face de lui l'indication de la lettre à écrire pour déchiffrer.

Bien que des groupes de deux lettres ou chiffres puissent sembler suffisants pour fournir un ample choix de représentations des lettres, on a parfois affaire à des groupes plus longs. Dans la partie plutôt historique de la cryptographie, on trouvera même l'alphabet de Lord Bacon, où les seuls caractères employés sont A et B, mais où

chaque lettre est représentée par 5 caractères (C = AAAAA, S = AABBB, etc...).

L'usage de la télégraphie n'autorise guère aujourd'hui une pareille prodigalité, mais, en superposant à ces combinaisons certaines conventions secrètes, en employant par exemple deux formes de lettres, l'une représentant A, l'autre B (si on suppose que toutes les minuscules figurent les A, toutes les majuscules les B, la graphie vingt, en minuscules, représentera A, viNGT représentera S), on peut entreprendre sur les chiffres anciens certaines recherches curieuses. Un exemple intéressant d'étude de ce genre, relatif à Shakespeare, a été publié dans le *Mercure de France*, de 1921 à 1923, par le général Cartier, ancien chef de la Section du Chiffre au ministère de la Guerre (Voir numéro du *Mercure de France*, du 1er février 1923).

Avant d'indiquer d'autres physionomies des systèmes de substitution simple, nous parlerons du décryptement de ces systèmes, en prenant comme type le cryptogramme où les lettres du clair sont représentées par des lettres. Il y a lieu de remarquer que lorsqu'ils ont affaire à des écritures qui ne leur sont point familières, à des procédés stéganographiques, beaucoup de cryptologues préfèrent, au lieu de travailler sur le texte communiqué, remplacer chaque caractère par une lettre ou un nombre. Ces derniers signes, auxquels leurs yeux sont accoutumés, leur permettent de voir certaines particularités qui leur échappent dans l'écriture primitive. On doit donc reconnaître les différents caractères et les identifier. Nous supposerons d'abord qu'ils ne sont pas en nombre supérieur à 26, ce qui permet d'escompter que le texte est français, et nous ferons de plus l'hypothèse qu'il s'agit en effet d'un texte français.

Les cryptogrammes se présentent parfois sous forme de groupes de lettres de longueur inégale, ce qui donne à penser que l'auteur a chiffré chaque mot du texte clair et a laissé subsister les séparations entre les mots. Mais, le plus souvent, et pour répondre aux règles de service

télégraphique, on a affaire à des successions de groupes de 5 lettres ou chiffres où rien n'indique le commencement et la fin des mots, ou bien, dans les lettres, à des lignes ininterrompues.

Le décryptement des substitutions est basé sur la considération des fréquences.

Si l'on compte, dans différents textes d'une même langue, assez longs pour que les règles du calcul des probabilités puissent s'appliquer, le nombre de certains éléments, lettres, suites de 2 lettres que l'on appelle bigrammes, mots fréquemment employés tels que verbes auxiliaires, conjonctions, prépositions, etc... on trouve que chacun de ces éléments a un pourcentage à peu près constant sur l'ensemble des éléments de même nature (lettres, bigrammes, mots).

Ainsi, si l'on considère le nombre de fois qu'une même lettre se reproduit dans un texte de 1.000 lettres, on trouvera, en français, les pourcentages ou fréquences suivantes :

E = 17	N = 8,7	A = 7,2	I = 6,8
R = 6,8	S = 6,8	T = 6,7	U = 6,7
O = 6,6	L = 4,9	D = 4,6	C = 3,5
M = 3	P = 2,8	V = 1,8	F = 1,3
B = 0,9	G = 0,7	Q = 0,7	H = 0,5
X = 0,5	J = 0,3	Y = 0,3	Z = 0,3
K = 0,01	W = 0,01		

Ces nombres sont empruntés à Valerio. D'autres auteurs (Viaris par exemple) en donnent d'autres qui diffèrent un peu. On a besoin pratiquement de se rappeler qu'une proportion de 1/5e à 1/7e de E est normale, et que les lettres les plus fréquentes sont, à peu près dans l'ordre, celles qui forment le mot à tournure cabalistique ESARINTULO. L'S et l'A, dans les relevés de Viaris arrivent en effet à 8.0 et 8,2 % tandis que l'N n'a que 7,2 %. Un autre point intéressant est le pourcentage des voyelles sur l'ensemble des lettres qui est de 44 %.

Nous rappellerons la fréquence des lettres dans quelques langues étrangères :

Allemand :

E = 18	N = 9,4	R = 7,6	I = 7,2
T = 6,6	S = 6,3	D = 5,5	U = 5,1
A = 4,6	H = 4,4	L = 3,7	C = 3,1
G = 3,0	O = 2,5	Z = 2,4	M = 2,0
B = 1,9	W = 1,6	F = 1,5	K = 1,3
V = 1,0	P = 0,7	J = 0,6	

Anglais :

E = 13	T = 9,1	O = 8	A = 8
N = 7,5	R = 7	I = 6,5	S = 6,5
H = 6	D = 4	L = 3,5	C = 3
F = 3	U = 3	M = 2,5	P = 2
Y = 1,5	W = 1,5	G = 1,5	B = 1
V = 1	K = 0,5	X = 0,3	J = 0,1
Q = 0,1	Z = 0,1		

Russe :

(orthographe d'avant-guerre avec les lettres muettes)

O = 10 A = 8 N = 7 E = 6
T = 6 I (lettre en N renversé) = 5 R = 5
S = 5 V = 5 E = 4,5 I = 4 D = 3
IA = 3 P = 3 K = 3 M = 2,5
I (lettre de forme latine) = 2 OUI = 2 OU = 2
IE = 2 Z = 1,5 B = 1,5 I (muet) = 1,5
TCH = 1 G = 1 I (final) = 1 X = 1
J = 1 IOU = 1 CH = 0,5 CHTCH = 0,3
TZ = 0,2 E (après IE dans l'alphabet = 0,2
F = 0,1

Espagnol :

E = 14	A = 12	O = 9	N = 7	S = 7
I = 7	R = 6,5	L = 5,5	D = 5	C = 5
T = 4,5	U = 3,5	P = 3	M = 3	G = 1,5
B = 1	Y = 1	V = 9	F = 7	J = 6
Q = 5	Z = 4	H = 3	X = 2	GN = 1
K = 0	W = 0			

Italien :

E = 12,5	I = 10	A = 10	O = 9	R = 7
L = 6,5	N = 6,5	T = 6	S = 6	C = 4
D = 4	P = 3	U = 3	M = 2,5	G = 2
V = 1,5	H = 1	B = 1	Z = 1	F = 1
Q = 0,5	J = 0			

On trouvera dans Valerio, Ier Volume, des renseignements complémentaires sur les principales langues (bigrammes fréquents, particularités diverses), et des matériaux de toute sorte tant sur ces dernières que sur la langue française.

De même qu'il y a une fréquence pour les lettres, il y en a une pour les suites de deux lettres ou bigrammes. Nous empruntons encore à Valerio le tableau de fréquence des bigrammes français obtenus en relevant sur un texte d'environ 1.500 lettres les séquences de deux lettres. On n'a pas tenu compte de la séparation des mots, si bien qu'avec cette manière de faire, des Z de commencement ou de fin de mots ou des Q terminant le mot cinq par exemple peuvent faire bigramme avec des lettres auxquelles ils ne seraient jamais accolés à l'intérieur d'un mot français. Les lettres du haut du tableau sont les premières des bigrammes, celles de gauche les secondes, ainsi AE ne s'est pas rencontré, EA s'est rencontré 8 fois. Les nombres de la ligne du bas sont les fréquenees sur 1.500 lettres. Ils diffèrent de quelques unités du total des chiffres de la colonne, les lettres de début de phrase ou de fin n'ayant pas fourni de bigrammes. (Voir tableau ci-après.)

Table des Bigrammes

(1.500 lettres environ)

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	1	4	8	12	8	4		1	2			12	3
B	3												4
C	4		4		12				1				
D	1		1	1	21				4				
E		2	11	32	10	3	4	6	17	2		32	19
F	1				5	2			1				
G	2				3				4				
H			3		2								
I	10	1	1	8	1	1	1					5	8
J					1							1	
K													
L	9	3			16				7			10	
M	4		1	1	20				3				1
N	18				39		4		10			2	
O		2	14	2		6			10			4	6
P	8				12								4
Q	1				1				1			1	
R	19	1	2	4	19	2	2		7				
S	3	1			42				8				
T	10		2		17				18				
U	8		6	8	13			1				4	1
V	7				6				2				
W													
X									6				
Y												2	
Z					1								
	109	14	54	68	255	19	11	8	103	5	»	73	46

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
9		6		10	5	5	7	7			1	3
1	1						1					
10	3			4	8		6				1	
8	1			4	13	13	1			1		
24		8		25	19	21	8	9		3		
2		1		1	1		3				1	
				1								
						1				1		
3	10	1		11	12	17	8	4		1		
					1		2					
1	1	1		8	6	5	2			2		1
	6			3	2	1	4					
12	28				1	4	13					
10		11		12	6	5		6			1	
	1	2		4	3	2	6					
2				1	2	1					1	
1	11	4		3	1	12	15	1				
16	7	4		3	6	4	9					
25	1	1		7	8	3	8					
3	27	3	11	3	8	4						
2	1			4	1		5					
							2					
2	1											
						3						
131	99	42	11	104	101	101	100	77	»	8	5	4

Parmi les procédés qui facilitent souvent certaines remarques il faut placer celui qui consiste à représenter la fréquence d'une lettre par une ligne de longueur proportionnelle à cette fréquence. Si par exemple, pour le français, nous portons en abscisses 26 longueurs égales et qu'en chaque point nous écrivions une lettre de l'alphabet normal, et tracions une ordonnée, que nous portions sur l'ordonnée de A sept fois une unité arbitraire, sur celle de B une fois cette unité, sur celle de C 3, 5, de D 4, 6, de E 17, etc..., nous aurons un dessin d'aspect caractéristique, qu'on peut encore préciser en joignant par un trait les extrémités de toutes les ordonnées, et qui forme le graphique normal de la langue française. Dans la méthode de Jules César, le graphique du cryptogramme serait analogue au graphique normal, transporté parallèlement à lui-même.

La notion de fréquence étant admise, on comptera chaque caractère du cryptogramme, et on en déterminera la fréquence pour 100.

Le caractère le plus fréquent correspondra, dans la grande majorité des cas et toujours si le cryptogramme est un peu long et n'a pas été forgé pour faire une curiosité cryptographique, à la lettre E. Nous rappelons que nous traitons ici le cas de substitutions simples, et que dans ce type de cryptogrammes les E doivent avoir une fréquence comprise entre 14 % et 20 %. (Si l'on n'a pas une fréquence de la lettre la plus fréquente comprise entre 1/7 et 1/5, on se méfiera de ne pas avoir affaire à une substitution simple.)

Ceci acquis, nous remplacerons dans notre texte le caractère le plus fréquent par E.

Si les mots du cryptogramme sont séparés, on considérera alors les mots courts où figure e, de, le, ne, en, je, et, est... En se guidant sur la fréquence des lettres, on arrivera à identifier un certain nombre de caractères. On fera attention ainsi que n est plus fréquent que d (ne, de) et beaucoup plus fréquent que j (je). On sera guidé par certaines particularités de la langue française : les lettres isolées indiquent des probabilités de a, j, l, m, n, s, t.

Une lettre redoublée dans le corps d'un mot est probablement une consonne, et les lettres qui précèdent et suivent ce redoublement ont beaucoup de chances d'être des voyelles. La découverte de « le » entraînera celles de « les », de « la ». Les mots présentent des particularités propres qui permettent, lorsqu'on en connaît la longueur et une ou deux lettres, de les identifier sur des listes qu'ont préparées les grands laboratoires de décryptement (mots de n lettres ayant toutes les lettres différentes, ayant deux lettres semblables (ce qu'on appelle une répétition),trois lettres semblables, deux répétitions, un redoublement, des redoublements de 3 lettres, pas de lettre e, 2 lettres e, 3 lettres e, etc...). Si bien qu'en général le décryptement des substitutions simples à mots séparés n'est pas une besogne extrêmement compliquée, quand on est fixé sur la langue et qu'on n'a pas affaire aux langues orientales qui n'écrivent pas les voyelles.

Si les mots ne sont pas séparés, le problème devient beaucoup plus difficile.

Une bonne méthode à suivre, lorsqu'on n'a aucune idée préconçue sur le sujet du cryptogramme, et que l'on veut prendre la méthode analytique, est, une fois l'E déterminé, de s'attacher aux lettres qui précèdent et suivent les E, et de considérer le tableau des bigrammes.

Nous y voyons que les séquences où entre E sont surtout des groupes consonne-voyelle ou voyelle-consonne, mais plus rarement des diphtongues voyelle-voyelle. Or certaines voyelles sont très fréquentes. Dans les lettres très fréquentes, celles qui ne se placent que rarement à côté de E ont donc beaucoup de chances d'être des voyelles. Parmi celles-ci, A ne se place qu'exceptionnellement devant E (fin de mot en a et commencement de mot en e, aéro, etc...). IE est beaucoup plus fréquent que EI; les séquences de O et de E, ou de E et de O, sont très rares; la séquence OU est relativement fréquente. On aura donc des éléments d'étude pour déterminer les voyelles. Lorsqu'on aura découvert les premières voyelles, on fera des hypothèses à ce sujet. On appuiera ces dernières par des considérations basées sur l'espacement des voyelles dans

la langue. Aucun mot français ne renferme de séquence de 5 consonnes. On ne peut trouver de telles séquences qu'en ajoutant à 3 consonnes de la fin d'un mot (et alors la 3e est s) deux consonnes du commencement d'un mot suivant. Sur six caractères différents qui se suivent, il doit donc y en avoir un qui représente une voyelle. Enfin le total du pourcentage des voyelles doit être de 44 % environ. Si l'on ajoute au total des fréquences des voyelles déjà connues, la fréquence d'une lettre sur laquelle on fait l'hypothèse qu'elle est voyelle, cela ne doit pas donner un total très supérieur à 44 %, surtout si ce n'est pas la dernière voyelle à trouver.

Une fois les voyelles trouvées, les considérations de bigrammes aideront à déterminer les consonnes.

On a ainsi pour les consonnes fréquentes :

es	42,	se	19
en	39,	ne	24
el	16,	le	32
er	19,	re	25

S et N suivent donc plus souvent E qu'elles ne le précèdent. L et R au contraire.

On arrive ainsi à établir la traduction de fragments de mots, et, quand ces traductions permettent des hypothèses sur les lettres qui précèdent ou suivent, on renforce ces hypothèses par la considération des fréquences.

La marche indiquée ci-dessus n'est pas d'ailleurs à développer dans un ordre rigoureux : recherche des voyelles, puis des consonnes. A mesure que l'on peut faire des hypothèses, il faut les faire et les exploiter. Ainsi on peut très bien ne pas trouver facilement certaines voyelles, mais avoir l'attention attirée par des bigrammes commençant par E et revenant à des intervalles inférieurs à une douzaine de lettres; on pensera à une série de féminins pluriels et on aura l'ES; la dernière lettre du document est à considérer à ce point de vue.

Nous n'essaierons pas de discuter plus avant sur les procédés à prendre pour ces opérations. Chaque crypto-

logue a ses petits « trucs » dans l'application des procédés généraux. Nous donnerons seulement un exemple de la manière dont on peut traiter un tel problème.

Soit le cryptogramme de 130 lettres :

	10		20		30
yjxmg	xbxuf	jgecu	jebzd	xamnm	zdflg
	40		50		60
fafnj	ofndj	gvjxe	fnnme	vrjzj	kafnb
	80		90		190
fnzag	ncuje	bnrux	ofnjg	nnxkx	felgf
	100		110		120
bjrvf	nofui	fxaaf	gtfvr	fafku	fnbje
	130				
nadxn	vmxuf				

Faisons les fréquences :

a 8, b 6, c 2, d 4, e 7, f 20, g 8, i 1, j 12, k 3. l 2, m 5, n 16, o 3, r 4, t 1, u 7, v 5, x 11, y 1, z 4.

f est la lettre la plus fréquente; 20 sur 130 donne 15 1/2 %. Ce n'est pas tout à fait normal pour l'E, mais c'est une proportion possible, et, le cryptogramme étant court, il ne faut pas être trop exigeant pour les résultats basés sur le calcul des probabilités.

Nous admettons f = E.

Nous allons alors compter pour chaque lettre, les séquences qu'elle donne avec E; nous écrirons ci-dessous les lettres du cryptogramme dans l'ordre des fréquences décroissantes, en indiquant pour chacune d'elles, par un nombre précédent celui qui indique la fréquence, le nombre de fois qu'elle précède f, par un nombre suivant le susdit, le nombre de fois qu'elle suit f.

n	= 0/16/8,	j	= 0/12/1,	x	= 1/11/1,	g	= 2/8/1,
a	= 4/8/2,	e	= 4/7/1,	u	= 3/7/1,	b	= 1/6/1,
m	= 0/5/0,	v	= 1/5/1,	d	= 1/4/0,	r	= 1/4/0,
k	= 0/3/1,	o	= 3/3/0,	z	= 0/4/0,	c	= 0/2/0,
l	= 0/2/1,	i	= 1/1/0,	t	= 1/1/0,	y	= 1/1/0.

Voyelles probables, comme étant fréquentes et donnant peu de séquences avec E = j, x, m.

En comptant f, nous avons donc 4 voyelles probables. Cherchons tout de suite à déterminer les autres. Le total des fréquences de f, j, x, m est 48. La proportion de 44 % sur 130 lettres donnerait 57. La lettre Y étant peu fréquente dans le clair n'apportera pas un gros élément au total. C'est vers les lettres qui se rencontrent 8 fois, c'est-à-dire probablement chez g ou a, peut-être chez e ou u, que nous devons trouver la voyelle cherchée, a est à écarter, il a trop de séquences avec e. On peut donc prendre g comme première hypothèse.

Nous pouvons d'ailleurs essayer autrement de chercher notre voyelle manquante. Soulignons dans notre texte les lettres f, j, x, m, admises comme voyelles.

	10		20		30
y*jxmg*	*xbxuf*	*j*gecu	*j*ebzd	*xamnm*	zd*f*lg
	40		50		60
*fa*f*nj*	o*f*nd*j*	gv*jxe*	*f*nn*m*e	vr*jzj*	ka*f*nb
	70		80		
*f*nzag	ncu*j*e	bnrux	o*f*n*j*g....		

Entre les 61e et 67e lettres, nous avons une séquence de 7 lettres non soulignées nzagncu. L'une d'elles doit être une voyelle. Or n donne trop de séquences avec E, z et c sont bien rares pour une voyelle autre que Y, bien fréquentes pour Y. Restent u et g : c'est g qui donne le moins de séquences avec E (3 sur 8 fois, contre 4 sur 7). D'autres arguments, non décisifs pris isolément, mais formant une forte présomption par leur recoupement, plaident pour g voyelle : à la lettre 80, elle est devant un redoublement et les redoublements autres que ée (et rarement oo) sont des consonnes, à moins qu'on ne soit à cheval sur deux mots, et sont entre deux voyelles. Si nous comptons les séquences de voyelles hypothétiques fjxm avec u et g, nous en trouvons moins pour g que pour u.

Nous pouvons donc admettre l'hypothèse que g est une

voyelle. Remarquons que ce procédé de séparation des voyelles en considérant les intervalles, exposé dans Valerio, est général et fécond. En supposant que les deux séquences de l'x avec l'f nous aient effrayés, et que nous n'ayons admis que f, j et m comme voyelles, le procédé appliqué; au cryptogramme :

10		20		30
y*j*x*m*g	xbxu*f*	*j*gecu	*j*ebzd	xa*m*n*m*	zd*f*lg
40		50		60
*f*a*f*n*j*	o*f*nd*j*	gv*j*xe	*f*nn*m*e	vr*j*z*j*	ka*f*nb
70		80		90
*f*nzag	ncu*j*e	bnrux	o*f*n*j*g	nnxkx	*j*elg*f*....

nous donnait à étudier les séquences gxbxu, ebzdxa, nzagncu, ebnruxo, gnnxkx, où la fréquence de l'x ne peut manquer d'attirer l'attention. Lorsqu'on hésite entre plusieurs lettres pour déterminer les dernières voyelles, on peut compter pour chaque lettre douteuse le nombre et la grandeur des intervalles qui la séparent des voyelles déjà trouvées (par exemple 3 intervalles de 1, 4 intervalles de 2, 1 intervalle de 6) et établir la moyenne de ces intervalles en faisant la somme des produits du nombre d'intervalles par leur grandeur [par exemple $(3 \times 1) + (4 \times 2) + (1 \times 6)$] et en la divisant par le nombre total d'intervalles considérés $(3 + 4 + 1)$. La lettre pour laquelle cette moyenne est la plus grande a bien des chances d'être la voyelle cherchée.

Cherchons donc à identifier nos voyelles probables j, x, m, g. Le tableau des bigrammes (séquences avec E) et les fréquences nous mènent à identifier j avec A, et m avec O, ces deux lettres donnant peu de séquences avec E, et A étant la plus fréquente. Des considérations analogues nous feront adopter x = I et g = V.

Écrivons donc ces lettres dans le cryptogramme :

10		20		30	
yjxmg	xbxuf	jgecu	jebzd	xamnm	zdflg
.AIOU	I.I.E	AU...	A....	I.O.O	..E.U

40		50		60	
fafnj	ofndj	gvjxe	fnnme	vrjzj	kafnb
E.E.A	.E..A	U.AI.	E..O.	..A.A	..E..

70		80		90	
fnzag	ncuje	bnrux	ofnjg	nnxkx	felgf
E...U	...A.	I	.E.AU	..I.I	E..UE

100		110		120	
bjrvf	nofui	fxaaf	gtfvr	fafku	fnbje
.A..E	..E..	EI..E	U.E..	E.E..	E..A.

nadxn	vmxuf
...I.	.OI.E

Cherchons les consonnes. Dans les fréquences, celle de n est la plus forte. Cette lettre suit E plus qu'elle ne le précède. Elle est la 3e du groupe présumé de 5 consonnes de la 70e à la 74e lettre. Elle donne avec E des séries de séquences fn qui correspondent parfaitement à des ES possibles dans une phrase. Nous admettrons donc n = S, et nous écrirons les S dans le cryptogramme.

u, d'après sa fréquence, et précédant E plus qu'il ne le suit, peut correspondre à R. Si nous essayons de remplacer u par R, nous arrivons à deviner le début du cryptogramme : J'AI OUI DIRE. Nous en tirons y = J, b = D. Ce dernier résultat n'est pas en contradiction avec la fréquence, mais remarquons que les séquences DE sont moins nombreuses dans notre texte qu'elles ne le sont normalement.

Nous avons deux fois le bigramme UE précédé de I qui ne figure que ces deux fois. Nous conclurons I = Q.

Pour avoir la série des lettres fréquentes « erasintulo », il nous faut encore N T L. Les fréquentes du cryptogramme non identifiées sont e, a, v — e et v suivent E aussi souvent qu'elles le précèdent, a le précède moitié plus souvent qu'elle ne le suit. On essaiera a = L, et, se basant sur l'ordre des fréquences e = N, v = T.

Arrivé en ce point du décryptement, il deviendra facile de compléter les mots et de trouver le texte clair :

yjxmg	xbxuf	jgecu	jebzd	xamnm	zdflg
JAIOU	IDIRE	AUNGR	ANDPH	ILOSO	PHEQU
fafnj	ofndj	gvjxe	fnnme	vrjzj	kafnb
ELESA	MESHA	UTAIN	ESSON	TCAPA	BLESD
fnzag	ncuje	bnrux	ofnjg	nnxkx	felgf
ESPLU	SGRAN	DSCRI	MESAU	SSIBI	ENQUE
bjrvf	nofui	fxaaf	gtfvr	fafku	fnbje
DACTE	SMERV	EILLE	UXETC	ELEBR	ESDAN
nadxn	vmxuf				
SLHIS	TOIRE				

Il faut remarquer que bien souvent on devra procéder à plusieurs hypothèses sur la correspondance de certaines lettres avant de trouver celle qui convient. Mais nous venons d'exposer ici une méthode pour conduire systématiquement les essais : c'est la méthode en quelque sorte analytique.

Il en est une autre, qui est à cette première ce que la méthode géométrique est à l'analytique dans certaines sciences; et, suivant la tournure d'esprit des opérateurs, certains préfèrent l'une à l'autre, et certains, incapables d'aboutir avec l'une des méthodes à la solution d'un problème difficile, la conquièrent au moyen de l'autre avec une maestria déconcertante.

Cette autre méthode est celle du mot probable.

On fait, soit par suite d'opinions plus ou moins assises concernant le sujet du cryptogramme, en s'appuyant sur ce qu'on sait de sa date, des correspondants, soit par suite d'une indiscrétion sur le sujet traité, etc..., l'hypothèse qu'un certain mot *doit* se trouver dans le texte; et on cherche dans le texte une série de lettres qui reproduise la physionomie de ce mot, ses particularités orthographiques.

Supposons que par suite d'une conversation avec le

destinataire du cryptogramme précédent, nous supposions que le texte renferme le mot : philosophe ou philosophie.

Nous devrons trouver dans le cryptogramme une séquence où nous rencontrerons deux fois, avec 5 lettres d'intervalle, un bigramme correspondant à ph..., lettres assez rares. Les trois lettres précédent le second bigramme seront fréquentes, et la même (o), s'y retrouvera deux fois. Certains décrypteurs ne s'attachent même pas, dans une première recherche, à la considération des fréquences, et, sous leur cryptogramme, copié de manière que toutes les lettres se trouvent également éloignées l'une de l'autre, ils promèneront un morceau de papier portant au même intervalle les lettres du mot PHILOSOPH, qu'ils identifieront facilement avec zdxamnmzd. Ayant ainsi obtenu une « entrée » dans le cryptogramme, ils déduiront les lettres inconnues des lettres connues et du texte.

Dans certaines classes de documents, télégrammes militaires ou diplomatiques, affaires de banque, de mines, etc..., il n'est pas impossible de faire des hypothèses très sérieuses sur la présence de certains mots dans le texte. Lorsqu'un décrypteur a beaucoup travaillé sur certains correspondants, et est habitué à leurs expressions, il arrive à se faire un bagage de mots à essayer. Alors les changements de clefs, et parfois de système, ne lui opposent plus les difficultés d'une étude de décryptement absolument nouvelle qu'exigerait la méthode analytique.

CHAPITRE III

SUBSTITUTIONS SIMPLES A REPRÉSENTATIONS MULTIPLES

Nous nous sommes étendus sur le décryptement des substitutions simples, parce qu'il faut parfaitement connaître ces procédés pour aborder les déchiffrements des substitutions plus compliquées.

Fort nombreux en effet sont les procédés pour aggraver dans les substitutions la besogne du décrypteur.

Nous avons vu que la base du décryptement, c'est la considération des fréquences. La lettre la plus fréquente correspond à l'E. On va tâcher de masquer ces fréquences, de faire que la lettre la plus fréquente ne corresponde plus à l'E, et le décrypteur sera embarrassé.

On peut par exemple distinguer E accentué (qui a sa place dans l'alphabet Morse) et E non accentué.

Un autre procédé assez simple, qui n'augmente pas le nombre de représentations dans le tableau de correspondance et n'exige que l'emploi des 26 caractères de l'alphabet, c'est de donner à E plusieurs représentations en supprimant celles de lettres rares : J qu'on remplace dans le clair par I, W qu'on remplace par deux V, K qu'on remplace par C ou Q.

Par ces moyens la fréquence de l'E se trouve répartie entre plusieurs caractères.

Le décrypteur doit envisager la possibilité d'un tel artifice. S'il opère par mot probable, il ne s'inquiétera pas de représentations différentes pour les E du mot qu'il essaie. S'il suit la voie analytique, il aura recours au tableau des bigrammes qu'il établira pour son cryptogramme,

sur le modèle du tableau normal des bigrammes figurant plus haut. Il y remarquera que certaines lettres donnent des fréquences avec beaucoup d'autres lettres de l'alphabet, ne laissant que relativement peu de cases vides dans leur ligne et dans leur colonne. Ces lettres ont des chances d'être des voyelles, surtout si elles se combinent peu entre elles, et on peut découvrir ainsi plus de voyelles que n'en comporte l'alphabet de la langue employée. Les questions des redoublements (consonnes probables), des lettres qui les précèdent et les suivent (voyelles probables), doivent être soigneusement examinées. Enfin il sera bon de faire une recherche dont nous parlons pour la première fois, mais que nous mentionnerons bien souvent au cours de ces études, celle des répétitions.

Supposons que le mot « ENNEMI » soit chiffré deux fois dans le cryptogramme, où l'E a deux représentations, et que ces deux chiffrements soient les suivants : FGGWNJ et FGGFNJ.

Si le chiffreur n'était pas faillible, cette hypothèse ne se produirait probablement pas et « Ennemi » serait chiffré toujours de la même manière. Mais tous les chiffreurs sont faillibles. Nous conclurons sans paraître trop audacieux que W et F sont deux représentations d'une même lettre du clair, et, remplaçant partout où elle figure la seconde de ces deux représentations par la première, nous retomberons sur la substitution simple que nous savons traiter. On recherchera donc dans le cryptogramme toutes les séquences à peu près identiques, on les soulignera à l'aide de crayons de couleur ou on les portera sur une feuille de papier de manière à pouvoir les comparer, et ces comparaisons pourront amener à reconnaître qu'on n'a plus affaire à une substitution simple proprement dite, mais à une substitution simple à représentations multiples, et serviront en même temps à ramener cette dernière à une substitution simple proprement dite.

Ce procédé, qui ne peut guère s'étendre avec le tableau de concordance en lettres, peut prendre une très vaste extension si l'on emploie des caractères arbitraires, ou des groupes de lettres ou de chiffres. Dans la pratique,

nous avons eu fréquemment à étudier des cryptogrammes chiffrés avec des substitutions simples à représentations multiples, c'est-à-dire avec des tableaux de concordance où un même caractère ou bigramme du cryptogramme représente toujours la même lettre du clair, mais où une lettre du clair peut être représentée par plusieurs caractères ou polygrammes du cryptogramme.

De tels procédés peuvent être réalisés, ou par un tableau de concordance (ou un tableau chiffrant et un déchiffrant) où figurent sur une colonne toutes les lettres du clair, ayant en face d'elles leurs différentes figurations, ou par des tableaux de 25 cases comme ceux dont nous avons parlé, mais où l'on admet pour chaque lettre plusieurs représentations.

Si l'on place dans les 25 cases les 25 lettres, et que chaque colonne et chaque ligne corresponde à une lettre ou un chiffre choisis de telle sorte qu'en lisant dans l'ordre : ligne-colonne, on ne retrouve jamais un groupe obtenu en lisant dans l'ordre colonne-ligne (si par exemple les lettres des colonnes sont différentes des lettres des lignes) on aura 2 représentations pour chaque case, suivant qu'on fera suivre la lettre de la ligne de la lettre de la colonne ou qu'on l'en fera précéder :

	1	2	5	6	9
3	a	f	h	j	n
4	g	b	l	p	r
7	i	m	c	t	v
8	k	g	u	d	y
0	o	s	n	z	e

Dans le tableau ci-dessus 1 peut être représenté par 45 ou 54, sans crainte de confusion. En admettant plusieurs représentations pour chaque colonne et chaque ligne, on multiplie les représentations des lettres.

	1,2	3,4	5,6	7,8	9,0
1 3	z	j	k	l	m
5 7	y	i	b	c	n
9 0	x	h	a	d	o
2 4	v	g	f	e	p
6 8	u	t	s	r	q

Tableau B.

	S,E	N,R	F,B	A,C	T,D
G M	f	g	h	i	j
H P	p	q	r	s	t
J Q	u	v	x	y	z
K S	k	l	m	n	o
L X	a	b	c	d	e

Tableau C.

Dans le tableau B, à condition de fixer l'ordre : colonne-ligne, ou ligne-colonne, nous avons également 4 représentations par lettre; par exemple avec l'ordre ligne-colonne, h est représenté par 93, 94, 03, ou 04. Mais il faut fixer l'ordre, car dans l'ordre colonne-ligne 93 représenterait m, et 04 p.

Dans le tableau C, les lettres des colonnes étant différentes de celles des lignes, nous avons 8 représentations par lettre : q peut être remplacé par HN, HR, PN, PR, NH, NP, RH, RP.

Des cryptogrammes de cette nature sont déjà compliqués, lors même qu'un unique tableau de concordance reste quelque temps en service et permet d'avoir une certaine quantité d'éléments de travail.

Le principe des recherches est l'examen des répétitions. Il faut arriver à diminuer le nombre des représentations d'une même lettre. Dans la pratique, la chose est souvent plus facile que ne le promet la théorie. Les lettres rares donnent des renseignements aussi utiles que les lettres de la série « erasiutulo » dont on a dilué les fréquences. Considérons en effet le tableau C, tel qu'il est construit, et supposons un cryptogramme forgé avec ce tableau. Les combinaisons représentant le z (T, D, J, Q) seront rares ou inexistantes. Au contraire (T, D, K, S) = o, et

(T, D, L, X) = e seront fréquentes. Dans la colonne voisine (A, C, J, Q) = y, rares, (A, C, K, S) = n fréquentes. On arrive ainsi à considérer K, S comme faisant partie d'une autre combinaison indicatrice de ligne ou de colonne que J, Q, puisque ces deux dernières lettres paraissent rarement avec A, C, T, D, tandis que K et S y paraissent fréquemment, et on peut avec suffisamment d'éléments identifier entre eux certains indicatifs de lignes et de colonnes et en réduire le nombre. Mais, comme nous l'avons dit, c'est surtout sur les répétitions où le chiffreur emploie certains mêmes groupes pour quelques-unes des lettres, et des groupes différents pour d'autres, qu'il faut compter.

Exemple : soient les deux débuts de télégrammes

(1)	IPTSQ	IFPIX	HDTPE	LXBGF	TXSBA
(2)	EPSTQ	IPFEX	TPDPX	IXBMF	DLKBG
(1)	MSNAG	HDXIM	CPFTX		
(2)	CNSAM	TPLIC	GBHTL		

qui l'un et l'autre, avec le tableau C, veulent dire : « pour attaché militaire ». En les écrivant l'un sous l'autre, et en les comparant, on voit au 4e groupe apparaître une des séquences XBGF et XBMF qui amorcent l'hypothèse que M du texte 2 peut être remplacé par G du texte 1. Cette hypothèse se recoupe au 6e groupe (AG = AM). L'aspect général des groupes 1 et 2, où TS correspond à ST, FP à PF, aiguillera sérieusement l'attention d'un décrypteur *averti* sur la formation du crypto par groupe de 2 lettres et la représentation d'une lettre par un groupe de 2 caractères *dont l'ordre* est indifférent (TS = ST). Cette remarque fondamentale ayant été faite, la comparaison des deux textes permettra de retrouver les éléments désignant les lignes et les colonnes (IP = EP, donc I = E, recoupé par IX = EX, DP = TP = HD, d'où D = T, H = P, etc...). Bien entendu, dans la pratique, les choses ne seront pas souvent faciles à reconnaître sur deux seuls exemplaires, mais des comparaisons nombreuses faites avec esprit de suite amènent, parfois au bout de plusieurs

jours ou de plusieurs semaines, l'observation d'un détail qui aiguille les identifications que nous avons supposées ici, et permettent au décrypteur de reconnaître et le procédé, et les éléments du décryptement.

Le procédé du mot probable, combiné avec les fréquences, doit être employé dans ces travaux : nous l'avons utilisé dans des études qui donnèrent des résultats plusieurs années de suite, de la manière suivante. Les lettres rares restent rares quel que soit le procédé. Nous faisions le relevé des fréquences de chaque bigramme, et nous cherchions un mot probable, dans le genre du mot philosophe cité plus haut, où des lettres rares se trouvaient à un intervalle donné (nous ne parlons pas d'une répétition, mais seulement de *lettres rares*, qui peuvent être différentes). Les noms propres étrangers : *Wilh*elm, Sazono*ff*, sont souvent avantageux à cet égard. Après avoir souligné de façon différente les bigrammes très fréquents et les bigrammes très rares du cryptogramme, nous promenions au-dessous une feuille de papier où était marqué l'intervalle des lettres rares. Chaque coïncidence était examinée lettre par lettre avec les fréquences, et donnait lieu à un essai de décryptement d'une partie de télégramme. Il fallait bien des tâtonnements, mais on avait souvent d'heureux résultats.

Nous n'avons pas souvent dans la pratique rencontré de substitutions à correspondances multiples en lettres. Nous en avons beaucoup rencontré en chiffres. Le plus souvent, les télégrammes ainsi chiffrés passaient, avant la guerre, en groupes de 5 chiffres ou de 4 chiffres. Une première difficulté était de les distinguer des télégrammes faits avec des dictionnaires, qui passent de la même manière. Il y avait lieu d'abord de compter le nombre total de chiffres du document : si ce nombre était pair, sans être multiple de 4 ou de 5, on avait un premier motif de supposer un système alphabétique et non codique. On s'attaquait alors aux répétitions, et si là également on trouvait des parties communes dont le nombre de lettres, tout en étant pair, n'était multiple ni de 4 ni de 5, la sup-

position était renforcée. Enfin des répétitions ayant de nombreuses coïncidences de 2 chiffres et différences de 2 chiffres n'étaient guère admissibles avec des dictionnaires, comme

2432 1614 1846 2539 et 2432 8514 1872 8039

par exemple.

Il est à remarquer que la nature humaine est ainsi faite, qu'il est extrêmement rare, lorsqu'un chiffreur a plusieurs représentations à sa disposition pour une lettre ou un mot, qu'il n'en adopte pas certaines dont la fréquence, à la longue, est double ou triple des autres. Cela facilite la besogne des décrypteurs, en laissant réapparaître certaines fréquences.

Les tableaux employés par les chiffreurs se réduisent assez souvent à un carré de 100 cases numérotées, dans lesquelles on inscrit les lettres à chiffrer, en donnant plus de représentations aux lettres fréquentes qu'aux autres si le travail est fait par un cryptologue, ou sans prendre cette précaution s'il est fait par un profane. Certaines lettres sautent aux yeux, sur ces tableaux, plus facilement que d'autres, et c'est une des causes qui poussent les chiffreurs à employer plutôt une représentation donnée, pour une lettre, que les autres représentations de la même lettre, moins lisibles.

Quand on connaît le système employé par des correspondants en groupes de 2 chiffres ou de 2 lettres, on commence par couper le cryptogramme en tranches de 2 caractères pour séparer les lettres et chercher les fréquences. Un même groupe de 2 représentant toujours la même lettre du texte, on peut faire le compte des fréquences de chacun de ces groupes et entamer l'étude du cryptogramme par cet élément.

On a alors cherché à dérouter le décrypteur dès ce début de son étude, et il y a des procédés pour rompre cette succession de groupes de 2, si bien que lorsque le décrypteur croit avoir affaire au groupe représentant une lettre du clair,

il est en réalité à cheval sur le 2e caractère d'un tel groupe et le 1er du groupe suivant, et son travail ne signifie rien.

Parmi ces procédés, nous pouvons en citer quelques-uns :

a) Tableau de concordance formé de nombres de 1 et 2 chiffres, tels que le décrypteur reconnaît immédiatement les groupes de 1 chiffre et ceux de 2.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
1	2	3	4	5	60	66	67	68	69	70	76	77	78	79

p	q	r	s	t	u	v	w	x	y	z
80	86	87	88	89	90	96	97	98	99	00

(On prendrait un alphabet incohérent de préférence, mais le principe serait le même; 5 chiffres ne sont employés que dans des groupes de 1, les 5 autres que dans des groupes de 2.)

b) Tableau de 25 cases formé avec des lettres indicatrices de lignes et de colonnes toutes différentes de celles de la première ligne du tableau par exemple, et la convention que ces lettres de la première ligne seront chiffrées par elles-mêmes (ou par leur voisine de droite sur la ligne) au lieu d'être chiffrées par un groupe de 2 lettres.

	A E	D H	G V	U C	B F
	j	k	l	m	n
I X	a	b	c	o	p
O Q	d	e	f	q	r
S Y	g	h	i	s	t
P Z	u	v	x	y	z

Italie se chiffrera GYBSEXLVYHO.

c) Introduction de chiffres (ou lettres) nuls. Prenons par exemple un tableau de concordance de 00 à 99, où nous supprimons tous les nombres commençant par 4. Dans la suite de chiffres qui représente le cryptogramme, le groupement 44 ne pourra pas apparaître, puisque le 4 terminant 04, 14, 24, etc... ne sera jamais suivi du 4 d'un groupe en 40, tandis que 22, 33, etc... se produiront soit par de telles successions (13 suivi de 35 par exemple) soit parce que 33 est dans le tableau de concordance. Si à la suite d'un 4 du cryptogramme, nous écrivons un 4, nul, avant le groupe représentant la lettre suivante, nous aurons intercalé un chiffre qui rompra la cadence des groupes de 2, et que le déchiffreur saura être nul puisque 44 n'existe pas autrement; il le raiera et n'en tiendra pas compte.

Exemple : soit le fragment de tableau

e	i	m	n	o	p	r	s	u
17	24	36	38	61	72	83	84	94
19			54					
25								

ENNEMI REPOUSSÉ, pourra être traduit par 17385 42536 24483 17726 19484 48419. Le décrypteur, ignorant de la nulle, coupera : 17, 38, 54, 25, 36, 24, 48, 31, 77, 26, 19, 48, 44, 84, 19, et trouvera 2 groupes 19, par exemple, quand un seul a été employé.

Nous n'insisterons pas sur ces procédés qui viennent compliquer les substitutions à représentations multiples. Même quand on a beaucoup de documents faits avec le même tableau, les décryptements sont ordinairement difficiles; la base en est la comparaison des répétitions qui permettent d'éliminer les causes de trouble, et la considération des fréquences. Il sera prudent d'établir ces dernières par séries de 50 à 100 groupes au plus, de manière à s'assurer que l'allure générale du graphique des fréquences ne change pas trop dans le cours du document, phénomène qui sera produit par les divers procédés signalés ci-dessus pour tromper sur la composition des

bigrammes. On pourra alors être amené à comparer, particulièrement au moyen des graphiques de fréquences, les fréquences obtenues avec des décalages de 1 lettre ou chiffre dans la succession des tranches de 2, et la comparaison des graphiques avec ou sans décalage, révélant des parties comparables, pourra mettre sur la trace du décalage du cryptogramme et de la méthode employée. En tout cas, nous ne connaissons pas de méthode automatique à appliquer sur des cryptogrammes de cette nature.

Mais, dans ce même genre, il y a mieux. Nous avons admis que les correspondants employaient le même procédé et le même tableau pour un nombre de documents assez considérable, nous fournissant plusieurs éléments d'étude. Or il existe des systèmes où l'alphabet change avec chaque cryptogramme, ou même plusieurs fois au cours d'un même cryptogramme. Il est évidemment fort simple d'avoir plusieurs alphabets de correspondance et d'en changer aussi souvent que l'on veut, en indiquant par un numéro d'ordre ou un groupe réservé à cet usage l'alphabet qu'on emploie. Des tableaux, où les lettres indicatrices des lignes et des colonnes sont changées à la volonté des correspondants, qui indiquent, soit par des conventions relatives aux dates des documents, soit par des mots spéciaux en tête des textes, les éléments de chiffrement, donneront des résultats analogues.

Nous traiterons sommairement un exemple d'emploi d'un appareil donnant une substitution à représentation multiple facilement modifiable.

Supposons que l'on sache que l'ennemi emploie des appareils dans lesquels, entre deux séries de chiffres qu'on ne fait varier qu'en changeant l'appareil entier, se déplace une bande de papier portant les lettres de l'alphabet dans un ordre donné par une clef. Des conventions de dates et d'heures fixent la position de la bande mobile par rapport aux séries de chiffres.

Au début des opérations, la position de la bande fut rarement modifiée, on eut la chance d'avoir plusieurs télé-

grammes chiffrés avec les mêmes représentations (deux pour chaque lettre).

Entre différents télégrammes interceptés au jour 3, choisissons-en deux, dont les débuts offrent des similitudes frappantes :

EM. groupe armées à 7e et 8e corps — 2 h. — 66316 13819 52575 32060 64593 82364 13663 03920 68501 55322 10381 73916 22642 06133 17321 16634 60303 93138 66206 43860 52596 12038 17206 06468 38356 45520 66605 86638 52381 96162 53201 45623 38236 61364 10392 06850 61105 35510 24226 65515 35645 62066 50

EM. groupe à 7e corps — 5 h. — 66386 13119 61573 92060 64683 11766 13643 03920 59502 32052 12615 51017 64162 26650 59535 52060 66593 13564 55346 66064 31926 41917 66525 61123 64561 21711 32662 06010 39313 86620 64316 06853 56206 06668 31146 45520 6660.

Si nous comptons les fréquences des groupes de 2 chiffres dans ces deux textes, nous trouvons :

	10	11	12	13	14	15	16	17	19	20	22	23	24	30	31	32	33	34	35
1er texte :	4	1	0	2	1	2	1	3	2	10	3	3	1	2	2	1	1	1	2
2e texte :	2	2	2	1	1	0	1	4	2	8	1	2	0	1	7	1	0	1	1

	38	39	50	52	53	55	56	57	58	59	60	61	62	64	66	68	92
1er texte :	10	4	3	3	4	3	2	1	1	2	5	5	1	8	9	3	0
2e texte :	2	3	2	2	2	4	3	1	0	3	6	4	0	9	10	1	1

Ces relevés nous confirment que les deux textes ont bien été chiffrés avec des documents identiques, les mêmes groupes y sont fréquents, et surtout, ce qui trompe moins encore, les mêmes groupes y sont rares — car un groupe fréquent dans un texte lorsque le chiffreur a employé une des représentations de la lettre beaucoup plus que l'autre, peut devenir rare dans le second si le chiffreur a opéré de manière inverse, mais une lettre rare ne donne que des groupes rares.

Si alors nous considérons les textes, nous voyons que certaines tranches offrent des similitudes nombreuses. Nous ferons l'hypothèse qu'elles représentent les mêmes mots.

1er texte début : 66 31 61 38 19 52 57 53 20 60 64 59
2e texte début : 66 38 61 31 19 61 57 39 20 60 64 68
1er texte gr. 28 : 66 38 52 38 19 61 62 53 20 14 56 23

38 23 64 13 66 30 39 20 68 50
31 17 66 13 64 30 39 20 59 50
38 23 66 13 64 10 37 20 68 50

1er texte gr. 15 : 17 32 11 66 34 60 30 39 31 38 66 20 64 38 60
2e texte gr. 26 : 17 11 32 66 20 60 10 39 31 38 66 20 64 38 60

1er texte gr. 23 : 60 64 68 38 35 64 55 20 66 60
1er texte fin : 35 64 56 20 66 50 fin
2e texte gr. 16 : 60 66 59 31 35 64 55 34 66 60
2e texte fin : 60 66 68 31 35 64 55 20 66 60 fin

et nous en tirerons les correspondances

38 = 31, 61 = 52, 53 = 39, 66 = 64, 68 = 59, 62 = 57, 23 = 17, 32 = 11, 34 = 20, 30 = 10, 60 = 50.

Il faut une certaine prudence dans ces hypothèses. Des mots très voisins, Charmes et Charles, pourront donner lieu à une hypothèse erronée tendant à assimiler le groupe qui représente M à celui qui représente L. Aussi n'admettrons-nous pas de différences portant sur plus d'une lettre, encadrée entre deux mêmes groupes ou deux groupes reconnus d'autre part équivalents, et ne tiendrons-nous pas compte de la séquence 14, 56, 23 du premier texte groupe 31. On peut, lorsque la matière est moins riche que dans l'exemple, faire aussi des remarques telles que celle-ci, le groupe 31 est fréquent dans le deuxième texte, rare dans le premier. Il est possible que le chiffreur ait adopté plus particulièrement une représentation différente dans chacun des textes, et le groupe 38, qui est rare dans le deuxième texte et fréquent dans le premier, pourrait

bien être accolé avec 31 pour donner une fréquence constante.

Remplaçons dans un des cryptogrammes les groupes dont nous croyons connaître l'équivalence, en prenant la représentation la plus faible dans l'échelle des nombres par exemple. On aura :

64 31 52 31 19 52 57 39 20 50 64 59 31 17 64 13 64 10 39
20 59 50 15 39 22 20 31 17 39 16 22 64 20 52.....

Le groupe le plus fréquent est 64, qui vient dix-sept fois sur 106 lettres. La fréquence est un peu faible pour E. En substituant on a :

E. . . . . E . . . E . E . . etc.

Comme nous ne voulons pas nous appesantir sur cet exemple, nous admettrons que l'adresse donne au décrypteur l'idée d'employer ces 3 E au mot septième. Reportant les valeurs de lettres ainsi obtenues, nous aurons.

64 31 52 31 19 52 57 39 20 50 64 59 31 17 64 13 64 10 39 20
E T T S E P T I E M E

59 50 15 39 22 10 31 17 39 16 22 64 20 52
P T I E

On devine, avec les répétitions de 52 pour le confirmer, le mot ÉTAT MAJOR, et puisque 19 donne M, c'est qu'il a la même valeur que 13 qui a donné M de septième. De même en reportant les nouvelles lettres découvertes, on voit se dessiner le mot FONCTIONNERA, et de ce décryptement on déduit que n est représenté par 22 et 64.

On pourra donc arriver à retrouver la valeur des deux groupes attribués à chaque lettre, et avoir un tableau de ce genre.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
52	21	10	37	64	?	?	14	17	57	58	11	13	16	39	59
61	69	30	92	66	?	?	35	23	62	?	32	19	22	53	68

Q	R	S	T	U	V	X	Y	Z
?	20	50	31	55	12	?	24	?
?	34	60	38	56	33	?	?	?

permettant de traduire les deux textes :

1° État-major septième corps fonctionnera Villers-Cotterets à partir 7 heures. K. État major huitième corps à Coucy 9 heures;

2° État major septième corps ira Vauciennes pour 7h 1/2 au lieu Villers-Cotterets pour 7 heures.

Il y a des lettres pour lesquelles on n'a trouvé qu'une représentation, ou même pas du tout.

Si, le lendemain par exemple, l'ennemi change la position de la bande mobile, et qu'on ait assez de télégrammes ou des télégrammes avantageux pour trouver des équivalences, on arrivera à décrypter encore la correspondance, et on aura un nouveau tableau.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
11	16	50	39	23	10	21	?	64	?	?	24	14	52	31	24
32	22	60	53	71	30	?	?	66	?	?	54	35	61	38	54

Q	R	S	T	U	V	X	Y	Z
?	20	17	59	55	12	20	?	33
?	34	23	68	56	33	?	?	?

Par comparaison avec le premier tableau, on pourra compléter les groupes de chiffres qui vont par deux, et écrire 34 sous 20 par exemple.

On aura ainsi le moyen de traduire les télégrammes, ramenés à une substitution à représentation unique, mais en recommençant pour chaque position de la bande un travail fastidieux, et parfois hérissé de difficultés. Un problème se pose alors : reconstituer un ensemble qui donne les mêmes résultats que l'appareil, c'est-à-dire où, par un simple déplacement de la bande portant l'alphabet dans un ordre reconstitué convenable, entre les deux séries de chiffres rangés dans un ordre convenable, on passe d'un déchiffrement à l'autre. Pour cela il faut ranger lettres et chiffres suivant une loi telle que lorsque la lettre A se déplace de 52 à 11, la lettre B se déplace de 21 à 16, etc... c'est-à-dire que l'intervalle de 52 à 11 dans la série des nombres écrits sur l'appareil soit égal à l'inter-

valle de 21 à 16 etc., On trouvera au chapitre 9 la solution de ce problème.

Ayant alors reconstitué un appareil jouissant des mêmes propriétés que celui de l'ennemi; c'est-à-dire tel que pour une position de la lettre A en face d'un certain groupe quelconque, toutes les lettres se trouvent en face du groupe qui les représente, on pourra, même avec des matériaux insuffisants pour retrouver un tableau analogue à ceux qui précèdent, lire les télégrammes. Un diagramme de fréquences établi sur les lettres de la bande suivant leur ordre, et comparé à un diagramme établi sur les chiffres du cryptogramme suivant l'ordre parallèle des nombres écrits sur l'appareil permettra, en faisant coïncider par déplacement de la bande les maxima et minima des deux diagrammes, de trouver immédiatement la position de la bande.

De tels appareils ont été employés. On changeait la position de la bande fréquemment, mais on en distinguait la position en plaçant en tête du texte l'indication d'un des deux groupes placés en face d'une lettre, comme A 11, ou I 66; etc., ce qui permettait, avec un grand nombre de textes, de grouper ceux qui avaient même indicatif, et donnait un renseignement qui, combiné avec les similitudes de fréquences, facilitait le classement par cryptogrammes de même clef.

Un procédé du même genre est décrit dans le traité de cryptographie de Carmona (Madrid 1894). L'appareil comprend une bande sur laquelle est écrit l'alphabet incohérent, se déplaçant devant un tableau où une même colonne, correspondant à une lettre dans chaque position de la bande, contient plusieurs représentations. Le problème, un peu plus compliqué par la multiplicité des représentations, se traiterait de la même manière.

Enfin, l'appareil que nous avons étudié, à deux représentations, et que Carmona attribue, d'après Fleissner, à des cryptologues autrichiens, a été employé encore autrement à notre connaissance. Partant d'une position donnée de la bande, on chiffrait une série de lettres, 10 par exemple, puis on déplaçait la bande d'un intervalle de lettres pour

chiffrer les 10 lettres suivantes, etc... Autrement encore, on indiquait après un nombre de lettres quelconque un changement de position de la bande au moyen d'une lettre rare, on donnait comme repère la nouvelle position de cette lettre rare ou de l'A, et on chiffrait une autre tranche de longueur différente de la première. On obtient ainsi des cryptogrammes très bien défendus contre les indiscrets, mais ce n'est plus à proprement parler de la substitution simple, puisqu'au cours du même document un groupe donné du cryptogramme a des significations différentes. En réduisant les tranches successives à une lettre, on a un type classique de substitution à double clef, système dont l'étude va faire l'objet du chapitre suivant.

Avant de clore la question des substitutions multiples, nous signalerons celles qui sont faites avec le réservoir presque inépuisable que constitue un ouvrage imprimé. On peut, en convenant d'employer un certain ouvrage, à une page convenue d'avance ou indiquée en tête du cryptogramme, remplacer chaque lettre de l'alphabet par l'indication d'une ligne et de la place où figure cette lettre dans la ligne et changer les éléments de position de la lettre imprimée à chaque nouvelle représentation. On reconnaît souvent ce procédé à l'aspect des cryptogrammes formés par groupes de deux nombres. En théorie, comme il n'y a pas de répétitions, un tel procédé est absolument sûr, mais les lettres y sont représentées par des groupes de trois ou quatre caractères, ce qui est encombrant. En pratique, avec la paresse des chiffreurs qui laissaient passer des répétitions, ne séparaient pas les lettres des conjonctions, des articles, etc... si bien que l'on reconnaissait ces mots courts à la présence de deux lettres voisines sur la même ligne, et avec des textes assez nombreux, nous avons vu réussir des décryptements de cryptogrammes de cette nature.

CHAPITRE IV

SUBSTITUTIONS A DOUBLE CLEF
MÉTHODE DE VIGENÈRE ET ANALOGUES

Généralités.

Nous avons fait allusion à la fin du chapitre précédent à des changements de tableau de concordance au cours d'un même cryptogramme. De pareils systèmes exigent la connaissance de la part du déchiffreur de deux conventions : 1°) la formation des tableaux de concordance; 2°) l'ordre dans lequel on les emploie. Ces conventions entre chiffreur et déchiffreur, avons-nous dit, constituent les clefs des systèmes. Nous aurons donc affaire alors à des systèmes exigeant deux clefs : on les appelle substitutions à double clef. Comme nous le verrons dans la suite de cette étude, les systèmes à double clef sont faciles à inventer, et la diversité en est grande. Un certain nombre d'entre eux sont classiques, et ont donné lieu à des travaux intéressants. Nous en parlerons d'abord, non pas tant parce qu'on les rencontre fréquemment à notre époque, que parce qu'il nous semble indispensable d'en connaître parfaitement le décryptement pour aborder les systèmes plus compliqués qui s'y rattachent.

Nous ferons la première étude sur des systèmes alphabétiques. Supposons qu'au lieu de nous servir d'un même tableau de concordance entre l'alphabet du clair et celui du cryptogramme, ce qui nous donnerait une substitution simple, nous ayons plusieurs tableaux de concordance différents, et que nous les employions successivement en changeant de tableau à chaque lettre du clair. La lettre E

du clair, par exemple, sera représentée par une lettre différente dans chacun de ces tableaux. Inversement, une lettre quelconque m du cryptogramme correspondra suivant le tableau à différentes lettres du clair. Ainsi, tandis que dans la substitution simple proprement dite, une lettre du clair était représentée toujours par un même caractère du cryptogramme, lequel représentait toujours cette même lettre — que dans la substitution simple à représentations multiples, une lettre du clair avait différentes représentations dans le cryptogramme, chacune de ces dernières par contre représentant uniquement et toujours cette lettre, nous aurons, dans la substitution à double clef, des représentations différentes pour une lettre du clair suivant la place qu'elle occupe dans le cryptogramme, et une lettre du cryptogramme pourra représenter successivement différentes lettres du clair.

Pour nous faire comprendre, prenons un exemple simple : supposons que nous ayons trois tableaux de concordance, comprenant, en face de l'alphabet clair normal, comme alphabets de substitutions, trois alphabets régulièrement ordonnés, décalés par rapport à l'alphabet normal de 1, 2 ou 3 lettres, si bien que ces tableaux (que nous désignerons souvent à l'avenir par l'alphabet de substitution qui y figure, et que nous appellerons par exemple alphabet 2 ou alphabet c) seront :

Tableau 1	*Tableau 2*	*Tableau 3*
A — b	A — c	A — d
B — c	B — d	B — e
C — d	C — e	C — f
etc.	etc.	etc.

Nous conviendrons d'employer successivement ces tableaux dans l'ordre 1, 2 et 3.

Le mot ENNEMI sera chiffré fpqfol.

Tableau de Vigenère.

	A	B	C	D	E	F	G	H	I	J	K	L	M
A	a	b	c	d	e	f	g	h	i	j	k	l	m
B	b	c	d	e	f	g	h	i	j	k	l	m	n
C	c	d	e	f	g	h	i	j	k	l	m	n	o
D	d	e	f	g	h	i	j	k	l	m	n	o	p
E	e	f	g	h	i	j	k	l	m	n	o	p	q
F	f	g	h	i	j	k	l	m	n	o	p	q	r
G	g	h	i	j	k	l	m	n	o	p	q	r	s
H	h	i	j	k	l	m	n	o	p	q	r	s	t
I	i	j	k	l	m	n	o	p	q	r	s	t	u
J	j	k	l	m	n	o	p	q	r	s	t	u	v
K	k	l	m	n	o	p	q	r	s	t	u	v	w
L	l	m	n	o	p	q	r	s	t	u	v	w	x
M	m	n	o	p	q	r	s	t	u	v	w	x	y
N	n	o	p	q	r	s	t	u	v	w	x	y	z
O	o	p	q	r	s	t	u	v	w	x	y	z	a
P	p	q	r	s	t	u	v	w	x	y	z	a	b
Q	q	r	s	t	u	v	w	x	y	z	a	b	c
R	r	s	t	u	v	w	x	y	z	a	b	c	d
S	s	t	u	v	w	x	y	z	a	b	c	d	e
T	t	u	v	w	x	y	z	a	b	c	d	e	f
U	u	v	w	x	y	z	a	b	c	d	e	f	g
V	v	w	x	y	z	a	b	c	d	e	f	g	h
W	w	x	y	z	a	b	c	d	e	f	g	h	i
X	x	y	z	a	b	c	d	e	f	g	h	i	j
Y	y	z	a	b	c	d	e	f	g	h	i	j	k
Z	z	a	b	c	d	e	f	g	h	i	j	k	l

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
n	o	p	q	r	s	t	u	v	w	x	y	z
o	p	q	r	s	t	u	v	w	x	y	z	a
p	q	r	s	t	u	v	w	x	y	z	a	b
q	r	s	t	u	v	w	x	y	z	a	b	c
r	s	t	u	v	w	x	y	z	a	b	c	d
s	t	u	v	w	x	y	z	a	b	c	d	e
t	u	v	w	x	y	z	a	b	c	d	e	f
u	v	w	x	y	z	a	b	c	d	e	f	g
v	w	x	y	z	a	b	c	d	e	f	g	h
w	x	y	z	a	b	c	d	e	f	g	h	i
x	y	z	a	b	c	d	e	f	g	h	i	j
y	z	a	b	c	d	e	f	g	h	i	j	k
z	a	b	c	d	e	f	g	h	i	j	k	l
a	b	c	d	e	f	g	h	i	j	k	l	m
b	c	d	e	f	g	h	i	j	k	l	m	n
c	d	e	f	g	h	i	j	k	l	m	n	o
d	e	f	g	h	i	j	k	l	m	n	o	p
e	f	g	h	i	j	k	l	m	n	o	p	q
f	g	h	i	j	k	l	m	n	o	p	q	r
g	h	i	j	k	l	m	n	o	p	q	r	s
h	i	j	k	l	m	n	o	p	q	r	s	t
i	j	k	l	m	n	o	p	q	r	s	t	u
j	k	l	m	n	o	p	q	r	s	t	u	v
k	l	m	n	o	p	q	r	s	t	u	v	w
l	m	n	o	p	q	r	s	t	u	v	w	x
m	n	o	p	q	r	s	t	u	v	w	x	y

Substitutions à double clef avec emploi d'alphabets normaux.

Vigenère. — Dans les systèmes classiques que nous allons examiner d'abord, on emploie des alphabets normalement ordonnés. Afin d'éviter de préparer pour chaque cryptogramme les tableaux de concordance dont on veut se servir, et dont la découverte sur une feuille de papier égarée faciliterait la besogne du décrypteur en restreignant les recherches aux alphabets qui y figurent, on fait emploi de ce qu'on appelle en France « Tableau carré de Vigenère », du nom du cryptologue français du XVII^e^ siècle que certains auteurs considèrent comme l'inventeur d'un système longtemps regardé comme très difficilement déchiffrable, tandis que d'autres en font remonter la paternité à Trithème. Nous n'insisterons pas sur les questions d'invention en cryptographie : le secret qui entoure ordinairement les manifestations pratiques de cette science est tout à fait favorable aux compétitions d'auteurs. Le tableau de Vigenère est figuré ci-contre.

Comme on le voit, il se compose d'autant d'alphabets parallèles normalement ordonnés qu'il y a de lettres dans l'alphabet, chacun décalé d'une lettre par rapport à celui qui le précède. On peut faire des tableaux à 25 ou à 24 lettres, en supprimant le w et une autre lettre, j ou k.

Pour utiliser ce tableau, nous conviendrons de désigner chacun des alphabets par sa première lettre, celle qui dans le tableau de concordance correspondrait à A du clair. Si nous avons à chiffrer ENNEMI en nous servant des alphabets B C K L successivement nous trouverons sur la ligne de E dans l'alphabet B (colonne ayant comme première lettre B) la première lettre f, sur la ligne de N dans l'alphabet C la deuxième lettre p, sur la même ligne dans l'alphabet K la troisième lettre x, sur la ligne E alphabet L la quatrième lettre p, puis nous reprendrons l'alphabet B pour y trouver sur la ligne de l'M la cinquième

lettre n, et l'alphabet C pour y trouver k sur la ligne de l'I. Nous aurons alors fpxpnk.

On donne comme clef unique, le tableau étant connu et par suite aucune clef n'étant nécessaire pour former les alphabets, la suite des lettres qui indiquent les alphabets à prendre, en plaçant ces lettres dans l'ordre où l'on doit employer les alphabets, ici : BCKL. Généralement, pour qu'il soit facile de retenir cette clef, on donne un mot ou une phrase dans une langue connue. On dit alors que la clef est *claire*. Quand la clef comprend une série de lettres sans aucun sens, elle est dite *incohérente*.

Cryptogrammes à clef courte. — Dans l'étude de déchiffrement que nous allons faire, nous supposerons que la clef est courte, c'est-à-dire qu'elle contient beaucoup moins de lettres que le cryptogramme, ce qui entraîne la conséquence suivante : Quand on a employé les alphabets correspondant à une longueur de la clef, on recommence à prendre l'alphabet qu'on avait employé pour chiffrer la première lettre, et ainsi de suite. Si donc la clef a n lettres, les lettres numéro $1, n+1, 2n+1, 3n+1$, etc., du texte sont chiffrés avec le même alphabet, les lettres 2, $n+2$, $2n+2$, etc., avec un même alphabet, etc. Avec une clef courte, le nombre n étant petit, le même alphabet sert à chiffrer beaucoup de lettres qui dans le clair se trouvent à des intervalles égaux. C'est sur cette hypothèse, que la clef est courte, très souvent conforme à la réalité, que repose la méthode de décryptement que nous allons exposer, et dont, croyons-nous, la première présentation a été faite par M. Kerckhoffs, reprenant et développant une remarque de Kasiski (dont l'ouvrage, en allemand, date de 1863).

Soit à chiffrer la phrase :

Quelles que soient les questions que puisse soulever l'étude faite ci-après...

avec la clef Lyon.

Pour faire pratiquement un chiffrement, on a l'habitude de couper le texte en tranches de n lettres, n étant la longueur de la clef, d'écrire la clef au-dessus de chaque

tranche, puis, marquant dans le tableau de Vigenère, par exemple avec une règle, le premier (puis le deuxième, etc.) alphabet à employer, de chiffrer d'abord toutes les lettres à chiffrer avec cet alphabet c'est-à-dire la première, la $n + 1$, la $2n + 1$, etc... au lieu de prendre les lettres dans l'ordre du texte pour les chiffrer une à une en changeant chaque fois d'alphabet. On gagne ainsi du temps et on évite des erreurs.

En opérant ainsi, nous avons :

Lyon	lyon	lyon	lyon	lyon	lyon	lyon	lyon
QUEL	LESQ	UESO	IENT	LESQ	UEST	IONS	QUEP
b s s y	w c g d	f c g b	t c b g	w c g d	f c g g	t m b f	b s s c
lyon	lyon	lyon	lyon	lyon	lyon	lyon	lyo
UISS	ESOU	LEVE	RLET	UDEF	AITE	CIAP	RES
f g g f	p q c h	w c j r	c j s g	f b s s	l g h r	n g o c	c c g.

Nous ferons quelques remarques sur le texte clair et le cryptogramme correspondant.

D'abord, les redoublements de lettres du clair ne correspondent en rien à ceux du cryptogramme, contrairement à ce qui se passe dans les substitutions simples, et nous trouverons des lettres triplement redoublées. On pourrait tout aussi bien trouver cinq ou six fois de suite la même lettre; de pareilles séquences écartent l'hypothèse d'une substitution simple (sous réserve de nulles introduites à dessein).

Considérons ensuite les 4 trigrammes QUE du clair. Le 1er et le 4e sont semblablement placés par rapport à la clef, et sont chiffrés avec les mêmes alphabets; la même lettre est transformée par le même alphabet; ils sont alors chiffrés par un même trigramme bss. Le 2e et le 3e sont, entre eux, semblablement placés par rapport à la clef, mais différemment des deux autres, ils sont tous deux chiffrés par dfc. On en conclut : *Lorsque deux polygrammes semblables sont semblablement placés par rapport à la clef, ils donnent dans le cryptogramme des polygrammes semblables.* La réciproque d'ailleurs n'est pas vraie, car :

1° le hasard des clefs peut donner des polygrammes semblables dans le cryptogramme avec des polygrammes du clair différents, pourvu qu'ils soient différemment placés par rapport à la clef (Voir bss correspondant à DEF de ÉTUDE FAITE), et 2° la clef peut présenter une répétition partielle qui ramène les mêmes alphabets sans qu'ils soient semblablement placés par rapport à la clef (Exemple : Clef : Marceau-Marseille; texte : quelles que soient. Les deux trigrammes QUE seront chiffrés avec les mêmes alphabets MAR, et donneront dans le cryptogramme les mêmes trigrammes. Ils ne seront pourtant pas semblablement placés par rapport à la clef).

Malgré ces exceptions, on peut dans la grande majorité des cas faire l'hypothèse suivante : Deux polygrammes analogues du cryptogramme proviennent de deux polygrammes semblables du clair, *semblablement placés par rapport à la clef*, et par suite le nombre de lettres qui séparent l'une de l'autre les premières lettres de ces polygrammes est un multiple du nombre de lettres de la clef, car ce nombre correspond à un nombre exact de répétitions de la clef.

Dans notre exemple, les intervalles qui séparent les polygrammes répétés sont :

heptagramme :	wcgdfcg	12 lettres :	3×2^2
trigramme :	bss	28 lettres :	7×2^2
—	bss	21 lettres :	7×3^2
bigramme :	wc	24 lettres :	$3 \times 2 \times 2^2$
	cj	3 lettres :	
	gg	11 lettres :	

On tient toujours plus de compte des répétitions longues que des bigrammes, que le hasard peut facilement former. Le facteur le plus fréquent du nombre de lettres des intervalles est 2^2, c'est-à-dire 4, longueur de notre clef.

Notons que nous pourrions avoir une hésitation devant la fréquence du facteur 3. Quand le texte est long, les facteurs dus à des intervalles provenant de répétitions fortuites sont en général facilement éliminés devant la fré-

quence des facteurs provenant réellement de répétitions de polygrammes semblablement placés. Mais si plusieurs solutions semblent possibles, il faut les essayer successivement.

Si la clef a 4 lettres, les 1re, 5e, 9e, etc... lettres du document ont été chiffrées avec un même alphabet, et on peut les traiter, en les considérant à part de tout le reste du cryptogramme, comme les éléments d'une substitution simple, où la lettre plus fréquente est E. De même les 2e, 6e, 10e lettres donneront lieu à une étude analogue, etc.

Comme conclusion pratique, lorsqu'un cryptogramme ne donne comme fréquences de ses lettres rien qui puisse permettre de conclure à une substitution simple (c'est-à-dire que la lettre la plus fréquente ne figure pas avec un pourcentage voisin de 17, que d'autres lettres ne correspondent pas sensiblement par leurs fréquences de 6 % à SARIN, et qu'aucune lettre n'est très rare), on peut soupçonner une substitution à double clef. On cherchera alors les répétitions de polygrammes, on déterminera le nombre de lettres qui séparent chacune de ces répétitions de la suivante, et on cherchera si ces nombres ont un diviseur commun, qui serait la longueur de la clef ou un multiple de cette longueur. Une fois cette longueur admise, on écrit le cryptogramme par tranches de cette longueur, les unes sous les autres, de manière que, la clef ayant n lettres, la 1re lettre du cryptogramme, la $n + 1$re, la $2n + 1$re, etc... se trouvent sur une même colonne, et on cherche les fréquences des lettres d'une même colonne. Si l'on peut déterminer l'E d'un des alphabets, comme cet alphabet est normalement ordonné, on retrouve la traduction de toutes les lettres de la colonne, et la lettre qui correspond à l'A du clair donne une lettre de la clef. Si l'on ne peut déterminer l'E pour une des colonnes, il est rare que le contexte des colonnes trouvées, et celui de la clef, qu'il ne faut pas oublier, ne donnent pas des lettres des colonnes dont il s'agit (si la clef est claire, c'est souvent la clef qui donnera la solution dès qu'on en aura les premières lettres parce qu'on pourra deviner les suivantes. Si c'est une clef incohérente, elle ne servira à rien). D'ailleurs la considération des graphiques de fréquence dans chaque colonne sera

avantageuse pour déterminer la position de l'alphabet, même si E n'est pas la lettre la plus fréquente.

Nous n'insisterons pas sur cette méthode; elle est expliquée en détail dans Kerckhoffs et dans Valerio, pour ne citer que ceux-là, car les substitutions à double clef ont donné lieu dans le dernier quart du XIX^e siècle à des travaux remarquables. Il faut la connaître, car elle est la base des études qui vont suivre. L'auteur doit d'ailleurs dire qu'en une carrière déjà longue, il ne se souvient pas d'avoir vu de substitution de la méthode classique de Vigenère, en dehors des exercices qu'il a faits pendant ses études et des « inventions » qui lui ont été soumises par des cryptologues pleins de bonne volonté mais dénués d'érudition.

Décryptement par emploi du mot probable. — Nous avons exposé ici la méthode analytique. La méthode du mot probable s'applique également. Toute une école, à la suite de Bazeries, pour laquelle la qualité maîtresse du décrypteur est l'esprit intuitif, prétend même que cette méthode est la plus générale et réussit presque toujours. Nous verrons, de fait, que dans les complications des systèmes à double clef, c'est à elle qu'il faut souvent recourir. Il importe donc de bien savoir l'appliquer. Dans les cryptogrammes type Vigenère, quand on y soupçonnera l'existence d'un mot, on cherchera à remonter du cryptogramme à ce mot, et on étudiera la suite des alphabets qui auraient donné le chiffrement. Si ces alphabets présentent une périodicité, on admettra que la clef (qui correspond à cette périodicité) est trouvée, et on étendra la traduction en essayant cette clef en dehors du mot probable.

Soit le cryptogramme :

AAUQN XSZWF EAIBA..

où nous soupçonnons le mot : division

Supposons que ce mot soit en tête. Le 1^er A du cryptogramme représenterait alors la lettre d. Or si, dans le tableau de Vigenère, nous cherchons l'alphabet qui donne A pour représenter d, c'est-à-dire si nous suivons la ligne

de D jusqu'A et voyons quelle est la 1re lettre de la colonne, nous trouverons que c'est l'alphabet X. X serait alors le 1re lettre de la clef. Si AAUQNXSZ représentait DIVISION, la clef serait : XIZIVPEM. Ce résultat ne nous donne aucun élément pour la solution du problème. Essayons sur la lettre suivante d'un rang vers la droite. Pour que AUQNXSZW représente DIVISION la clef doit être XMVFFKLJ.; encore rien. Décalons notre essai d'un rang encore. UQNXSZWF donnera DIVISION avec la clef RISPARIS. Cette fois nous avons une périodicité; en continuant l'essai de la clef, EAIBA avec la clef PARIS donne au déchiffrement : PARTI. La clef est donc bonne.

(Pour déchiffrer un cryptogramme avec le tableau de Vigenère, on considère la lettre de la clef, on descend la colonne jusqu'à ce qu'on trouve la lettre du cryptogramme à traduire avec cette clef, et on suit la ligne jusqu'à la gauche du tableau; la lettre de la ligne dans la colonne A est la traduction. Comme pour chiffrer, il est bon de couper le texte en tranches de longueur égale à celle de la clef et d'écrire cette dernière au-dessus de ces tranches.)

Nous avons ici une clef particulièrement nette parce qu'elle est claire, mais une clef incohérente se trahirait par la répétition d'une suite de lettres dans le même ordre. Toutefois la méthode ne réussit que si le mot probable est plus long que la clef, sinon les répétitions de celle-ci n'apparaissent pas.

Cryptogrammes à clefs longues. — Qu'on emploie la méthode analytique ou celle du mot probable, on voit donc que les clefs longues gênent le décrypteur. Dans la méthode analytique, avec une clef longue on aura moins de répétitions de la clef, donc moins de chances d'avoir des répétitions de polygrammes semblablement placés, moins d'éléments pour chaque alphabet qui comprend une série analogue aux 1re, n + 1e, 2 n + 1e... lettres, puisque n est plus grand, et plus de difficultés pour rétablir les alphabets et même pour déterminer la longueur de la clef. Avec un seul cryptogramme, les difficultés pourront être considérables, surtout si le cryptogramme est court.

Si l'on a plusieurs cryptogrammes faits avec la même clef, on pourra négliger la recherche de la longueur de la clef. En effet (à moins que le chiffreur ne mette des lettres nulles en tête de ses cryptogrammes après avoir chiffré) les premières lettres de tous ces cryptogrammes sont chiffrés avec la 1re de la clef, donc avec le même alphabet, et, en écrivant ces cryptogrammes les uns sous les autres, nous pourrons traiter la 1re colonne du tableau ainsi obtenu comme nous avons traité la 1re colonne de notre cryptogramme type coupé en tranches écrites les unes sous les autres. La colonne des 2es lettres sera traitée de la même manière, et ainsi de suite. La clef sera donnée par le déchiffrement lui-même.

Recherche de lettres-origines autres que E. — La difficulté que l'on peut alors rencontrer, c'est de ne pas trouver, faute d'éléments assez nombreux, et même en employant les graphiques, les E des différentes colonnes. On peut alors avoir recours à un procédé suivant. Comme plusieurs autres qu'on trouvera dans la suite, il a été exposé par le commandant Bassières, membre de la Commission de cryptographie militaire. Nous l'indiquerons, ainsi que d'autres travaux de ce distingué cryptologue, comme méthode ingénieuse, qu'on n'a sans doute pas souvent l'occasion d'appliquer, mais qui fait parfaitement connaître les particularités des systèmes à double clef et peut servir dans l'étude de procédés compliqués relevant de cette classe de cryptogrammes.

Soient les débuts de cryptogrammes chiffrés avec la même clef et avec un tableau de Vigenère :

1°	X	Q	Y	B	Y
2°	N	Q	I	T	I
3°	X	W	C	A	W
4°	N	Q	W	P	R
5°	Z	V	G	Z	E
6°	Z	V	Y	P	Q

Nous chercherons si dans la 1re colonne se trouvent deux lettres que nous fixerons arbitrairement, E et S par

exemple. Établissons le tableau de correspondance suivant, composé de deux alphabets normalement ordonnés, E de l'un correspondant à S de l'autre; nous les appellerons (e) et (s).

(e) A B C D E F G H I J K L M N O P Q
(s) O P Q R S T U V W X Y Z A B C D E

(e) R S T U V W X Y Z
(s) F G H I J K L M N

Les deux lettres d'une colonne quelconque de ce tableau ont entre elles le même intervalle que E et S dans l'alphabet normal. Si l'une des lettres de (e) représente le chiffrement de E dans un alphabet du tableau de Vigenère, la lettre correspondante de (s) représentera le chiffrement de S dans le même alphabet. Examinons, dans notre tableau des débuts des 6 documents, la 1re colonne : elle renferme les lettres X, N, Z. A X dans l'alphabet (s), correspond dans l'alphabet (e) J, qui n'est pas une de ces lettres. A N correspond Z, qui s'y trouve. Si Z représente E, N peut représenter S, dans le même alphabet, l'alphabet V du tableau de Vigenère où X correspond à C, et les premières lettres de nos cryptogrammes seront, dans l'ordre des documents numérotés de 1 à 6 :

C, S, C, S, E, E

chiffrées avec l'alphabet V. La 1re lettre de la clef serait V.

Faisons le même essai pour la 2e colonne. Elle comprend les lettres QWV. Q correspond à C, qui n'est pas dans la colonne; W à I, V à H qui n'y sont pas non plus. La colonne ne semble donc pas contenir à la fois E et S. Cherchons si elle ne contient pas un autre couple de lettres, I et N par exemple :

A B C D E F G H I J K L M N O P Q
F G H I J K L M N O P Q R S T U V

R S T U V W X Y Z
W X Y Z A B C D E

Dans les alphabets décalés de manière que N coïncide avec I, Q donne L, que nous n'avons pas, W donne R que nous n'avons pas, mais V donne Q que nous avons. Si donc Q représente I, V représentera N; cela correspond à l'alphabet I, la suite de nos 2es lettres sera I, I, O, I, N, N, et, en rapprochant cette 2e colonne de la 1re, nous aurons pour le début de la clef VI, et pour les débuts des textes les bigrammes

CI SI CO SI EN EN

tout à fait acceptables en français.

La 3e colonne comprend les lettres YICWG.

Nous vérifierons facilement qu'elle ne contient ni le couple ES, ni le couple IN. Cherchons si elle ne contient pas le couple NR.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

R	S	T	U	V	W	X	Y	Z
V	W	X	Y	Z	A	B	C	D

Nous avons dans la colonne Y, I, W qui ne nous donnent pas de correspondance avec une autre lettre de la colonne, mais C correspond à Y qui se trouve dans la colonne, et G correspond à C qui s'y trouve aussi. Quelle correspondance choisir? Essayons-les successivement, en juxtaposant le résultat des essais à la partie des cryptogrammes déjà traduite.

G correspond à R et C correspond à N en clef P, qui donne Y = J, I = T, W = H. On aurait pour la clef VIP.. et pour les documents les trigrammes écrits ci-dessous à gauche. Avec la correspondance C pour R, Y pour N, en clef L (ce qui donne VIL), on aurait I = X, W = L, G = V et les trigrammes de droite :

Clef VIP	*Clef VIL*
C I J	C I N
S I T	S I X
C O N	C O R
S I H	S I L
E N R	E N V
E N J	E N N

En examinant ces trigrammes, la série de la clef VIL paraît plus plaisante que celle de la clef VIP (CIJ, ENJ), et on pourrait rejeter cette dernière. Néanmoins, pour montrer comment se déroule une semblable étude, nous laisserons subsister l'indécision. Nous passerons à la colonne suivante. Des essais faits sur les lettres qu'elle contient BTAPZ nous montreront qu'elle ne contient ni le couple ES, ni le couple IN, ni le couple NR. Nous y trouvons le couple EI, avec les correspondances en clef L, T = I, P = E, B = Q, A = P, Z = O. Juxtaposons ces résultats aux deux séries de trigrammes; nous avons :

Clef VIPL	*Clef VILL*
C I J Q	C I N Q
S I T I	S I X I
C O N P	C O R P
S I H E	S I L E
E N R O	E N V O
E N J E	E N N E

Les quadrigrammes de la clef VIPL sont à rejeter (CIJQ, CONP). La clef est donc VILL.

Nous arrêterons là le développement de cet exemple.

Cryptogrammes très courts. — Pour montrer encore un exemple de procédés qui peuvent développer l'ingéniosité des personnes ferventes d'études cryptologiques, nous résumerons une autre communication du même auteur sur le décryptement de quelques cryptogrammes très

courts. Nous supposons toujours que nous travaillons sur des substitutions faites avec le tableau de Vigenère.

Soient les textes :

1°	KAUVJ	VGVBI	GINAL	R
2°	QRHWT	ECZPU	V	
3°	WEQIA	EQLBT	G	
4°	HAUHF	ZYSTF	OCOCV	

Nous allons chercher la clef par un procédé mécanique pour ainsi dire, par essais successifs.

Cherchons si la première lettre de la clef est A.

Si c'est A, les premières lettres des textes clairs seront K, Q, W et H, n'ayant point été changées par le chiffrement.

A la 2e lettre de la clef correspondra l'alphabet qui aura donné les 2es lettres des textes, A R E A. Si cette deuxième lettre de la clef est A, les 2es lettres des clairs sont A R E A; si elle est B, les 2es lettres du clair sont (voir Tableau de Vigenère, lettres correspondant dans la clef B aux lignes sur lesquelles figurent A, R et E) Z, Q, D, Z. Formons un tableau donnant pour chaque clef possible les correspondances avec les 2es lettres des cryptogrammes, c'est-à-dire les 2es lettres du clair. Nous supposons, avons-nous dit, que les 1res lettres du clair sont K, Q, W, H.

Clef A.

	a	b	c	d	e	f	g	h	i	j	k	l	m
K	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
Q	R	Q	P	O	N	M	L	K	J	I	H	G	F
W	E	D	C	B	A	Z	Y	X	W	V	U	T	S
H	A	Z	Y	X	W	V	U	T	S	R	Q	P	O

n	o	p	q	r	s	t	u	v	w	x	y	z
N	M	L	K	J	I	H	G	F	E	D	C	B
E	D	C	B	A	Z	Y	X	W	V	U	T	S
R	Q	P	O	N	M	L	K	J	I	H	G	F
N	M	L	K	J	I	H	G	F	E	D	C	B

Si un texte clair commence par Q, la 2e lettre est U. C'est donc la clef X qui devrait donner la 2e lettre des cryptogrammes. Mais les débuts de nos textes seraient KD, QU, WH, HD. Sur ces 4 bigrammes, 3 sont impossibles en tête d'un texte français : Q n'est pas admissible comme 1re lettre d'un de nos documents, la 1re lettre de la clef n'est pas A.

Essayons B.

Si les premières lettres ont été chiffrées avec la clef B et ont donné K Q W H, les premières lettres du clair étaient J P V G. Formons un tableau analogue au précédent, pour chercher la 2e lettre de la clef.

Clef B.

	a	b	c	d	e	f	g	h	i	j	k	l	m
J	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
P	R		P				L						F
V	E		C				Y						S
G	A		Y				U						O

	n	o	p	q	r	s	t	u	v	w	x	y	z
	N	M	L	K	J	I	H	G	F	E	D	C	B
						Z				V			
						M				I			
						I				E			

Au commencement d'une phrase J ne peut être suivi que d'une voyelle — toutes les clefs qui ne correspondent pas à A E I O U Y sont donc à rejeter et nous n'avons pas figuré dans le tableau les lettres correspondantes. Les bigrammes PP, PF, PZ, PV ne peuvent commencer une phrase.

Restent les 2 solutions :

Clef BA	*Clef BG*
JA	JU
PR	PL
VE	VY
GA	GU

Si nous étions sûrs que la clef est claire, nous rejetterions la 2e solution, mais dans le doute nous hésitons entre les deux qui peuvent être acceptables si VY était le début d'un nom propre. On aurait alors à passer à la 3e lettre de la clef en faisant des essais d'abord sur la clef BA..., puis sur la clef BG... Mais, dans des cas de cette nature, on peut orienter les recherches au moyen du procédé suivant : dans le tableau des bigrammes on considère la fréquence de chacun des bigrammes proposés, on fait la somme de ces fréquences pour chacune de ces combinaisons, et il y a de fortes chances, surtout quand on opère sur des bigrammes assez nombreux, pour que le total le plus élevé désigne la combinaison à adopter.

Ici :

JA	=	0	JU	=	0
PR	=	4	PL	=	1
VE	=	9	VY	=	0
GA	=	0	GU	=	0
TOTAL		13	TOTAL		1

Nous adopterons la solution : clef BA...

Cherchons la 3e lettre de la clef. Les 3es lettres de nos textes sont U H Q U.

Clef BA.

	a	b	c	d	e	f	g	h	i	j	k	l	m
JA	U			R				N		L			
PR	H	G	F	E	D	C	B	A	Z	Y	X	W	V
VE	Q			N				J		H			
GA	U			R				N		L			

	n	o	p	q	r	s	t	u	v	w	x	y	z
	H						B						V
	U	T	S	R	Q	P	O	N	M	L	K	J	I
	D						X						R
	H						B						V

PR doit être suivi d'une voyelle, nous ne considérerons donc que les clefs qui donnent des voyelles.

JAH nous fait écarter la clef R, VEJ la clef H, VEH la clef L, restent les clefs D, T, Z, qui donnent trois séries de trigrammes possibles.

Nous allons traiter les bigrammes finaux de ces trigrammes comme les bigrammes du début de nos textes dans l'essai précédent en cherchant la somme des fréquences.

Clef BAD		*Clef BAT*		*Clef BAZ*	
JAR	19	JAB	3	JAV	7
PRE	25	PRO	12	PRI	11
VEN	39	VEX	0	VER	19
GAR	19	GAB	3	GAV	7
TOTAL	92	TOTAL	18	TOTAL	44

Nous adopterons la 1re solution : clef BAD.

Appliquons la même méthode pour les 4es lettres V W I H :

Clef BAD.

	a	b	c	d	e	f	g	h	i	j	k	l	m
JAR	V	U	*T*	*S*	R	*Q*	P	O	N	M	L	K	*J*
PRE	W	V	U	T	S	R	*Q*	P	O	N	M	L	K
VEN	I	*H*	G	F	E	D	C	*B*	A	*Z*	Y	X	*W*
GAR	*H*	G	F	E	D	C	B	A	*Z*	Y	*X*	*W*	V

	n	o	p	q	r	s	t	u	v	w	x	y	z
	I	*H*	G	*F*	E	D	C	*B*	*A*	*Z*	Y	*X*	*W*
	J	I	*H*	G	F	*E*	D	C	B	A	Z	Y	X
	V	U	T	S	*R*	Q	*P*	O	N	M	L	K	J
	U	T	S	R	Q	P	O	N	M	L	K	J	I

Examinant les tétragrammes que forment avec les trigrammes JAR, PRE, VEN, GAR les lettres qui se trouvent sur la même ligne et soulignant dans chaque colonne

la principale de celles qui nous font rejeter cette colonne, nous ne trouvons comme colonne admissible que celle qui correspond à la clef E (en admettant que nos phrases ne commencent pas par des noms propres en JARB, par exemple). On a alors :

Clef BADE.

JARR
PRES
VENE
GARD

on pourrait continuer ainsi. Mais JARR nous donne l'idée d'essayer s'il ne s'agit pas du verbe ARRIVER La 5e lettre du premier cryptogramme est J, qui correspondrait à I dans la clef B. Celle-ci donnerait les pentagrammes PRESS VENEZ GARDE. On continuerait le déchiffrement de proche en proche sur la clef BADE bientôt vérifiée.

Théoriquement, ce système pourrait être employé quand on ne possède que deux dépêches, ou même, si l'on est sûr que la clef est claire, qu'une seule. Mais on a d'autant moins d'hésitations et de tâtonnements que l'on a plus de textes.

Nous avons, au début de l'exposé de ces procédés de décryptement, insisté sur une condition qui en restreint l'emploi, c'est la nécessité de travailler sur des tableaux carrés à alphabets parallèles connus. Les substitutions à double clef s'emploient en effet avec des alphabets quelconques. Avant d'abandonner les tableaux classiques, nous mentionnerons, plutôt pour compléter le bagage cryptographique de nos lecteurs par la connaissance de termes de nomenclature consacrés que pour l'utilité dans leurs travaux, un certain nombre de systèmes décrits et étudiés dans les livres déjà cités.

Nous avons dit que pour chiffrer avec la méthode Vigenère on prend, en descendant le long de la colonne de la

lettre de la clef jusqu'à la ligne de la lettre du texte, la lettre qui se trouve à la rencontre de cette colonne et cette ligne pour chiffrer la lettre du clair.

Beaufort. — Dans la méthode de Beaufort, on emploie le même tableau carré que dans la méthode de Vigenère, mais on descend sur la colonne correspondant à la lettre de la clef jusqu'à ce qu'on rencontre dans cette colonne la lettre du clair, on suit alors la ligne jusqu'à la colonne de l'alphabet normal et on chiffre la lettre du clair avec la lettre de cette ligne (1).

Ainsi, soit le mot ENNEMI à chiffrer avec la clef BADE :

Système Vigenère.	*Système Beaufort.*
B A D E B A	B A D E B A
e n n e m i	e n n e m i
F N Q I N I	D N K A L I

Les procédés que nous avons décrits, en particulier la recherche de la longueur de la clef, la division du cryptogramme en tranches de cette longueur et la recherche des alphabets successifs, aussi bien que le procédé de recherche du mot probable, s'appliquent avec la méthode de Beaufort. Mais, particulièrement pour ce dernier procédé, il y a une remarque à faire. Repassons du cryptogramme DNKALI, chiffré par un système de substitution double que nous ne sommes pas sensés connaître, au clair ENNEMI et cherchons quelle est la clef qu'on a employée. En appliquant la méthode de Beaufort, nous chercherons D, lettre du cryptogramme dans la colonne de gauche, nous suivrons la ligne de D jusqu'à E, lettre du clair, et nous remonterons le long de la colonne qui nous donnera la lettre B de la clef. Mais si, ignorant que c'est un cryptogramme chiffré en Beaufort, nous appliquons la méthode

(1) Remarquons que ces opérations sont celles du *déchiffrement* dans le procédé Vigenère. Chiffrer, en Beaufort, un cryptogramme du type Vigenère, au moyen de sa clef, c'est le déchiffrer.

Vigenère, nous prendrons la ligne de E du clair, nous la suivrons jusqu'à D, lettre du cryptogramme, et nous remonterons le long de la colonne jusqu'à sa 1re ligne; nous trouverons alors Z et pour la clef, au lieu de BADE, nous aurons ZAXW, ce qui nous présentera une clef incohérente et ne nous servira de rien dans nos recherches, tandis qu'on peut deviner une lettre d'une clef claire.

Mais si nous considérons les deux alphabets complémentaires (inversés à l'exception de A) :

A B C D E F G H I J K L M
A Z Y X W V U T S R Q P O

N O P Q R S T U V W X Y Z
N M L K J I H G F E D C B

nous voyons que Z correspond à B, X à D, W à E.

On dit alors que la clef de Beaufort est complémentaire de la clef de Vigenère, et, lorsqu'on trouve pour un système de substitution double une clef incohérente, il est prudent de s'assurer que les lettres complémentaires de celles que l'on a trouvées pour la clef ne donnent pas une clef claire.

Gronsfeld. — La méthode de Gronsfeld consiste à employer une clef numérique, dont les chiffres donnent le décalage, par rapport à l'alphabet normal, de l'alphabet à employer pour la lettre du clair correspondante. Étant donnée la simplicité de cette méthode quand on ne décale que de quelques lettres, elle est assez employée.

Soit la clef : 1034 pour chiffrer ENNEMI

1 0 3 4 1 0
E N N E M I
F N Q I N I

Nous prenons pour E la lettre suivante F, pour le 2e N la 3e lettre à la suite Q, etc... On voit que cela revient absolument à la méthode de Vigenère, et que notre clef

se traduirait en lettres par BADE. Mais il faut remarquer que l'on n'emploie que les décalages de 0 à 9, et que par suite les recherches étant limitées aux 9 lettres suivant une lettre du clair, les alphabets que l'on retrouve un à un ne doivent pas être décalés de plus de 10 lettres l'un par rapport à l'autre.

Cette remarque entraînera un procédé de déchiffrement spécial pour les cryptogrammes genre Gronsfeld. Pour expliquer cette méthode, due au cryptologue déjà cité pour ses remarques ingénieuses sur les systèmes Vigenère, nous supposerons que nous sommes sûrs que l'on n'a pas dépassé 4 dans la clef. Dans le cas général, où les chiffres de la clef peuvent aller jusqu'à 9, le tableau ci-après aurait 10 lignes au lieu de 5, mais on opérerait d'une manière analogue.

Soit le cryptogramme V Q E D W D N L F U D O F V U G...

Écrivons au-dessus de chaque lettre du cryptogramme les 4 lettres qui la précèdent dans l'alphabet normal :

4	R	M	A	Z	S	Z	J	H	B	Q	Z	K	B	R	Q	D
3	S	N	B	A	T	A	K	I	C	R	A	L	C	S	R	E
2	T	O	C	B	U	B	L	J	D	S	B	M	D	T	S	F
1	U	P	D		V	C	M	K	E	T	C	N	E	U	T	G
0	V	Q	E	D	W	D	N	L	F	U	D	O	F	V	U	H

Cherchons dans les premières colonnes à grouper les lettres à raison d'une par colonne de la gauche à la droite pour former des mots français.

Nous voyons par exemple :

S' (ligne 3)
un (lignes 1-2)
une (1-3-0), etc...

S' exigerait comme 2e mot, commençant à la 2e colonne, un verbe commençant par une voyelle. Nous n'avons que la voyelle O et n'en pouvons pas ici former un verbe.

UNE doit être suivi d'un mot féminin commençant à la 4e colonne. Nous voyons à cette colonne le commen-

cement du mot AVANIE (3-1-3-0-3-1), et la clef serait 1 3 0 3 1 3 0 3 1, mais nous ne pouvons aller plus loin. En prenant UN, nous trouvons à partir de la 3e colonne le mot CAVALIER (2 3 1 3 2 3 1 3) et en continuant avec la clef 1 3 2 3 nous formons le mot BLESSÉ, qui nous confirme l'exactitude de cette solution.

CHAPITRE V

RÉGLETTES ET CADRANS

Saint-Cyr. — Nous n'avons pas rencontré très fréquemment, dans la pratique, d'application des systèmes classiques employés sur des tableaux. Mais on en fait un large emploi dans les appareils à chiffrer, en particulier dans ce qu'on appelle la méthode de Saint-Cyr, qui tente toujours les inventeurs et a encore donné lieu à des brevets, heureusement S. G. D. G., peu de temps avant la guerre.

Nous ne considérons pas à vrai dire qu'il y ait une méthode de Saint-Cyr; il y a une application mécanique élégante de la méthode de Vigenère. L'appareil, ou réglette de Saint-Cyr, se compose d'une règle avec un coulisseau. Sur la règle est écrit l'alphabet, généralement répété deux fois à la suite l'une de l'autre; sur le coulisseau est l'alphabet, de manière que lorsque les deux A coïncident, toutes les lettres coïncident. Si on place l'A du coulisseau en face du B de la règle, l'alphabet de la règle représente par rapport à l'alphabet du coulisseau (décalé d'une lettre) l'alphabet B du tableau de Vigenère, et en décalant 25 fois le coulisseau lettre par lettre on a sur la règle, par rapport aux lettres du clair portées sur le coulisseau, les 25 décalages des alphabets de Vigenère, la lettre placée en face de l'A du coulisseau indiquant la lettre de la clef.

Pour chiffrer le mot ENNEMI avec la clef BADE, nous placerons successivement le coulisseau comme dans la figure ci-après :

A B C D E F G H I J K L M N O P Q... Règle

A B C D *E* F G H I J K L M N O... coulisseau p^{r} B

A B C D E F G H I J K L M *N* O P Q... coulisseau p^{r} A

A B C D E F G H I J K L M *N*... coulisseau p^{r} D

En faisant tourner la figure de 90° dans le sens des aiguilles d'une montre, de manière que l'A de l'alphabet soit en haut, on reconnaît bien les alphabets du tableau de Vigenère.

En lisant sur le coulisseau dans ses positions successives les lettres du mot à chiffrer et écrivant les lettres qui leur correspondent sur la règle, on a FNQ...

En plaçant l'A du coulisseau en face de la lettre clef sur la règle, et lisant la lettre écrite sur le coulisseau en face de la lettre du clair lue sur la règle, on a la substitution de Beaufort. On comprend tout de suite pourquoi, en mettant les alphabets verticaux : on descend l'alphabet de la clef jusqu'à la lettre du clair, et on prend la lettre de l'alphabet A correspondante.

Cette réglette a été modifiée par l'adjonction de chiffres, de signes de ponctuation, etc... Elle a reçu des représentations multiples pour chaque lettre. Enfin, pour rendre l'objet plus maniable, et éviter la nécessité de répéter deux fois l'alphabet pour avoir la coïncidence, on a inscrit les deux alphabets de la règle et du coulisseau sur deux cadrans concentriques. Bien entendu, on peut employer ces cadrans avec un mot clef, en amenant successivement l'A du cadran extérieur par exemple jouant le rôle de coulisseau, en coïncidence avec les lettres de la clef lues sur le cadran intérieur, puis en cherchant sur ce cadran intérieur pour l'écrire dans le cryptogramme la lettre qui coïncide avec la lettre du clair à chiffrer lue sur le cadran extérieur, mais l'usage des cadrans et la facilité de déplacer indéfiniment l'un des cadrans par rapport à l'autre en tournant toujours dans le même sens a créé des méthodes de chiffrement un peu spéciales, que nous examinerons ici. Nous supposerons pour cette étude que

les alphabets sur lesquels nous travaillons sont des alphabets normaux.

Cadrans. — On emploie fréquemment les cadrans de la manière suivante. Partant d'une position initiale, définie par la coïncidence d'une lettre du cadran extérieur avec une lettre du cadran intérieur, on fait tourner le cadran après chaque lettre chiffrée dans un sens convenu d'un angle constant correspondant à 1, 2, etc... lettres. Parfois on emploie des cadrans où la partie fixe porte 26 cases remplies par les 25 lettres de l'alphabet moins W et un repère et la partie mobile 26 cases remplies par les 26 lettres de l'alphabet. On prend la lettre du clair sur la partie fixe, et le repère sert de séparation entre les mots.

Les cryptogrammes ainsi obtenus sont analogues à des cryptogrammes de Vigenère faits avec une clef incohérente composée soit des lettres de l'alphabet dans leur ordre, soit des lettres prises de 2 en 2, 3 en 3, etc... La lettre E sera décalée dans chaque alphabet de 1, 2... rangs sur le précédent. On retombera sur le 1er alphabet au plus tard pour la 27e lettre chiffrée, car si n est le nombre de lettres dont on fait tourner le cadran, après la 26e lettre ou aura tourné de $n \times 26$, c'est-à-dire de n alphabets complets et on retombera sur la 1re lettre du 27e, qui est analogue à tous les autres et au premier. En coupant le cryptogramme en tranches de 26 on retombera donc dans le cas général. Si d'ailleurs on déplace le cadran par 2, on aura un premier retour à l'alphabet de début à la 14e lettre et les tranches de 13 lettres donneront la solution.

Il existe un procédé presque mécanique qui, au prix de quelques tâtonnements, permet de trouver la traduction du cryptogramme, quand les déplacements sont égaux.

Supposons d'abord que l'on fait tourner le cadran d'un angle constant. Soit le cryptogramme QSWNJYSYO.

Sous chaque lettre du cryptogramme, écrivons un alphabet normal, comme si nous cherchions la traduction d'un cryptogramme type Jules César.

Q S W N J Y S Y O
R T X O K Z T Z P
S *U* Y P L A U A Q
T V Z Q M B V B R
U W *A* R N C W C S
V X B S O D X D T
W Y C *T* P E Y E U
X Z D U Q F Z F V
Y A E V *R* G A G W
I B F W S H B H X
A C G X T *I* C I Y

etc....

Considérons les polygrammes formés avec la première lettre de la première colonne et les lettres des autres colonnes décalées d'un intervalle par colonne, soit en descendant QTYQNDYFW, soit en montant (en supposant toujours le tableau prolongé, la 1re ligne étant écrite sous la dernière, etc...) QRUKFTMRG. Ces deux polygrammes ne sont pas des mots français. Nous opérons de même sur la 2e lettre R, la 3e S, etc... Cela ne nous donne rien.

Reprenons la 1re lettre, et considérons les lettres des autres colonnes décalées de deux intervalles. Nous lisons : QUATRIEME.

Si l'on n'avait rien trouvé avec un décalage de 2, on aurait essayé un décalage de 3, etc... La méthode est générale, et, en employant une règle qu'on fait pivoter autour de la lettre de la 1re colonne examinée, elle est rapide.

On peut convenir de faire tourner le cadran d'angles variables après chaque lettre, et certaines machines à chiffrer réalisent automatiquement cette opération. Supposons donc qu'on ait appliqué une clef numérique 1, 2, 3, 4, par exemple. Considérons, pour avoir des déplacements égaux comme ceux que nous avons étudiés ci-dessus, le mouvement comme composé de grands déplacements *égaux* de 1 + 2 + 3 + 4 ou 10 lettres, ces grands dépla-

cements comprenant les petits déplacements intérieurs inégaux 1, 2, 3, 4 comme subdivisions à étudier ultérieurement. Nous avons dit que l'on retombe sur le 1er alphabet au bout de 26 déplacements égaux : si l'on ne chiffrait que la première lettre après chaque grand déplacement, on retomberait sur le 1er alphabet à la 26e lettre. Mais, après cette lettre, avant d'atteindre la 1re lettre du 2e grand déplacement, nous avons ajouté au cryptogramme les 3 lettres correspondant aux petits déplacements 2, 3, 4. Nous aurons donc 26 fois 4 lettres avant de retrouver, non pas le même alphabet, mais la même série. La tranche est donc de $26 \times 4 = 104$ lettres. En réalité, quand le nombre des lettres du grand déplacement est divisible par 2, la tranche est de moitié, soit 52 lettres.

Il est alors très difficile avec ces longues tranches d'appliquer la méthode générale. Si l'origine du chiffrement d'une série de cryptogrammes est sûrement la même, on appliquera les méthodes décrites plus haut pour les cryptogrammes où la répartition en tranches est difficile. Sinon on aura recours au mot probable.

On peut aussi essayer la méthode suivante, qui fait partie des études du commandant Bassières auxquelles nous avons déjà fait des emprunts. Afin d'en abréger l'exposé, nous ne détaillerons pas les opérations dans l'exemple ci-après :

Soit un cryptogramme qu'on sait être chiffré avec 2 cadrans concentriques, avec alphabets normaux sur les deux cadrans. Un essai du type précédent pour le décalage constant n'a rien donné; on est amené à supposer une clef faisant tourner les cadrans d'angles inégaux.

LDPNN PHDQJ EWBJI EGDIZ WUYVV
FPNYB QFAZZ BRRGJ HFHRL JQCVG
HJLRG AMNKW PBN.

Chiffrer par angles sériés par une clef telle que 2-1-3,

c'est chiffrer avec une série de tableaux carrés accolés, où les alphabets de la ligne supérieure se suivent (l'A de l'un venant se juxtaposer au Z de l'autre) en prenant une clef telle que ACDGIJMOPS, etc... dont les intervalles entre les lettres sont 2-1-3-2-1-3-2-1-3...

Or considérons un bigramme chiffré dans un tableau carré au moyen d'une série de bigrammes clefs dont les lettres ont un intervalle constant; par exemple, dans l'alphabet normal, le bigramme EN chiffré au moyen des bigrammes clefs de même intervalle 2, AC, GI, MO. Le chiffrement, en système de Beaufort, nous donne :

Clef	A C	G I	M O
Clair	E N	E N	E N
Cryptogramme	E L	Y F	S Z

L'intervalle de E à L, de Y à F, de S à Z, dans l'alphabet normal, est 7. Les bigrammes obtenus ont donc un intervalle constant, d'ailleurs égal à la différence entre l'intervalle des lettres du bigramme à chiffrer (intervalle EN = 9) et l'intervalle des bigrammes clefs (intervalle A à C, G à I, M à O = 2). En système Vigenère ce serait la somme.

D'autre part, quand on chiffre avec un cadran en tournant toujours le disque mobile d'un même angle, dans le sens des aiguilles d'une montre, de 5 lettres par exemple, si l'on considère le chiffrement d'une même lettre de la partie fixe dans chacune des positions des cadrans, on a une suite de lettres lues sur le disque mobile ayant entre elles des intervalles égaux, de 5 lettres dans l'alphabet en remontant. Ainsi la lettre A, chiffrée avec un 1er alphabet A et des angles constants de 5 (ou sur un tableau avec les alphabets A, F, K, P, etc.), donnera A, V, Q, L, etc. Dans le sens de l'alphabet normal, les intervalles de ces lettres sont égaux à 26 — 5, soit 21. Inversement, à des intervalles AVQL, comptés dans le sens de l'alphabet normal de 21, correspondent pour le cadran des déplacements dans ce même sens de 5 (26 — 21).

Ces remarques étant faites, nous allons d'abord cher-

cher le nombre de termes de la clef numérique, le nombre, autrement dit, de petits déplacements inégaux compris dans un des grands déplacements égaux que nous avons considérés dans la description du système.

Si deux bigrammes du clair, ayant un même intervalle entre leurs lettres, ont été chiffrés avec des bigrammes clefs présentant aussi un même intervalle entre leurs lettres, nous venons de voir qu'ils ont donné des bigrammes présentant cette même particularité (la réciproque n'est pas vraie : on peut avoir des bigrammes du cryptogramme ayant même intervalle résultant de bigrammes quelconques du clair et de la clef). Or les bigrammes clefs distants d'une ou plusieurs longueurs de clefs auront par définition même de la méthode de chiffrement, la qualité mentionnée ci-dessus, de présenter le même intervalle entre leurs lettres. Si, par exemple, la clef est 1-2-4 (elle est par suite à 3 éléments, elle a une longueur de 3), l'intervalle 1 dans la série des bigrammes clefs se représentera au bout de 3 déplacements des cadrans, puis de 6, puis de 3 *n*. L'intervalle 2, tout semblablement, se représentera de 3 en 3 déplacements du cadran, etc... (la réciproque n'est pas vraie, on peut avoir une clef telle que 1-2-1, 1-2-1, où des intervalles de 1 se présentent sans qu'on ait tourné d'une longueur de clef). Donc, parmi les bigrammes du cryptogramme présentant entre leurs lettres un même intervalle, un certain nombre (ordinairement la majorité) proviendront de bigrammes du clair ayant même intervalle et distants d'une ou plusieurs longueurs de clefs. En considérant la répartition de ces bigrammes à même intervalle dans le cryptogramme, et cherchant la distance qui les sépare dans ce cryptogramme, on pourra trouver la longueur de la clef.

Les bigrammes successifs de notre cryptogramme présentent les intervalles que nous avons écrits au-dessous (par exemple de L à D il y a 18 lettres de l'alphabet normal).

LD	DP	PN	NN	NP	PH	HD	DQ	QJ	JE	EW	WB
18	12	24	0	2	18	22	13	19	21	18	5

BJ	JI	IE	EG	GD	DI	IZ	ZW	WU	UY	YV	VV
8	25	22	2	23	5	17	23	24	4	23	0

VF	FP	PN	NY	YB	BQ	QF	FA	AZ	ZZ	ZB .....
10	10	24	11	3	15	15	21	25	0	2 .....

Considérons le nombre de lettres qui séparent des séries de 2 bigrammes présentant le même intervalle entre les lettres, on trouve entre autres :

LD — PH	(intervalle 18)	5 lettres
PH — EW	—	5 lettres
PN — WU	(intervalle 24)	18 lettres
NP — EG	(intervalle 2)	11 lettres
NP — ZB	—	20 lettres

etc...

Si on opère de même pour tous les intervalles, on trouve, comme principaux facteurs des nombres de lettres, 5, 2 et 3, les produits où entre le facteur 5 étant un peu plus fréquents. On admettra donc que notre clef a 5 éléments, que la longueur en est 5. Au cas où le premier résultat ne serait pas suffisamment net, on devrait faire sur plusieurs longueurs successivement, les essais décrits ci-après.

Nous écrirons alors notre cryptogramme sur 5 colonnes :

L D P N N	B R R G J
P H D Q J	H F H R L
E W B J I	J Q C V G
E G D I Z	H J L R G
W U Y V V	A M N V W
F P N Y B	P B N
Q F A Z Z	

Cherchons maintenant de combien de cases le cadran a tourné pour une période comprenant la somme des petits déplacements inégaux, ou le total des chiffres qui constituent la clef (par exemple, si la clef est : 2-0-1-3-6, cherchons le nombre 12). Nous verrons tout à l'heure le but de cette recherche.

Les trois bigrammes LD, PH, et EW proviennent, sup-

posons-nous, de bigrammes de la clef ayant même intervalle entre leurs lettres (l'intervalle indiqué par le premier chiffre de la clef). Ces trois bigrammes ont d'autre part même intervalle entre leurs lettres (L à D; P à H; E à W = 18). Supposons que ces bigrammes, ou du moins d'eux d'entre eux, LD et PH représentent un même bigramme du clair. L et P seraient donc la représentation d'une même lettre, obtenue par un déplacement du cadran égal à une seule longueur de la clef. Le cadran aurait donc tourné de manière à donner entre les deux représentations alphabétiques successives L et P d'une même lettre un intervalle de 4. Comme nous l'avons vu, le cadran aurait tourné de 26—4 soit 22 lettres, et la période de la clef aurait 22 lettres.

Faisons la même étude sur PH et EW : encore une seule longueur de la clef, mais l'intervalle alphabétique de P à E est de 15; ceci nous donne une solution différente, longueur de clef : 26 — 15 = 11 lettres.

Pour faire pencher la balance, essayons encore, par exemple, sur FH et JL aux 9e et 11e lignes, 2e et 3e colonnes. L'intervalle commun de F à H et de J à L est de 2. Considérons alors F et J. Ces lettres sont à deux longueurs de clef, et ne sont qu'à 4 lettres de distance dans l'alphabet. Il faudrait alors pour une clef qui a cinq éléments, un déplacement de 24 lettres $\left(26 - \frac{4}{2}\right)$. C'est possible. Mais remarquons qu'on n'altère pas le résultat en admettant que le déplacement des cadrans correspond non à 4 lettres, mais à 4 + 26, ce qui fera retomber sur la même lettre. La longueur de la clef serait alors $\left(26 - \frac{30}{2}\right)$, soit 11. Ce que nous avons déjà trouvé.

On multiplierait ces calculs, en ajoutant, lorsque la distance qui sépare les lettres dans l'alphabet n'est pas divisible par le nombre de longueurs de clefs qui séparent les bigrammes de même intervalle envisagés, le nombre de fois 26 lettres nécessaire pour que la division devienne possible. En passant en revue tous les groupes de bigrammes ayant même intervalle entre leurs lettres, et placés de même

manière par rapport à la clef, c'est-à-dire dans les mêmes colonnes, nous trouverions que la longueur de la clef est bien 11, c'est-à-dire que le total des déplacements d'une même période est de 11 lettres. Chacune des lettres de la 2e tranche de 5 de notre cryptogramme a donc été chiffrée dans une position du cadran, différant de 11 lettres dans l'alphabet lu de bas en haut, de la position dans laquelle a été chiffrée la lettre correspondante de la 1re tranche. Par exemple, si A du clair était chiffré par A dans la 1re tranche, il l'a été par P dans la 2e. En ramenant toutes les lettres de la 2e tranche de ces 11 places dans l'alphabet, c'est-à-dire en remplaçant P par A, nos nouvelles lettres seraient celles qu'on aurait obtenu en chiffrant la 2e tranche avec les mêmes positions du cadran que la 1re, et, en remontant ainsi les tranches successives, nous aurons un cryptogramme chiffré avec le système de Beaufort et une clef de longueur limitée auquel nous pourrions appliquer la méthode générale.

Pour faire la transformation, écrivons les deux alphabets ci-dessous, dont le premier est décalé de 11 lettres par rapport au deuxième.

l m n o p q r s t u v w x y z a b c d e f g h i j k
a b c d e f g h i j k l m n o p q r s t u v w x y z

et remplaçons les lettres de chaque tranche du cryptogramme, prises dans l'alphabet du dessous, par celles qui leur correspondent dans l'alphabet du dessus, en répétant l'opération pour chaque tranche autant de fois qu'il est nécessaire pour la ramener au même alphabet que la première.

LDPNN	ASOBU	ASXFE	LNKPG	
	PHDQJ	PHMUT	ACZEV	
		EWBJI	PROTK	
			EGDIZ	etc...

Nous pouvons alors placer les tranches du nouveau cryp-

togramme l'une sous l'autre, pour chercher les fréquences :

LDPNN
ASOBU
ASXFE
LNKPG
. . . . .

Une des méthodes connues nous donnera la clef ABDDH et la traduction :

Clef	ABDDH	ABDDH	ABDDH	ABDDH...
Cryptogramme	LDPNN	ASOBU	ASXFE	LNKPG...
Clair	L e s q u	a t r e b	a t a i l	l o n s

n'ont quitté leur quartier que ce matin quatre heures.

Si nous cherchons alors les déplacements à imprimer au cadran, ou la clef numérique, nous constatons dans la clef ABDDH que l'intervalle de A à B est de 1, celui B à D = 2, de D à D = o, de D à H = 4. Les premiers termes de la clef sont donc 1, 2, 0, 4, dont le total est 7. Nous avons dit que le total des termes de la clef était 11, le dernier terme est donc 4, et la clef est 1-2-0-4-4.

Ces méthodes trouveront leur application dans l'étude de cryptogrammes obtenus avec certaines machines à chiffrer.

CHAPITRE VI

AUTOCLAVES ET PROCÉDÉS DIVERS POUR COMPLIQUER LE SYSTÈME DE VIGENÈRE

Textes-Clefs. — La méthode analytique de déchiffrement des cryptogrammes du type Vigenère repose, comme nous l'avons vu, sur la détermination de la longueur de la clef, pour retrouver la périodicité des alphabets employés. On embarrassera donc beaucoup le décrypteur si l'on supprime toute périodicité. Un des procédés employés dans ce but consiste à prendre une clef très longue, aussi longue même que le cryptogramme. On peut y parvenir en employant réellement une clef très longue, fable, suite de nombres écrits en toutes lettres, etc. Mais il y a un autre procédé, dit autoclave. Il consiste, après avoir employé une clef courte, facile à retenir et à orthographier (ce qui n'est pas toujours le cas des clefs longues) pour chiffrer le début du texte clair, à continuer le chiffrement en employant ce texte lui-même comme clef.

Autoclaves. — Pour chiffrer en autoclave avec la clef BADE le texte : L'ENNEMI ATTAQUE, on disposera le chiffrement comme suit :

Clef : BADELENNEMIATT
Clair : LENNEMIATTAQUE

Au déchiffrement, les premières lettres déchiffrées au moyen de la clef convenue BADE donneront la clef pour la suite.

La méthode classique pour déchiffrer un cryptogramme autoclave défini comme ci-dessus est celle du mot probable; la clef étant claire puisque c'est un texte à transmettre, on arrivera à la solution quand les premières lettres des alphabets permettant de passer du texte au mot probable donneront une suite formant un mot ou un fragment de mot. Mais on peut, faute de mot à choisir, ne pas aboutir. Si l'on a plusieurs cryptogrammes, comme le début est chiffré avec la même clef de convention, on peut, en les écrivant les uns sous les autres, appliquer une des méthodes exposées plus haut aux premières colonnes ainsi formées.

Les études du commandant Bassières ont porté sur les autoclaves et il a exposé les considérations ci-après.

Remarquons d'abord que dans un système autoclave, si la clef a 6 lettres, c'est la 1re lettre du clair qui servira de clef pour la 7e lettre. Si donc on connaît la 1re, on connaîtra la 7e. Celle-ci aura servi de clef pour la 13e, que par suite nous trouverons sans difficulté et ainsi de suite.

De plus (et cette remarque exige que l'on emploie le tableau de Vigenère ou un tableau du même type jouissant de la qualité visée ci-dessous tandis que la remarque précédente exige seulement qu'on connaisse l'alphabet qui a servi à chiffrer) dans le système de Vigenère, on obtient la même lettre en chiffrant, par exemple, M avec l'alphabet R qu'en chiffrant R avec l'alphabet M. Si l'on considère dans un texte clair quelconque, l'intervalle séparant deux lettres successives, celui-ci peut prendre une infinité de valeurs. Parmi ces valeurs, il s'en trouvera qui sont égales à la longueur de la clef.

Si une première lettre quelconque se trouve précédée et suivie, à un intervalle égal à la longueur de la clef, d'une même deuxième lettre, cette première lettre servira de clef pour chiffrer la 2e répétition de la seconde, et sera chiffrée avec la 1re répétition pour clef. Cette proposition s'éclaircit par la comparaison des 2 lignes ci-dessous :

C L E F x A m n p E q r s A
x A m n p E q r s A

E est encadré entre 2 A à des intervalles égaux à la clef. Le 1er A sert de clef pour chiffrer E, et E sert de clef pour chiffrer le 2e A. Les deux chiffrements, de E avec clef A, de A avec clef E, seront, en Vigenère, représentés par la même lettre, et les deux lettres semblables ainsi obtenues dans le cryptogramme seront séparées par un intervalle égal au nombre de lettres de la clef. La réciproque n'est pas vraie, et des lettres semblables peuvent se trouver à des intervalles quelconques. Mais de nombreux relevés ont donné une majorité certaine, parmi les intervalles qui séparent les répétitions d'une même lettre, à celui qui représente la longueur de la clef.

Soit donc le cryptogramme, autoclave et chiffré en Vigenère :

CEDHE LCIUG EWZDM EMRVN MEMHG
JEQRF TICLR PEDCP RPEFI V

Si nous relevons les intervalles des répétitions d'une même lettre entre 5 et 10 (nous supposerons que nous sommes certains que la clef a entre 5 et 10 lettres) tels que EWZDME (5 lettres), ELCIUGE (6 lettres), CEDHELC (7 lettres), nous trouverons 11 intervalles de 6 lettres contre 2 de 5, 1 de 7, 1 de 9. Nous admettrons alors que la longueur de la clef est 6 lettres.

(Dans le système de Beaufort, on peut faire une recherche du même genre, mais il faut remarquer qu'au lieu de retrouver la même lettre quand S est chiffré en clef M par exemple, ou M chiffré en clef S (ce qui est le cas dans le système Vigenère), on trouve la lettre complémentaire prise dans les alphabets inversés diminués de A.

A B C D E F G H I J K L M
A. Z Y X W V U T S R Q P O

N O P Q R S T U V W X Y Z
N M L K J I H G F E D C B

Le cryptogramme donné plus haut comme exemple devient, si on le chiffre en Beaufort :

UWDHW BGIOS EKRNE GELFX WUWFG
ZWSJT HACDR REVYB JJWHI F.

Nous chercherons les intervalles de U, non plus avec U, mais avec G, de W avec E, etc..., et nous arriverons au même résultat que ci-dessus.)

Reprenons notre Vigenère, et cherchons à reconstituer la clef. A cet effet coupons le cryptogramme en séries de 6 lettres.

C E D H E L	G J E Q R F
C I U G E W	T I C L R P
Z D M E M R	E D C P R P
V N M E M H	E F I V

Faisons des hypothèses sur la 1re lettre de la clef, supposons que ce soit A; la 1re lettre du clair, chiffrée avec la clef A, sera alors C. Cette 1re lettre servira de clef pour la 7e, qui est traduite par C et qui sera donc A. La 13e lettre rendue par Z en clef A, serait Z; la 19e rendue par V en clef Z, serait W, etc... En continuant nous trouverions que si la 1re lettre de la clef était A, les premières lettres claires des tranches de 6 seraient

CAZWKJVJ

Par un raisonnement analogue, si B était la 1re lettre de la clef, on aurait comme premières lettres claires des tranches de 6 :

BBYXJKUK

On continuerait de même, et on aurait un tableau pour les 26 lettres :

Clef A, C A Z W K J V J
— B, B B Y X J K U K
— C, A C X Y I L T L

— Y, E Y B U M H X H
— Z, D Z A V L I W I

Dès qu'on a une ligne de ce tableau, les autres s'en déduisent, en écrivant en colonne l'alphabet normal de haut en bas pour les colonnes paires, de bas en haut pour les colonnes impaires.

Il y a une de ces séries et une seule, celle qui correspond à la vraie première lettre de la clef, qui est la bonne, les lettres y sont des lettres du clair, et le clair est soumis à la loi des fréquences. Si nous avions assez d'éléments, nous y trouverions l'E avec sa fréquence maxima et la ligne correspondant au maximum de E serait la bonne. Mais puisque dans le cas général on ne peut espérer appliquer sur cette seule lettre la loi des fréquences, on peut au moins essayer de l'appliquer à un groupe de lettres fréquentes, par exemple à E S A R I N T U L O. Nous ferons donc, pour chaque ligne du tableau, le total des présences de ces lettres, et nous admettrons comme bonne (au besoin s'il y a plusieurs résultats égaux, après des essais faits en juxtaposant les colonnes suivantes), la ligne qui donne le plus fort total.

Nous ne reproduirons ici que les colonnes qui donnent les totaux les plus élevés.

Clef E,	Y E V A G N R N	—(1 E, 1 A, 1 R, 2 N) = 5
— I,	U I R E C R N R	6
— L,	R L O H Z U K U	5
— R,	L R I N T A E A	8
— V,	H V E R P E A E	5

La 1re lettre de la clef sera donc R.

Pour chercher la 2e lettre de la clef, nous construirons un tableau analogue sur la 2e colonne EIDNJIDF, en supposant d'abord que la lettre est A, puis B, etc...

On a :

Clef A,	E E Z O V N Q P	 4
— B,	D F Y P U O P Q	 2
— E,	A I V S R R M T	 6
— F,	Z J U T Q S L U	 5

C'est la lettre E qui nous donne le maximum. Les deux

premières lettres de la clef seront donc R E, et les bigrammes reconstitués du cryptogramme seront :

LA....RI....IV....NS....TR....AR....EM....AT..

Tous ces bigrammes sont parfaitement acceptables. Nous ne pousserons pas la reconstitution plus loin. La clef est Rennes et le texte : La 4e division se mettra en marche demain matin.

On opérerait de même sur les lettres suivantes de la clef. Mais nous rappellerons qu'au cas où l'on hésiterait entre deux solutions à un moment donné, on pourra avoir recours aux totaux des fréquences. Si nous avions hésité ici (par exemple par suite d'une erreur de lettre diminuant la fréquence ERASINTULO sur la clef E) entre la clef E et la clef F, nous aurions considéré les totaux des fréquences des bigrammes obtenus en juxtaposant aux premières lettres des tranches chacune des solutions possibles pour les deuxièmes.

Clef R E		*Clef R F*	
L A =	12	L Z =	0
R I =	11	R J =	0
I V =	2	I U =	0
N S =	16	N T =	25
T R =	12	T Q =	1
A R =	19	A S =	3
E M =	20	E L =	16
A T =	10	A U =	8
TOTAL	102	TOTAL	53

La solution de la clef R E était encore indiquée par ce procédé.

Nous ferons remarquer que nous n'avons pas supposé que la clef était claire. Il faut également admettre que parfois une partie des opérations ne donnera pas du premier coup, sur un document court, la bonne solution.

Si par exemple le procédé qui donne la longueur de la clef nous induit en erreur, nous nous en apercevrons parce que la suite des recherches pour trouver les lettres de la clef ne nous donnera rien qui vaille, et nous recommencerons nos essais avec une autre longueur de clef, celle qui vient après la première dans la liste des fréquences d'intervalles de laquelle nous avons déduit cette longueur.

On peut attaquer les cryptogrammes autoclaves faits avec le système de Vigenère ou celui de Beaufort en utilisant la constatation suivante :

Si nous chiffrons la phrase : La quatrième division... avec la clef Rennes et un système autoclave avec tableau de Vigenère, nous obtenons (Voir plus haut) :

CEDHE LCIUG EWZDM EMRV.....

Nous venons de voir que nous pouvions déterminer la longueur de la clef, qui est de 6 lettres. Coupons notre texte en tranches de 6.

CEDHEL CIUGEW ZDMEMR V.....

Déchiffrons la 2e tranche CIUGEW en prenant pour clef la 1re CEDHEL et en employant le tableau de Vigenère. Nous avons

Clef :	CEDHEL
Texte :	CIUGEW
Résultat :	AERZAL

Servons-nous de ce premier résultat comme clef pour déchiffrer de même la 3e tranche, puis du nouveau résultat pour déchiffrer la 4e, etc... Comme l'opération de chiffrement en système Beaufort est la même que celle du déchiffrement en Vigenère, on peut, au point de vue pratique, dire qu'ayant commencé à chiffrer en système Beaufort la 2e tranche avec la clef CEDHEL (1re tranche), on chiffre les autres avec une clef autoclave qui au lieu d'être le *clair* du texte à chiffrer, est le cryptogramme obtenu.

Nous obtenons ainsi :

```
CEDHEL  AERZAL  ZZVFMG  WORZAB  .....
CIUGEW  ZDMEMR  VNMEMH  GJEQRF  .....
AERZAL  ZZVFMG  WORZAB  KVNRRE  .....
```

Or si l'on chiffre directement le texte : La quatrième division... avec un tableau de Vigenère et une clef formée de la juxtaposition de notre clef Rennes avec la suite des lettres correspondantes aux lettres de cette clef dans le tableau des lettres complémentaires déjà évoqué :

```
A B C D E F G H I J K L M
A Z Y X W V U T S R Q P O

N O P Q R S T U V W X Y Z
N M L K J I H G F E D C B
```

c'est-à-dire avec la clef RENNESJWNNWI, on obtient :

```
R E N N E S J W N N W I
L A Q U A T R I E M E D
C E D H E L A E R Z A L

R E N N E S J W N N W I .....
I V I S I O N S E M E T .....
Z Z V F M G W O R Z A B .....
```

C'est la première ligne de notre chiffrement précédent. Cela s'explique de la façon suivante.

Chiffrer en Vigenère, c'est décaler la lettre du clair d'autant de rangs qu'on a passé d'alphabets. On aura donc le rang de la lettre du cryptogramme en ajoutant au numéro d'ordre de la lettre du clair celui de la lettre de la clef, cette dernière étant numérotée dans un alphabet où A = 0, B = 1, etc... Considérons alors comment nous avons obtenu les deux textes CEDHEL AERZAL...

Les opérations faites pour chiffrer la 1re tranche du clair LAQUAT avec la clef RENNES ont été les mêmes dans les deux procédés (L + R, 11e lettre + 17e = 28e ou 2e = C).

Pour la 2e tranche AERZAL, c'est d'une part le résultat du déchiffrement de CIUGEW avec la clef CEDHEL.

CIUGEW est le chiffrement de RIEMED avec la clef LAQUAT, soit lettre à lettre RIEMED + LAQUAT (R + L = 17 + 11 = 28 ou 2 = C).

CEDHEL est de même LAQUAT + RENNES.

AERZAL = RIEMED + LAQUAT — LAQUAT — RENNES = RIEMED — RENNES.

D'autre part, AERZAL est le résultat du chiffrement de RIEMED par JWNNWI, c'est-à-dire RIEMED + JWNNWI.

Or, comme nous l'avons fait remarquer, JWNNWI est complémentaire de Rennes. RENNES + JWNNWI = 26 (le total de chaque groupe de lettres de même rang R + J, E + W, etc...). Donc JWNNWI = — RENNES.

Il est donc tout naturel qu'on trouve le même résultat.

3e tranche :

ZZFMG = ZDMEMR — AERZAL
= IVISIO + RIEMED — RIEMED + RENNES
= IVISIO + RENNES

c'est-à-dire IVISIO chiffré avec la clef RENNES, et ainsi de suite.

Le cryptogramme que nous avons obtenu en chiffrant en système de Beaufort le texte donné autoclave à partir du 2e groupe au moyen d'une clef formée du 1er groupe puis d'une autoclave, a été transformé en un texte obtenu avec une *clef non autoclave.* Le procédé général pour la solution des problèmes de double substitution s'applique. On pourra donc, quand les autres procédés auront échoué, ou pour obtenir des confirmations d'hypothèses, faire des hypothèses sur la longueur de la clef et par suite essayer avec des tranches de 4, 5, 6 lettres, etc... de traiter les résultats obtenus comme des substitutions à clef limitée.

Ici l'hypothèse de 6 lettres à la clef et la disposition

en tranches de 12 lettres serait confirmée par deux répétitions de trigrammes :

C E D H E L A E r z a L
Z Z V F M G W O r z a B
K V N R r e j N P U A L
V Q N V r e j P V A

Quand le cryptogramme a été chiffré par la méthode de Beaufort, les opérations sont encore plus simples.

Le chiffrement de la phrase : La quatrième division... avec la clef Rennes et un système autoclave sur procédé de Beaufort nous donne :

UWDHWB GIOSEK RNEGEL FXWUWT GZWSJT HACDRR EVYRJJ WHIF

Chiffrons ce cryptogramme, à partir du 2e groupe, par le système Vigenère, en prenant comme clef le 1er groupe suivi du résultat même du chiffrement, nous avons :

UWDHWB AERZAL RRVFEW W...
G I O S E K RNEGEL FXWUWF G...
A E R Z A L RRVFEW WORZAJ C...

Or le chiffrement du texte clair avec la simple clef Rennes, en système Beaufort, donne

RENNES RENNES RENNES R...
LAQUAT RIEMED IVISIO N...
UWDHWB AERZAL RRVFEW W...

La première ligne du tableau précédent nous donne donc une transformation de notre cryptogramme autoclave proposé en un cryptogramme à clef limitée; et nous pourrons faire des essais, en supposant successivement différentes longueurs de la clef, pour chercher un texte où des répétitions nous permettront de croire que nous avons la solution de longueur de clef cherchée et de travailler sur les colonnes pour y retrouver les alphabets.

Il y a des cas où l'on emploie comme clef non le texte

clair mais le cryptogramme lui-même. Lorsque le décrypteur connaît le tableau qui a servi à chiffrer, il n'a pas grande difficulté à retrouver le texte, puisqu'il possède et le cryptogramme, et la clef qui a servi à le chiffrer; il s'agit seulement de placer cette clef, puisque l'ignorance où l'on se trouve de la clef de convention laisse ignorer à quelle lettre du cryptogramme l'auto-chiffrement a été commencé. On y arrive avec quelques tâtonnements.

Autoclaves à clef d'une seule lettre. — On doit signaler les cryptogrammes autoclaves où la clef de convention n'a qu'une lettre, c'est-à-dire où une lettre est chiffrée avec la lettre qui la précède immédiatement. Ces cryptogrammes formés de lettre en lettre sont faciles à faire avec les cryptographes tels que la règle de Saint-Cyr sans effort de mémoire et sans recherches sur le texte pour retrouver les lettres à chiffrer avec un même alphabet (transcription de la clef au-dessus du texte ou mise en tableau). Les procédés indiqués plus haut permettent de ramener les autoclaves de cette nature chiffrés en Vigenère à une substitution avec clef de deux lettres, ceux qui sont chiffrés en Beaufort à une substitution simple.

On applique cette méthode aussi en prenant le cryptogramme comme clef. Certaines machines à chiffrer opèrent de cette manière. Comme nous l'avons dit plus haut, la solution du problème de décryptement est simple, lorsqu'on connaît le tableau de chiffrement et la clef. Si l'on donne : YYOII BSAEQ
on écrira :

Clef	?	Y	Y	O	I	I	B	S	A	E	Q
Cryptogramme	Y	Y	O	I	I	B	S	A	E	Q	U
Clair	?	a	q	u	a	t	r	i	è	m	e

Il faudra faire l'essai en Vigenère et en Beaufort. On remarquera que, une lettre chiffrée en alphabet A étant identique à elle-même, les deuxièmes lettres des redoublements sont des A du clair, et les lettres du cryptogramme qui suivent A ont été chiffrées sans modification.

Clefs interrompues. — En dehors des clefs longues, autoclaves ou non, un moyen fort prôné pour rompre la périodicité de la clef est le procédé des clefs interrompues. Au lieu de chiffrer avec la clef Boulogne-Boulogne-Boulogne..., on chiffre avec la clef Boulogne-Boul-Boulo-Boulogne... Bien entendu, si l'on interrompait la clef à des intervalles réguliers : Boulogne-Boul-Boulogne-Boul-Boulogne... on aurait simplement un cryptogramme chiffré avec la clef Boulogne Boul, où un certain nombre de répétitions apparaîtraient bien à cause de la répétition de Boul dans la clef, mais où les répétitions un peu éloignées indiqueraient la période Boulogne-Boul. L'intéressant est donc, pour gêner le décrypteur, d'interrompre la clef n'importe quand, à la volonté du chiffreur. Un procédé classique est d'indiquer cette rupture et le retour à la première lettre de la clef par un signe spécial, ordinairement la lettre W, qu'on réserve pour cet usage, en chiffrant les W du texte clair par deux V.

Le chiffrement se fera alors comme suit :

Clef	B O U L O G N E B O U L B O U L O G N E
Clair	L a q u a t r i è m e w d i v i s i o n
Crypto	M O K F O Z E M F A Y H E W P T G O B R

Clef	B O U L O G N B O U L O
Clair	s e m e t t w r a e n w
Crypto	T S G P H Z J S O Y Y K

Au déchiffrement, qu'on devra faire lettre par lettre au lieu d'écrire la clef Boulogne au-dessus du texte du commencement à la fin et de traduire toutes les lettres en clef A, puis en clef B, etc... comme on le fait souvent, ou reprendra au commencement de la clef chaque fois qu'on rencontrera un W.

Pour le décrypteur, la périodicité est rompue. Parfois, s'il n'y a pas trop de ruptures et si l'on a des répétitions rapprochées, on peut soupçonner la longueur de la clef en travaillant entre deux ruptures (d'ailleurs sans le savoir) et procéder à des essais, mais toute rigueur est bannie du procédé. Les études que nous avons exposées,

permettant de chercher successivement les lettres de la clef quand on a plusieurs cryptogrammes (ou même un seul avec une clef claire) ou de travailler sur les débuts de quelques cryptogrammes écrits les uns sous les autres, peuvent être répétées même avec une clef interrompue, en tenant compte de la possibilité de trouver dans le cryptogramme la lettre indicatrice de rupture (ainsi tous les bigrammes se terminant par W deviennent acceptables). Avec la méthode du mot probable, on pourra essayer le mot sans modification, mais en considérant à la fois le résultat obtenu dans une position, et dans la position décalée d'un rang à droite.

Exemple : cryptogramme FRCGKJGCZB; mot probable DIVISION.

Essais :

1°		F	R	C	G	K	J	G	C		2°	R	C	G	K	J	G	C	Z
	Clair	d	i	v	i	s	i	o	n			d	i	v	i	s	i	o	n
	Clef	C	J	H	Y	S	B	S	P			O	U	L	C	R	Y	O	M

3°	C	G	K	J	G	C	Z	B	
	d	i	v	i	s	i	o	n	
	Z	Y	P	B	O	U	L	O	

On voit dans le troisième essai les lettres OUL, qui ont déjà paru dans le deuxième essai, et doivent appartenir à la clef BOULO... (sans doute BOULOGNE).

On peut aussi faire des essais successifs en intercalant une nulle entre chacun des bigrammes du mot probable : dWivision, diWvision, etc... Tous ces procédés ont des chances de réussir avec une clef claire, mais avec une clef incohérente ou un peu longue le décrypteur aura du mal à aboutir.

Nulles. — Enfin on peut compliquer le décryptement par l'introduction de lettres nulles. Si ces nulles sont mises en tête, elles n'apportent pas de trouble sérieux, la périodicité générale n'est pas atteinte. Ce n'est que dans le cas où l'on travaillerait sur les fréquences dans les débuts de

télégrammes ou dans la recherche méthodique des lettres de la clef que des lettres rares ou formant des bigrammes rares viendraient apporter une gêne sérieuse, qu'elles soient laissées claires ou qu'elles soient chiffrées.

Si l'on répartit des nulles dans le texte, bien entendu il faut qu'elles ne soient introduites qu'après le chiffrement, sinon elles n'interrompraient pas la périodicité. On peut alors adopter pour nulles certaines lettres qu'on supprime des tableaux de chiffrement (Voir plus loin système de Porta), par exemple j, k, w, qu'on remplace dans le clair par i, c, v. Le déchiffreur raie d'abord tous les j, k et w du cryptogramme; le décrypteur ne trouve plus ses répétitions aux intervalles correspondant à la longueur de la clef. Mais ceci exige que le tableau soit secret, sinon le décrypteur saura bien que j, k, w n'y figurent pas, et en déduira que ces lettres sont nulles. Or, en général, quand on admet l'emploi du tableau carré de Vigenère à alphabets normaux, c'est pour ne pas se donner la peine de garder le tableau secret. Sinon ou aurait avantage à compliquer le tableau comme nous le verrons plus loin. D'autre part, en cas de transmission télégraphique, il faut tenir compte de l'existence d'erreurs venant de l'inscription par le télégraphiste d'une lettre pour une autre : si l'on raie des lettres avant déchiffrement, et qu'il y ait erreur sur une lettre à rayer, on complique les opérations par la rupture de la coïncidence de la clef et du texte ainsi émondé. Le même danger s'applique au cas où l'on introduit arbitrairement des nulles quelconques, que rien ne signale que l'impossibilité de traduire le cryptogramme ainsi modifié avec la clef sans déplacer à l'endroit de chaque nulle cette clef d'un rang à droite. C'est un procédé ennuyeux pour le déchiffreur, obligé d'opérer lettre à lettre, et qui, chaque fois qu'il se produit un dérangement dans le mot attendu, se demande s'il a affaire à une nulle, à une erreur du chiffreur ou à une erreur de transmission.

En tout cas, l'emploi des nulles, fort gênant pour le décrypteur quand il n'a qu'un seul cryptogramme, l'est moins, sauf en tête, quand on en a plusieurs et qu'on peut travailler sur les débuts.

Nous nous sommes très longuement étendus sur les substitutions à double clef avec alphabets normaux. C'est qu'elles ont donné lieu, comme nous l'avons dit, à beaucoup de travaux ingénieux. Certains même, comme de Viaris, ont introduit dans leurs théories des notations algébriques, concernant les relations entre le rang dans l'alphabet normal des lettres du clair (A), de la clef (E), du cryptogramme (Y) : A + E = Y (en comptant a = 0, b = 1, etc. : système Vigenère; A + Y = E : système Beaufort), et ont généralisé ces équations en indiquant de nouveaux systèmes. Comme exemple de complication du travail sur les tableaux à alphabets normaux, nous indiquerons celle de Rozier, qui, pour chiffrer une lettre, descend le long de la colonne du tableau correspondant à cette lettre jusqu'à ce qu'il rencontre la lettre de la clef, suit alors la ligne de cette dernière lettre jusqu'à ce qu'il rencontre la lettre suivante de la clef, et remonte la colonne pour inscrire dans le cryptogramme la lettre du haut de la colonne.

De tels systèmes, bien que difficiles, ont donné lieu à des études qui en ont montré le déchiffrement comme possible. Nous n'y insisterons pas dans ce recueil, consacré aux études d'ordre général.

CHAPITRE VII

SUBSTITUTIONS A DOUBLE CLEF
A ALPHABETS INCOHÉRENTS MAIS PARALLÈLES

Nous avons vu toutes les facilités que nous a données pour le décryptement la certitude que les cryptogrammes étaient chiffrés avec des procédés employant des alphabets normalement ordonnés.

Or, il est fait un emploi fréquent d'alphabets incohérents, soit d'un seul alphabet déplacé parallèlement à lui-même, donnant un tableau analogue à celui de Vigenère et pouvant être utilisé avec des règlettes type de Saint-Cyr ou des cadrans, soient d'alphabets totalement différents les uns des autres.

Le problème comprend alors, en général, la recherche non seulement de la clef qui indique l'ordre des alphabets, mais de l'alphabet ou des alphabets eux-mêmes. Pourtant, dans certains cas, ceux où le décrypteur connaît par une source quelconque les alphabets employés, la seule recherche est celle de la clef. Elle s'opère par les procédés que nous avons déjà exposés : recherche de la longueur de la clef par les répétitions, répartition du cryptogramme en tranches de cette longueur, recherche, dans chaque colonne constituée par la superposition de ces tranches, de la lettre E, ou de toute autre, dont l'identification permet de reconnaître l'alphabet employé, supposé connu, et d'en placer toutes les lettres.

Porta. — Comme alphabets classiques, nous citerons ceux du système de Porta. Nous les décrirons sous la forme où on les rencontre dans les vieux ouvrages, avec 22 let-

tres seulement (on chiffre le j avec l'i, le k au moyen du q, le v et le w avec l'u), mais on peut faire des tableaux analogues avec 26 lettres.

Le tableau est formé de 11 alphabets réciproques. Chacun d'eux est employé avec deux lettres clefs (même alphabet pour les lettres de la clef A ou B par exemple). La lettre d'une des lignes de l'alphabet se chiffre avec la lettre correspondante de l'autre ligne.

Tableau de Porta.

A. B	a	b	c	d	e	f	g	h	i	l	m	
	n	o	p	q	r	s	t	u	x	y	z	
C. D	a	b	c	d	e	f	g	h	i	l	m	
	z	n	o	p	q	r	s	t	u	x	y	
E. F	a	b	c	d	e	f	g	h	i	l	m	
	y	z	n	o	p	q	r	s	t	u	x	
G. H	.	.	.	.	.	.	.	.	.	.	.	.

etc.....

Exemple de chiffrement :

Clef	B	A	D	E	B	A	D	E	B	A
Texte	l	a	d	i	v	i	s	i	o	n
Cryptogramme	Y	N	P	T	H	X	G	T	B	A

Porta a ainsi indiqué un moyen commode de reconstituer de mémoire une série d'alphabets différents. Nous avons vu comment on peut reconstituer de tels alphabets au moyen de mots clefs.

Analyse des opérations d'un décryptement. — Afin de pouvoir présenter un certain nombre de remarques sur le déchiffrement des substitutions doubles à alphabets incohérents, nous prendrons un exemple de cryptogramme de cette sorte et nous en effectuerons l'étude, en passant rapidement sur les opérations déjà décrites et expliquées à propos des systèmes à alphabets normaux.

Soit le cryptogramme ci-dessous, que nous supposerons avoir été reçu en tranches de 5 chiffres, mais que, pour éviter de l'écrire une fois de plus, nous écrirons en tranches de 7.

L'étude des répétitions en effet nous y amène, car si la répétition de ox (tranches 23 et 27) est à un intervalle de $24 = 2^3 \times 8$,
celle de zw (15 — 28) à $95 = 5 \times 19$,
celle de wx (4 — 26) à $147 = 7^2 \times 3$,
celle de fx (2 — 4) à $18 = 2 \times 3^2$, etc..., la plupart des autres répétitions, surtout celles des polygrammes, mettent en évidence le facteur 7 [qdih (1 — 5), intervalle $28 = 2^2 \times 7$,
qdih (5 — 24) : $133 = 7 \times 19$,
pz (2 — 3) = 7 — lx (3 — 11) : $63 = 7 \times 3^3$ — lx (11 — 16) : $35 = 7 \times 5$ — rq (1 — 17) : $112 = 7 \times 2^3$ — dchqs 10 — 20) : $70 = 7 \times 2 \times 5$ — mvmde (20 — 25) : $37 = 7 \times 5$, etc...] La clef doit donc avoir 7 lettres.

1	2	3	4	5
yrqdihp	mfxkpzr	dlxcpzb	mzwxsfx	tsqdihl
6	7	8	9	10
mmxijzh	crfpslc	mlqtezq	grmaslr	itidchq
11	12	13	14	15
slxrswh	jriacqh	zrrdyhb	mbixekm	zwwpztm
16	17	18	19	20
mlxqoep	prqfzsb	mvuvssj	mzqturu	mvmdchq
21	22	23	24	25
smgtrrt	zvmdssr	yesdyox	whqdihu	mvmdcly
26	27	28	29	30
xwxzekm	zoxdvwq	wtxnzwe	mlreiwh	skqasqh
31	32	33	34	35
ekpiysl	mfxgmlh	xewqpch	xhxrieo	wrudxrm
36	37	38	39	40
mzwpert	mskqyrm	srmrpsm	meacern	cvzdurt
41	42	43	44	45
iwseofx	wqwgmwh	crayerc	mmgqilx	yesemrl

46	47	48	49	50
mvbkssb	zzygmrx	yeqeehp	mlaxfrj	mrumrkr
51	52	53	54	55
ivdterb	ifxrqzh	crudqzx	xzhnsrl	isqpyox
56	57	58	59	60
ywxdfre	ilwtvpe	mlrqpvr	mlqdorb	zzggmey
61	62	63	64	
xreecrm	ihrduqx	whkdckt	czxr	

Faisons dans chaque colonne le tableau des fréquences. Pour accélérer l'exposition, nous ne le reproduirons pas ici comme cette première opération nous le donnerait. On le trouvera plus bas avec des additions. Nous constatons que la comparaison des diverses colonnes ne nous indique aucun parallélisme, aucune égalité d'intervalles entre les lettres fréquentes, ce que fait généralement un relevé sur un cryptogramme genre Vigenère à alphabets normaux. Les alphabets ne sont donc probablement pas normalement ordonnés. Les lettres les plus fréquentes, sur 64 ou 63 lettres à la colonne sont dans chaque colonne :

m — 21 ; r — 12 ; x — 14 ; d — 17 ; s — 9 ; r — 16 ; h — 9 ;

nous les adopterons pour E. Ayant remplacé ces lettres par E dans leurs colonnes respectives, nous ferons le compte des séquences des autres lettres avec E, et nous avons alors le tableau de fréquence ci-après, complété par les séquences avec E.

TABLEAU

1		2		3		4		5		6		7	
m	0/21/1	r	1/12/0	x	0/14/2	d	2/17/1	s	1/9/1	r	1/16/0	h	0/9/0
i	0/7/0	l	6/9/3	q	2/10/4	r	4/6/1	c	4/7/2	h	0/7/0	x	1/8/0
z	1/6/1	v	4/7/0	w	0/6/0	t	0/5/0	e	0/7/3	s	3/6/0	m	3/7/3
w	0/5/1	z	3/7/2	m	2/5/3	q	1/5/0	i	3/6/0	z	0/6/2	b	2/6/3
x	2/5/1	e	1/5/0	r	1/4/2	e	0/5/0	m	0/6/2	w	1/5/3	r	0/5/1
y	0/5/1	w	0/4/2	u	3/4/2	g	2/4/0	y	2/5/1	l	2/5/1	q	0/4/0
c	3/5/3	h	0/4/1	s	0/3/1	p	0/4/1	p	0/5/0	k	0/4/0	l	2/4/3
s	1/4/1	m	2/3/1	g	0/3/0	a	0/3/2	o	1/3/1	e	0/3/0	t	3/4/1
g	0/1/1	s	1/3/0	a	1/3/0	x	0/3/1	u	2/3/2	q	1/3/2	p	0/3/2
e	1/1/0	f	2/3/3	i	1/3/1	i	1/2/0	z	0/3/0	f	1/2/0	e	1/3/2
j	1/1/1	p	0/2/1	k	0/2/1	c	1/2/0	f	1/2/2	o	0/2/0	u	1/2/2
d	0/1/0	k	0/2/0	f	1/1/0	n	1/2/1	q	1/2/0	c	0/1/1	c	1/2/2
p	0/1/1	b	1/1/0	i	0/1/0	k	1/2/1	v	1/2/0	t	0/1/0	y	0/2/0
t	0/1/0	o	0/1/1	d	0/1/0	z	1/1/0	j	0/1/0	v	0/1/0	j	1/2/2
		q	0/1/0	z	0/1/1	f	0/1/0	r	0/1/1	p	0/1/0	o	0/1/0
				h	0/1/0	v	0/1/1	x	1/1/1			u	1/1/0
				e	0/1/0	y	0/1/0						
				b	0/1/0								

Une première remarque : si nous avions eu des séquences très nombreuses avec les E des colonnes voisines pour une des lettres que nous avons admises comme E uniquement parce qu'elles étaient les plus fréquentes, il aurait fallu supposer que l'une au moins n'était pas E, puisque la séquence EE est rare, et vérifier sur les deux colonnes donnant lieu à ces séquences si une autre lettre fréquente, bien que n'étant pas *la plus* fréquente, ne semblait pas plutôt être l'E, ne donnant que peu de séquences avec E.

D'après le compte des séquences, nous pouvons faire des hypothèses sur certaines lettres en les classant en voyelles ou consonnes.

Nous laisserons dans le doute la situation des lettres qui ne viennent qu'une fois, et celle des lettres qui, fréquentes, ne donnent avec E que peu de bigrammes, ou ne donnent pas de bigrammes de la forme E-lettre, en même temps que d'autres de la forme lettre-E.

Nous considérerons alors comme voyelles probables, autres que R

1	2	3	4	5	6	7
i	k	w	t	p	h	x
		g	e	z	k	q
					e	y

Remarque. — Nous avons admis comme voyelle probable x7 (qui pourrait donner lieu à discussion puisqu'il a une séquence), parce qu'il n'a qu'une séquence sur huit présences. Toutefois nous serons prêts à renoncer à cette hypothèse.

Comme consonnes à peu près certaines, nous admettons

1	2	3	4	5	6	7
z	l	q	r	c	w	m
x	z	m	n	y	l	b
c	m	r	k	o	q	l
s	f	u		u		t
		i		f		e
						u
						c
						j

Nous n'avons pas de moyen actuellement de déterminer la valeur exacte de ces lettres. Récrivons le cryptogramme, en indiquant sous les lettres les hypothèses faites à leur sujet.

Nous ne reproduirons pas ici ce tableau. On le trouvera plus loin augmenté de quelques additions. De son examen aucun résultat important ne se révèle à nos yeux, sauf l'hypothèse que la première lettre du télégramme est un L, commencement de l'article LE. Nous portons cette valeur dans le cryptogramme; nous examinons immédiatement les séquences de L : trois fois sur quatre L est suivi de e de la 2e colonne (nous écrirons e2). Or, e2 est fréquent, et ne donne qu'une séquence avec E; d'après le tableau

des bigrammes, il y aurait des chances pour que nous ayons LA : les particularités de fréquence ne s'y opposent pas. On mettra donc A pour e2.

Malgré ces hypothèses nous ne pouvons aller plus loin.

Nous allons essayer de déterminer quelques voyelles au moyen des diphtongues, mais auparavant cherchons au moyen des longues séquences si nous ne pouvons découvrir quelques voyelles de plus. Au 55e groupe, nous trouvons une séquence de 5 consonnes sqpyo entre deux voyelles. Elle est possible, à condition que la 3e lettre p4 représente S. Or, p4 n'est pas très fréquent, et ne donne qu'une séquence sur 4 avec E; elle ne donnerait pas de ES, il est donc probable que ce n'est pas S. Comme il nous manque des voyelles, cherchons laquelle des 5 lettres aurait le plus de chances d'être une voyelle. Pour cela, considérons pour chacune des répétitions de chacune de ces lettres l'intervalle qui la sépare de la voyelle connue la plus voisine, faisons la moyenne de ces intervalles (total du nombre d'intervalles 1 + 2 fois le total des intervalles 2, etc... et la somme du tout divisée par la fréquence de la lettre). Nous avons :

S 2 — (2x1) + (1x2) = 4	intervalle moyen		4/3
q 3 — (9x1) + (1x2) = 11	—	—	11/10
p 4 — (3x1) + (1x3) = 6	—	—	6/4
y 5 — (3x1) + (1x2) + (1x3) = 8	—	—	8/5
o 6 — (2x1) = 2	—	—	2/2

Le plus grand intervalle moyen est celui de y5. Mais d'après le tableau des séquences nous avions fait l'hypothèse que y5 était une consonne. Nous nous trouvons avec deux hypothèses contraires, nous laisserons y5 douteux avec propension à penser que c'est une voyelle. Nous n'avons pas d'autre longue séquence entre voyelles.

Revenons à nos considérations de diphtongues. Nous savons que normalement les deuxièmes lettres ont des chances d'être U ou I, que la diphtongue la plus fréquente est OU, et que I précède assez souvent E et O, tandis qu'il

est précédé par A. Nous avons comme diphtongues en plaçant les lettres dans leurs colonnes :

1	2	3	4	5	6	7	
					h	q	(groupe 10 — 20)
		g	t				(21)
	A	w					(33)
		w	t				(56)
					e	y	(60)

Nous avons bien peu d'éléments. Nous retiendrons la possibilité pour t4 d'être U, pour y7 ou q7 d'être U; la diphtongue du groupe 33 est gênante (A amènerait U, mais alors t ne saurait être U). Comme on a à tenir compte des séquences de voyelles provenant de la fin d'un mot et du commencement du suivant, si l'on suppose que Aw est une séquence de cette sorte, on pourra essayer pour g3 et w3 les valeurs A et O.

Étant donnée la légèreté de la base sur laquelle reposent ces hypothèses, faute d'un texte assez long pour nous fournir de plus nombreux éléments, nous allons revenir à nos tableaux de fréquences, et, nous basant sur la fréquence de l2, q3, r4, et c5, et leurs séquences avec E, nous allons supposer que ces lettres représentent S. Nous portons cette valeur dans le cryptogramme, et nous avons le tableau suivant, où aucune invraisemblance ne vient infirmer nos hypothèses (De l'hypothèse sur les diphtongues, nous n'avons écrit dans le tableau que t4 = U).

1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
y r q d i h p	m f x k p z r	d l x c p z b	m z w x s f x
L E S E . v .	E . E c v . .	. S E . v . c	E c v . E . v
t s q d i h l	m m x i j z h	c r f p s l c	m l q t e z q
. . S E . v c	E c E . . . E	. E . . E c c	E S S v . . v

10

g r m a s l r	i t i d c h q	s l x r s w h	j r i a c q h
. E c . E c .	v . c E S v v	c S E S E c E	. E c . S c E

1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
z r r d y h b	m b i x e k m	z w w p z t m	m l x q o e p
c E c E . v c	E . c . . v c	c . v . v . c	E S E . c v .

20

p r q f z s b	m v a v s s j	m z q t u r u	m v m d c h q
. E S . v . c	E . . . E . c	E c S U c E c	E . c E . v v
s m g t r r t	z v m d s s r	y e s d y o x	w h q d i h u
c . v U . E c	c . c E E . .	L A . E c . v	. . S E . v c
m v m d c l y	x w x z e k m	z o x d v w q	w t x n z w e
E . c E S c v	c . E . . v c	c . E E . c v	. . E c v c c

30

m l r e i w h	s k q a s q h	e k p i y s l	m f x g m l h
E S c v . c E	c v S . E . E	. v . . c . c	E c E . . c E
x e w q p c h	x h x r i e o	w r u d x r m	m z w p c r t
c A v . v . E	c . E S . v .	. E . E . E c	E c v . S E c

40

m s k q y r m	s r m r p s m	m e a c e r n	c v z d u r t
E . . . . E c	. E c S . . c	E A . . . E .	c . . E c E c
i w s e o f x	w q w g m w h	c r a y e r c	m m g q i l x
v . . v c . v	. . v . . c E	c E . . . E c	E c v . . c v
y e s e m r l	m v b k s s b	z z x g m r x	y e q e e h p
L A . v . E c	E . . c E . c	c c E . . E v	L A S v . v .

50

m l a x f r j	m r u r m k r	i v d t e r l	i f x r q z h
E S . . . E c	E E c S . v .	v . . U . E c	v c E S . . E
c r u d q z x	x z h n s r l	i s q p y o x	y w x d f r e
c E c E . . v	c c . c E E c	v . S . c . v	L . E E . E c

60

i l w t v p e	m l r q p v r	m l q d o r b	z z g g m e y
v S v U . . c	E S c . v . .	E S S E c E c	c c v . . v v
x r e e c r m	i h r d u q x	w h k d c k t	c z x r
c E . v S E c	v . c E c c v	. . c E S v c	c c E S

Malheureusement l'examen de ce tableau ne nous donne encore aucun élément pour avancer dans le décryptement.

Portons cependant sur un tableau de concordance les valeurs obtenues :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1					m						y															
2	e				r														l							
3	g?				x										w?				q							
4					d														r		t					
5					s														c							
6					r																					
7					h																					

Symétrie de position. — Faisons une nouvelle hypothèse, fort importante. Supposons que le tableau de substitution comprenait bien des alphabets incohérents, mais que ces alphabets, comme ceux du tableau de Vigenère, étaient des alphabets parallèles, c'est-à-dire que nous avons le même alphabet transporté parallèlement à lui-même, toutes les lettres étant décalées d'un même intervalle d'un alphabet à l'autre. Nous aurions alors la même disposition qu'avec un jeu de réglettes du type Saint-Cyr, l'une portant l'alphabet normal, l'autre l'alphabet incohérent de substitution, et, quand nous connaîtrions la position d'une des lettres de la deuxième réglette pour un des 7 alphabets, nous pourrions en déduire la traduction des autres lettres, dont les intervalles avec celle-ci restent constants. Si, dans l'alphabet 2, e est à 4 intervalles de r, il en sera encore à 4 intervalles dans l'alphabet 4, et, de la position de r4 = S, nous déduirons e4 = O. C'est ce principe d'invariabilité des intervalles quand les alphabets sont parallèles que Kerckhoffs a mis en évidence sous le nom de symétrie de position, et qui permet, quand on connaît la signification de quelques lettres dans les différents alphabets, d'en déduire la signification de certaines autres en écrivant simplement les lettres dans un tableau, à leur intervalle des lettres déjà connues.

e4 est d'ailleurs d'après le tableau des fréquences une voyelle, et sa valeur O n'a rien qui choque nos hypothèses antérieures.

Mais si nous admettons l'hypothèse des alphabets parallèles, l'alphabet 6, qui a le même E que l'alphabet 2, sera le même alphabet que ce dernier. L'examen des fréquences des différentes lettres, malgré la différence de pourcentage de celles-ci, ne vient pas à l'encontre de l'hypothèse. L'ordre des lettres, par rang de fréquence, n'est pas le même, mais il n'y a pas d'opposition ni pour les fréquences, ni pour les séquences avec E. On pourra donc compléter la colonne 6 du tableau de correspondance et du cryptogramme.

Comme nous avons des lettres, communes aux alphabets 2 et 4, qui nous donnent un point de départ pour juxtaposer ces deux alphabets avec leur décalage, nous y transportons toutes les lettres qui figurent dans chacun d'eux. Nous avons t2 = G; d2 = Q, l4 = C, et nous pouvons transporter ces valeurs dans le cryptogramme.

Mais nous ne voyons toujours pas de mots qui s'y révèlent.

Cherchons à travailler sur la symétrie de position. Il nous faut trouver dans chaque alphabet au moins une lettre figurant déjà dans un autre, afin d'avoir un repère qui indique leur décalage réciproque. Nous avons fait sur x7 et q7, en les supposant voyelles, une hypothèse qui peut permettre des recherches sur ces lettres x q dont nous connaissons l'intervalle x3 — q3 égal à 14 lettres de l'alphabet normal; et nous allons étudier les voyelles dont l'intervalle normal est de 14. Cet intervalle est celui de AO et de UI. Essayons d'abord x7 = A, q7 = O; par symétrie de position, il en résulte h3 = I, h3 n'est pas bien fréquent, mais en dehors de cela pas d'objection. Sa situation à la tranche 54 correspond bien à une voyelle probable. Essayons maintenant x7 = U, q7 = I; il en résulterait h3 = O, la place est déjà, bien qu'avec un gros doute, prise par g3 ou w3. L'essai n'est pas bien convaincant. Nous pouvons le compléter en reportant y et w dans

l'alphabet 7, ce qui aurait pu nous fixer également sur la valeur de g3 et w3 (essais à faire g3 = A et w3 = O avec x7 = A et q7 = O, puis g3 = O et w3 = A avec les mêmes valeurs de x7 et q7), g3 = A et w3 = O donnent w7 = K, q7 = W. Ce sont deux lettres rares, et de fait g7 et w7 ont une fréquence nulle. Mais comme nous aurions un résultat de même nature avec g3 = O, w3 = A, nous n'avons pas tiré grand'chose de cette tentative. Nous n'avons rien qui infirme nos hypothèses, rien qui les appuie vivement.

Notre tableau de concordance est alors :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1				m								y														
2	e			r		t											d		l							
3	g?			x				h						w?					q							
4				d										e					r		t					
5				s															c							
6	e			r		t											d		l							
7	x			h						w?				q											g?	

Bien entendu, nous reporterons ces valeurs, comme hypothèses, dans notre cryptogramme, mais nous serons encore obligés de chercher de nouveaux éléments.

Essayons toujours d'introduire dans un des alphabets, une lettre figurant déjà dans un autre, pour avoir un repère permettant d'évaluer le décalage. Nous avons vu que y5, que nous avions considéré comme consonne, était probablement voyelle. Essayons y5 aux places de voyelles et estimons les résultats au moyen de l'intervalle ym tiré de l'alphabet 1. Si y5 = O, m5 = H; or m5 est fréquent et H rare. Si y5 = I, m5 = B, même observation. Si y5 = A, m5 = T, ce qui est tout à fait admissible, y5 = V donnerait une autre solution admissible, m5 = N. Mais si nous reportons alors dans l'alphabet 1 les intervalles ys et yc tirés de 5, nous trouvons avec y5 = A, s1 = P, c1 = D, ce qui concorde avec les fréquences (s1 = 4, c1 = 5) et pour y5 = U, s1 = V, c1 = J, ce qui n'est pas satisfaisant en raison de la rareté de J. Donc y5 = A.

Pendant que nous sommes dans cet alphabet 5, continuons à y étudier les voyelles. p5 = I, z5 = O donnerait p1 = T, z1 = Z, ce qui n'est pas satisfaisant pour la fréquence z1 = 6 et ne l'est guère pour p1 = 1. Par contre p5 = O, z5 = I donne p1 = Z, z1 = T, ce qui est tout à fait acceptable. Nous accepterons donc ces valeurs.

En admettant les hypothèses précédentes, notre cryptogramme est devenu ce qui suit (les majuscules sont les lettres identifiées, la minuscule c veut dire consonne, v voyelle) :

```
y r q d i h p   m f x k p z r   d l x c p z b   m z w x s f x
L E S E . v .   E . E c O . .   . S E . O . c   E c O . E . A

                5
t s q d i h l   m m x i j z h   c r f p s l c   m l q t e z q
. . S E . v c   E c E . . . E   D E . . E S c   E S S U . . O

                              10
g r m a s l r   i t i d c h q   s l x r s w h   j r i a c q h
. E c . E S .   v G c E S v O   P S E S E c E   . E c . S c E

                                              15
z r r d y h b   m b i x e k m   z w w p z t m   m l x q o e p
T E c E A v c   E . c . . v c   T . O . I G c   E S E . c A .

                                                          20
p r q f z s b   m v u v s s j   m z q t u r u   m v m d c h q
Z E S . I . c   E . . . E . c   E c S U c E c   E . c E S v O

s m g t r r t   z v m d s s r   y e s d y o x   w h q d i h u
P . v U . E c   T . c E E . .   L A . E A . A   . . S E . v c

                5
m v m d c l y   x w x z e k m   z o x d v w q   w t x n z w e
E . c E S S v   c . E . . v c   T . E E . c O   . G E c I c c

                              30
m l r e i w h   s k q a s q h   e k p i y s l   m f x g m l h
E S c O . c E   P v S . E . E   . v . . A . c   E c E . T S E

                                              35
x e w q p c h   z h x r i e o   w r u d x r m   m z w p c r t
c A O . O . E   T . E S . A .   . E . E . E c   E c O . S E c
```

40

m s k q y r m	s r m r p s m	m e a c e r n	c v z d u r t
E . . . A E c	P E c S O . c	E A . . . E .	D . . E c E c
i w s e o f x	w q w g m w h	c r a y e r c	m m g q i l x
v . . O c . A	. . O . T c E	D E . . . E c	E e A . . S A

45

y e s e m r l	m v b k s s b	z z x g m r x	y e q e e h p
L A . O T E c	E . . c E . c	T c E . T E A	L A S O . v .

50

m l a x f r j	m r u r m k r	i v d t e r b	i f x r q z h
E S . . . E c	E E c S T v .	v . . U . E c	v c E S . . E

55

c r u d q z x	x z h n s r l	i s q p y o x	y w x d f r e
D E c E . . A	c c I c E E c	v . S . A . A	L . E E . E c

60

i l w t v p e	m l r q p v r	m l q d o r b	z z g g m e y
v S O U . . c	E S c . O . .	E S S E c E c	T c A . T A v
x r e e c r m	i h r d u q x	w h k d c k t	c z x r
c E O S E c .	v . c E c c A	. . c E S v c	D c E S

avec le tableau de correspondance :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1			c	m							y								z							p
2	e			r		t											d		l							
3	g?			x				h						w?					q							
4				d										e					r							
5	y			s				z		-				p					c	m						
6	e			r		t											d		l							
7	x			h						w?				q										g?		

On pourrait commencer à chercher des mots probables dans le cryptogramme, par exemple les derniers mots, avec les lettres qui y sont connues et les hypothèses consonnes voyelles, pourraient être : DES ORDRES. Néanmoins, nous continuerons la méthode analytique avec le jeu de la symétrie de position et l'étude des fréquences.

L'examen des tableaux donnerait comme étude inté-

ressante à faire la recherche de la valeur de h6 (fréquence 7, séquences 0). Nous n'exposerons pas ici en totalité les essais à ce sujet. Le trigramme S h O des tranches nos 10 et 20 donnerait l'idée d'essayer h6 = I, hypothèse qui se heurterait aux résultats admis pour l'alphabet 3 (s'ils avaient une lettre commune, les autres lettres devraient l'être aussi). Les autres essais h6 = O par exemple, qui entraîne t3 = A, se heurtent aussi à des hypothèses précédentes ou ne sont pas convaincants. Il en reste l'impression que h6 n'est peut-être pas une voyelle.

Nos alphabets ont actuellement 2 à 2 des lettres communes : 1-5 = c m y s z p, 3-7 = g? x h w? q; 2-4 = ertdl; mais nous n'avons pas le moyen d'amalgamer ces 3 séries. Cherchons à identifier une lettre d'une série non encore identifiée, et existant dans une autre série, par exemple m7, qui est fréquente (7 fois) et semble une consonne (6 séquences avec E). Suivant l'ordre ESARINTULO, essayons d'abord l'hypothèse m7 = S. Il en résulterait d'après les intervalles de ce m7 hypothétique à q7 et à x7, que q1 représenterait A et x1 M; les fréquences de x1 (5 fois) et de q1 (0) rendent cette hypothèse peu vraisemblable.

Essayons alors m7 = R. Il en résulterait h1 = R, or h1 a la fréquence 0. Il en résulterait aussi, suivant que w3 est bien à sa place ou doit être permuté avec g3 (et également w7 et g7), que w1, dont la fréquence est 5, représenterait X ou J. Rejetons encore l'hypothèse.

Essayons m7 = N. Cela entraîne y7 = U, et y7 doit être une voyelle. z7 = B, p7 = I, c7 = M n'ont rien de choquant.

Dans l'alphabet 1, x1 = R est d'accord avec la fréquence 5 dont 3 séquences. Mais w1 = B, g1 = N ne va pas avec les fréquences w1 = 5, g1 = 1. Toutefois, comme nous avons hésité jusqu'à présent sur la répartition de w et g entre les deux places qui leur sont attribuées, en les intervertissant et écrivant w1 = N, g1 = B nous aurons des fréquences normales.

Nous avons maintenant deux suites de lettres de l'alphabet incohérent, rangées dans leur ordre et à leur intervalle :

g . c mq . . . . . y . w . s . x . z . h . . . p .

et

e . . . r . t . . . . . d . l . . . . . .

Malheureusement, les deux séries peuvent s'intercaler l'une dans l'autre de plusieurs manières différentes sans superposition de lettres.

En reportant les nouvelles valeurs dans le cryptogramme, en particulier p7 = I et en considérant h6 (qui vient 2e comme fréquence dans 6, que nous avons d'abord supposé voyelle parce qu'il ne donnait pas séquences avec E, puis que nous n'avons pu placer comme voyelle), nous lui trouvons des séquences avec des voyelles qui nous confirment que c'est probablement une consonne.

1re	tranche	LESE. hIE
10e	—	ESbOPSESE
13e	—	EAh. E
20e	—	ESbOP
48e	—	LASO. hIES

En essayant diverses traductions, on est conduit à supposer h6 = T. Comme e6 = S, h se placerait alors immédiatement à la droite de l dans l'alphabet incohérent qui deviendrait :

g e c m q r . t . . y . w . s . x d z l h . . . p .

Le tableau des alphabets est alors :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1		g	e	c	m	q	r		t			y		w		s		x	d	z	l	h				p
2 6	e	c	m	q	r		t			y		w		s		x	d	z	l	h			p		g	
3	w		s		x	d	z	l	h			p		g	e	c	m	q	r		t			y		
4		s		x	d	z	l	h			p		g	e	c	m	q	r		t			y		w	
5	y		w		s		x	d	z	l	h			p		g	e	c	m	q	r		t			
7	x	d	z	l	h			p		g	e	c		m	q	r		t		y		w		s		

et le commencement du cryptogramme donne :

```
y r q d i h p  m f x k p z r  d l x c p z b  m z w x s f x
L E S E . T I  E . E . O R P  S S E P O . .  E R A D E . A

t s q d i h l  m m x i j z h  c r f p s l c  m l q t e z q
I N S E . T D  E C E . . R E  D E . L E S M  E S S U R R O

g r m a s l r  i t i d c h q
B E R . E S P  . G . E S T O
```

Cette fois les mots se devinent facilement : « Le septième corps se portera demain sept décembre de Blesmes sur Robert-Espagne stop » et l'alphabet se complétera de proche en proche. Nous l'indiquons ci-dessous dans tout son développement.

a t n b y j w f s k x d z l h v o u p i g e c m q r

Le texte du cryptogramme est d'autre part, après la phrase déjà traduite : « ...stop. Ses éléments de tête atteindront la ligne Sermaize-St. Eulien vers une heure. stop. Couverture en place avant sept heures sur le front Veel-Longeville. stop. Le poste de commandement sera à Robert-Espagne, le général se rendra en personne auprès du général commandant le 2e corps à la cote 230 à la sortie sud de Veel. stop. Au fur et à mesure de leur arrivée dans la vallée de la Saulx, les troupes se mettront au repos en attendant des ordres. »

Nous pouvons avoir intérêt à chercher si la clef est claire et quelle elle est alors.

Remarquons à ce sujet que, bien que nous ne connaissions pas la lettre par laquelle commence l'alphabet incohérent et qui constitue un repère (ou : bien que nous ne connaissions pas le repère s'il est en dehors de l'alphabet), tout l'alphabet aura subi des déplacements parallèles à cette lettre. Si, en passant de la 1re colonne à la 2e, la lettre repère a été décalée de 2 lettres, toutes les lettres de l'alphabet auront été décalées de 2 lettres. La succes-

sion des lettres de la clef peut donc être indiquée non seulement par les lettres qui se trouvaient successivement en face du repère (et qui donneront un sens si la clef est claire), mais par les lettres se trouvant successivement devant une lettre quelconque de l'alphabet. Établissons donc la série de ces clefs, et s'il en est une claire nous la verrons apparaître.

Supposons que la lettre repère ait été p. Elle a été amenée successivement en face de Z X M L O X I. Cela ne donne rien. Supposons alors que c'était la lettre voisine de p. Cette lettre a été amenée successivement devant les lettres voisines des précédentes A Y N M P Y J. Pour continuer à chercher la lettre repère en considérant les lettres avec lesquelles elle a coïncidé, nous voyons qu'après avoir écrit sur une ligne la première série de ces lettres, nous n'avons qu'à continuer à écrire l'alphabet normal sous chacune d'elles* :

Z X M L O X I
A Y N M P Y J
B Z O N Q Z K
C A P O R A L

et nous trouvons la clef claire : caporal. En faisant cette opération dès qu'on a la traduction d'une même lettre dans plusieurs colonnes, on peut quelquefois deviner la clef et établir la position des colonnes encore inconnues par rapport aux autres.

Nous nous sommes trouvés pour cette étude dans des conditions assez favorables. Le cryptogramme était long : 445 lettres. Les E avaient dans chaque colonne la fréquence maxima. Les séquences avec E ont donné de bons renseignements, sauf pour h6. Nous avons d'ailleurs, dans l'exposé, cherché à appeler l'attention sur des séries de remarques à utiliser le cas échéant plutôt qu'à arriver à la traduction le plus vite possible. Enfin le tableau était fait avec des alphabets parallèles.

Même dans ce dernier cas, il est des cryptogrammes où

la méthode analytique se heurte à des difficultés très considérables, et où il faut avoir recours à la méthode du mot probable.

Exemple d'application de la méthode du mot probable. — Soit par exemple le cryptogramme suivant de 188 lettres. Nous supposons qu'il a été recueilli le 5 mai par un poste de T. S. F. au cours d'opérations militaires, et que nous savons que l'ennemi se sert d'une règle type Saint-Cyr avec un alphabet incohérent fréquemment changé.

Le radiotélégramme était émis par un poste de corps d'armée. Nous écrivons immédiatement, pour cette étude, le cryptogramme en tranches de 7 chiffres; les répétitions nous amènent à considérer en effet que la clef a 7 chiffres (qvt 1re et 6e tranches : 35 d'intervalle — ehlui 9e et 25e : 112, zke 10e et 20e : 70, ye 14e et 15e : 7 etc...) :

yeqvtbh jrkvrbn tkirsxq xhxqyqh

jehgoeb tsqvtfx tqxrsxb deaptly

xehluin zkerslx heiaxet crqfmhh

tskqpsb yemeqhh yetdqoh grwtokm

zlaqrrn yrwrsxb araqsln zkekysb

fsidorm zqwgcwx pkidyve weyfmnp

dehluib akaqcly xfwqur.

Les relevés des fréquences nous donnent pour chaque colonne :

1	2	3	4	5	6	7
t 4	e 9	a 4	q 6	s 4	l 4	b 6
y 4	k 5	i 4	r 4	o 3	r 3	h 5
z 4	r 5	w 4	d 3	r 3	x 3	n 4
x 3	s 3	h 3	v 3	t 3	b 2	x 3
a 2	q 2	q 3	f 2	u 3	e 2	m 2
d 2	f 1	e 2	g 2	y 3	h 2	e 1
j 2	h 1	k 2	e 2	c 2	i 2	p 1
c 1	l 1	x 2	a 1	q 2	s 2	q 1
f 1		m 1	x 1	m 1	f 1	t 1
g 1		t 1	k 1	n 1	k 1	y 1
h 1		y 1	p 1	p 1	n 1	z 1
p 1			t 1	x 1	o 1	
w 1					q 1	
					v 1	
					w 1	

Pour les colonnes 1 et 3 incertitude sur E. On peut bien en admettant que e2 et q6 représentent E, constater que yl a4 et i4 donnent des séquences avec e2 et q6 et ne doivent pas être E, mais les séquences s5 l6 et q4 s5 l6 (groupes 10 et 19) nous inspirent des doutes sur la valeur des premières lettres de la première ligne de notre tableau en tant que E. Ces doutes seraient renforcés par le relevé des séquences, que nous n'avons pas reproduit ici. La séparation des voyelles apparaît comme à peu près impossible.

Dans des cas semblables, il y a lieu de faire appel à la méthode basée sur l'hypothèse qu'un mot donné se trouve dans le cryptogramme et sur l'identification de ce mot. Ne connaissant pas les alphabets, le décrypteur ne pourra se contenter comme avec les tableaux de Vigenère à alphabets normaux de promener sous le texte du cryptogramme le mot probable et de chercher dans chaque position la lettre de la clef qui donnerait l'alphabet dans lequel la lettre du clair correspond à la lettre du cryptogramme. Il faut faire appel aux facultés d'intuition et d'ingéniosité du cryptologue.

Le cryptogramme dont il s'agit ayant été donné comme

exercice, voici comment le problème a été résolu par un des chercheurs.

Il a remarqué que, dans les données, on précisait que le document était radiotélégraphié par un corps d'armée. Il avait déjà traité des problèmes de ce genre, avec des renseignements analogues, et il avait remarqué qu'il s'agissait généralement d'informations ou d'ordres, et que la forme du début était fort souvent : « Le corps d'armée... » ou « la division... » avec des verbes au futur, des numéros d'unités, des dates. Par exemple « demain le corps d'armée attaquera... » ou « la deuxième division partira demain à n heures... », etc...

Son attention fut appelée sur certaines similitudes entre les deux premiers groupes :

y e q v t b h
j r k v r b n

deux v à 7 lettres d'intervalle, 2 b à 7 lettres d'intervalle, et, après un certain nombre d'essais ayant pour but de constituer des débuts de phrases présentant cette particularité, c'est-à-dire du type :

. . . v . b . . . . v . b

il arriva à adopter les mots « LA SIXIÈME DIVISION » qui, comme on le voit :

L A S I X I E
M E D I V I S
I O N

constituent une solution du problème, qui ne choque en rien le tableau des fréquences (l'X apparaît avec fréquence 3 sur 26, mais il faut admettre sur des cryptogrammes courts des écarts de cette grandeur).

Il partit donc de cette hypothèse et écrivit les valeurs trouvées dans le tableau de concordance :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1								t		y	j															
2	e				r								k													
3			k								i						q									
4								v																		
5																					r		t			
6								b																		
7				h													n									

Sachant que le cryptogramme avait été fait avec un alphabet mobile il appliqua la symétrie de position qui lui donna :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	i		e		q	r		t		y	j				k											
2	e			q	r		t		y	j				k												i
3			k								i		e				q	r		t					y	j
4								v																		
5	y	j			k								i		e			q	r		t					
6								b																		
7				h													n									

En portant ces valeurs dans le cryptogramme, il trouva :

y	e	q	v	t	b	h		j	r	k	v	r	b	n		t	k	i	r	s	q	x		x	h	x	q	y	q	h
L	A	S	I	X	I	E		M	E	D	I	V	I	S		I	O	N	.	.	.	.		.	.	.	A	.	E	

5

j	e	h	g	o	e	b		t	s	q	v	t	f	x		t	q	x	r	s	x	b		d	e	a	p	t	l	y
M	A	.	.	.	.	.		I	.	S	I	X	.	.		I	D	.	.	.	.	.		.	A	.	.	X	.	.

10

x	e	h	l	u	i	n		z	k	e	r	s	l	x		h	e	i	a	x	e	t		c	r	q	f	m	h	h
.	A	.	.	.	.	S		.	O	P	.	.	.	.		.	A	N	.	.	.	.		.	E	S	.	.	.	E

15

t	s	k	q	p	s	b		y	e	m	e	q	h	h		y	e	t	d	q	o	h		g	r	w	t	o	k	m
I	.	D	.	.	.	.		L	A	.	.	U	.	E		L	A	V	.	U	.	E		.	E	.	.	.	.	.

20

z l a q r r n y r w r s x b a r a q s l n z k e k y s b
. . . . V . S L E . . . . . . E . . . S . O P . A . .

f s i d o r m z q w g c w x p k i d y v e w e y f m n p
. . N . . . . . D . . . . . . O N . A . . . . Y . . . .

25

d e h l u i b a k a q c l y x f w q u r
. A . . . . . . O . . . .

Il n'y a rien de choquant dans les séquences ainsi obtenues. Nous avons dit qu'il y avait lieu de s'attendre à trouver vers le début du document un verbe au futur. Ce peut être ce verbe qui nous donne l'A du 4e groupe, auquel cas q4 serait R, et cette hypothèse permet d'ajouter au tableau les valeurs v1 = W, v2 = U, v3 = J, v5 = L, k4 = C, i4 = M, e4 = O, etc... Comme les valeurs obtenues ne sont pas en contradiction avec les fréquences, l'hypothèse de départ se trouve renforcée. Mais la lecture du document n'est pas possible encore.

On s'adressa alors à la date d'envoi : 5 mai. On a au 6e groupe le mot SIX suivi de 2 lettres inconnues et d'un I; on lut : LA SIXIEME DIVISION.....RADEMAIN..... SIXMAI....
et les identifications q6 = D, h3 = I, g4 = N, f6 = M, x7 = A permirent de raccorder tous les fragments d'alphabets des 7 colonnes et d'obtenir les lettres suivantes de l'alphabet de la réglette placée dans la position de l'alphabet 1 :

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
i . e . . q r . t n b y j . f . k x . . . h v . . .

Les premiers mots du cryptogramme devenaient alors

y e q v t b h j r k v r b n t k i r s x q x h x q y q h j e h g o e b
LASIXIE MEDIVIS IONS.PO RTERADE MAIN.AT

t s q v t f x t
I.SIXMA I ....

La position de s et de o dans l'alphabet s'en déduisit immédiatement. On put alors lire le texte :

« La 6e division se portera demain matin 6 mai de Sept-Saulx sur Aigny. stop. Ses avant-gardes atteindront la route La Veuve Beaumont sur Vesle à sept heures. stop. Cantonnement dans la zone Aulnay Athis Aigny Thours sur Marne. »

L'alphabet qui avait servi à préparer l'exercice est le suivant :

i g e c m q r a t n b y j w f s k x d z l h v o u p

Les remarques ci-dessus sur la forme, la destination possible, la date, etc..., sont de la nature de celles qu'on devra constamment employer pour résoudre les problèmes dont on ne peut trouver la solution par les méthodes analytiques. Ces dernières ont ordinairement l'avantage de ne comporter que des opérations presque mécaniques, dont on peut charger des aides, et les grands centres d'étude de cryptographie, lorsqu'ils connaissent par un moyen quelconque (souvent par la description publiée par l'auteur) des systèmes susceptibles d'être utilisés pour des buts de guerre ou de diplomatie, s'efforcent de trouver pour le décryptement des procédés basés sur des opérations qui n'exigent que de l'attention (relevés de fréquences, additions, symétrie de position, etc.) (1). Mais les cryptologues exercés emploient souvent des remarques telles que celles que nous avons citées ci-dessus, et l'expérience des années 1914 à 1918, pour ne citer que celle-là, prouve que dans la pratique on a souvent à sa disposition des éléments de cette nature, permettant des hypothèses beaucoup plus audacieuses que celles qui servirent au décryptement du dernier exemple. Le lecteur aurait donc tort de croire que de tels éléments de réussite

(1) Voir par exemple l'ouvrage intitulé *L'Indice de coïncidence et ses applications en cryptographie*, chez Fournier, 1921, traduction d'un ouvrage de langue anglaise.

ne se trouvent que dans les ouvrages de cryptographie, où l'auteur déchiffre un document qu'il a chiffré lui-même. La correspondance cryptographique, à condition qu'elle soit intense et qu'on ait des éléments de travail assez nombreux, fournit souvent des éléments d'étude si complets qu'un auteur n'oserait pas les utiliser tous pour résoudre un problème, de crainte d'être taxé d'exagération manifeste.

CHAPITRE VIII

SUBSTITUTIONS A DOUBLES CLEFS AVEC DES ALPHABETS NON PARALLÈLES OU PRÉSUMÉS TELS AVEC DES REPRÉSENTATIONS NUMÉRIQUES SIMPLES OU MULTIPLES, ETC.

Lorsqu'on a affaire à des cryptogrammes composés avec des alphabets incohérents différant l'un de l'autre, et qu'on ne connaît pas ces alphabets, le problème devient de plus en plus difficile.

Si la clef est assez courte et le cryptogramme assez long pour que les fréquences puissent donner des renseignements suffisants dans chaque colonne, on place les E, on cherche à reconnaître les voyelles et on traite chaque alphabet isolément, comme nous avions commencé à le faire dans l'exemple antéprécédent lorsque, faute d'éléments, nous avons dû faire appel à la symétrie de position pour profiter dans chacun des alphabets des découvertes déjà faites sur les autres, qui étaient parallèles. Si l'on a plusieurs cryptogrammes présumés faits avec la même clef, on peut travailler sur les commencements.

Mais nous considérons que des systèmes de ce genre, avec des clefs longues et changeant fréquemment, et en prenant la précaution de ne pas chiffrer de longs cryptogrammes, peuvent constituer un des meilleurs modes de communication secrète à l'heure actuelle, surtout si l'on prend la précaution d'éviter que la clef ne se révèle claire à un déchiffreur qui se serait procuré et les alphabets et un mot probable. Or, on peut éviter de révéler la clef

claire en chiffrant par exemple non pas dans l'alphabet indiqué par la lettre de la clef, mais dans l'alphabet voisin de droite ou de gauche.

Substitutions doubles à représentations numériques et multiples. — Tout ce que nous avons dit sur les systèmes à double substitution en caractères alphabétiques s'appliquerait aux systèmes où une lettre est figurée par un groupe de chiffres ou un groupe de lettres. On peut faire des tableaux, ou mieux des réglettes ou des cadrans, où les lettres sont remplacées par des groupes, et avoir alors toutes les dispositions mentionnées plus haut : Vigenère avec des groupes numériquement ordonnés tels que ceux de la 1re colonne soient la traduction des lettres de l'alphabet normal écrit à la gauche du tableau, alphabets incohérents parallèles, avec symétrie de position, alphabets incohérents quelconques. L'usage des groupes permet même d'introduire un nouvel élément, la représentation multiple. L'appareil à bande mobile décrit à la fin du chapitre III permet de chiffrer en substitution double avec représentation multiple et alphabets incohérents. C'est encore dans l'étude des mots répétés du clair, semblablement placés par rapport à la clef, qu'on peut espérer trouver un moyen d'entreprendre le décryptement de méthodes de ce genre, qui, il ne faut pas se le dissimuler, paraissent extrêmement sûres. Celles qui rentrent, avec l'appareil à représentations multiples, dans les applications du paragraphe suivant, le sont également, et ce n'est guère que sur des maladresses de chiffreur, par exemple sur l'inscription, en tête de tranches égales, de groupes repères indiquant les traductions successives de A et par suite l'ordre des groupes, que nous avons pu trouver des éléments de résultats satisfaisants.

Substitutions doubles par tranches. — Nous avons jusqu'ici fait allusion à des procédés où, en principe, les alphabets employés changent à chaque lettre, sauf redoublements de la clef.

Ces déplacements continuels, surtout quand on chiffre

avec des instruments tels que les règles de Saint-Cyr ou l'appareil de Carmona, ont quelquefois paru gênants. Aussi, dans certains cryptogrammes, reconnaît-on que le chiffreur chiffre plusieurs lettres de suite avec la même clef, par exemple les 5 lettres d'un même groupe du télégramme. On peut trouver aussi dans des documents écrits et non télégraphiés des substitutions dont la clef change à chaque mot, mais où tout un mot est chiffré avec la même clef. Comme les mots conservent alors leur physionomie, la méthode du mot probable est à appliquer; et souvent on reconnaît que le nombre d'alphabets de substitution est limité, que les n^e, $N + n^e$, $2N + n^e$, etc... mots sont chiffrés avec le même alphabet, si bien que, lorsque le système est ainsi déterminé, on peut, même sans découvrir le mot probable qui convient, traiter les documents par la voie analytique en groupant les mots chiffrés avec le même alphabet pour les traiter comme une substitution simple.

C'est dans cet ordre d'idées qu'il est parfois intéressant, lorsqu'on a un cryptogramme chiffré en mots séparés et qui n'est pas une substitution simple, d'écrire les mots les uns sous les autres, les lettres de même numéro en colonnes. Les finales des mots de même longueur révèlent parfois par leur similitude que le procédé employé a été une substitution double où la clef était interrompue à la fin de chaque mot et reprise du début pour chiffrer le mot suivant. En s'en tenant aux alphabets voisins de l'alphabet du clair, avec une clef genre Gronsfeld indiquant les décalages à faire subir à chaque lettre pour la chiffrer, on a un procédé qui peut être employé sans document, les opérations se faisant de tête. On peut du reste appliquer des procédés à clef « interrompue à chaque mot » aux transmissions télégraphiques, à condition d'indiquer l'interruption de la clef, ou la séparation des mots, comme nous l'avons vu plus haut, par exemple en faisant suivre chaque mot d'un W.

Changements d'alphabet. — Ce genre de procédé peut s'appliquer encore dans les conditions suivantes : après

avoir chiffré une partie d'un télégramme avec un alphabet incohérent se déplaçant parallèlement à lui-même (par exemple avec une réglette ou un cadran), ce qui permet aux correspondants d'opérer assez simplement, et au décrypteur de faire jouer, s'il connaît le système, la symétrie de position, on change l'alphabet sans changer la clef, ce qui n'exige par exemple que le remplacement de la face supérieure du coulisseau d'une règle genre Saint-Cyr par la face inférieure portant un autre alphabet. Cela ne complique pas beaucoup le travail des correspondants. Pour le décrypteur, cela ne change pas la longueur de la clef. S'il ne s'aperçoit pas alors que les répétitions se localisent dans les deux parties du télégramme sans chevaucher du commencement sur la fin (et encore en choisissant les alphabets on peut mettre aux mêmes places des lettres fréquentes et avoir des répétitions tout en changeant l'alphabet), il est complètement brouillé dans les comptes de fréquence.

Nous citons ce système parce qu'il a reçu des applications, en particulier dans les appareils à cadran. En divisant le cadran intérieur en un certain nombre de secteurs superposables, et en faisant jouer par exemple, sous forme de carton mince, ces secteurs l'un par rapport à l'autre, on dispose l'alphabet en séries de 4 ou 5 lettres dont on change facilement l'ordre relatif (M. Pasanisi est l'inventeur d'un appareil d'un type analogue).

C'est par l'étude des répétitions, dues à des maladresses de chiffreur, que nous avons vu obtenir les traductions de documents chiffrés par cette méthode, où d'ailleurs les indications destinées à indiquer l'ordre des secteurs (numérotés), la position de départ du cadran mobile par rapport au cadran fixe, et le décalage régulier à faire subir au cadran formaient un ensemble d'aspect spécial, attirant l'attention, et permettant d'essayer de grouper certains cryptogrammes pour les étudier ensemble. Le sujet serait trop long à traiter ici en détail, et n'aurait d'ailleurs pas l'intérêt d'un exemple d'ordre général. Nous n'y insisterons donc pas.

CHAPITRE IX

RECONSTITUTION D'ALPHABETS

Dans l'étude des substitutions à double clef, nous avons d'abord examiné l'emploi d'alphabets type Vigenère. Puis nous avons examiné les tableaux ayant un alphabet incohérent pour base, mais toujours du type Vigenère, avec un décalage d'une lettre en passant d'un alphabet à l'autre. Enfin, nous avons parlé des alphabets incohérents non parallèles. Fort souvent on ne sait pas *a priori* à quel type on a affaire; on reconstitue la traduction des lettres de quelques alphabets, parfois par des moyens réguliers, parfois grâce à une heureuse coïncidence (par exemple travail sur des débuts de télégrammes à clef longue, possession d'un fragment du texte clair d'un cryptogramme, etc.), et comme les tableaux de concordance sont souvent écrits par le décrypteur comme déchiffrants, l'ordre alphabétique étant celui de l'alphabet du cryptogramme, tandis que dans les tableaux de Vigenère l'ordre alphabétique est celui des lettres du clair, rien n'indique à première vue que les divers alphabets proviennent d'un tableau. Il y a lieu de rechercher si les divers alphabets sont parallèles ou non.

Alphabets repère ordonné. — Si l'alphabet repère du tableau (ou de la règle) est ordonné normalement, le redressement est facile.

Soient par exemple les résultats ci-après, où I est l'alphabet du cryptogramme, II et III deux alphabets de traduction donnant les lettres du clair pour deux périodes du déchiffrement :

I. — a b c d e f g h i j k l m n o p q r s t u v w x y z
II. — E A D N W L O K C M T B Q S P Y R V X H Z G J U I F
III. — L H K U D S V R J T A I X Z W F Y C E O G N Q B P M

En se donnant la peine de rétablir les tableaux de déchiffrement :

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
b l i c a z v t y w h f j d g o m q n k x r e s p u

et

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
k x r e s p u b l i c a z v t y w h f j d g o m q n

on voit que l'alphabet du cryptogramme est unique et simplement décalé.

Alphabet repère incohérent. — Mais, si, tout en ayant un tableau carré (ou un système analogue produisant un décalage d'alphabet sans intervertir les lettres), on n'a pas pris un alphabet repère en ordre normal, l'expérience que nous venons de faire ici ne réussira pas. Il y a pourtant intérêt à trouver, quand il existe, le dispositif qui donne toute la série des alphabets, par exemple le tableau unique.

Nous allons étudier le problème ainsi posé : reconstituer dans les alphabets un ordre qui permette (quand c'est possible) de ramener une série de tableaux de concordance reconstitués au cours du déchiffrement à un tableau carré, règle de Saint-Cyr ou cadran.

Ce problème se traite, en considérant que la distance linéaire ou angulaire des lettres de l'alphabet de base du tableau carré (ou du cadran) entre elles doit leur permettre de coïncider, dans toutes les positions que prend cet alphabet à mesure qu'il se décale, avec les lettres de l'alphabet du clair qui sert de repère. La distance entre deux lettres d'un même alphabet dans une des positions ne peut pas varier lorsque l'alphabet passe à une deuxième position. On en conclut que si un certain nombre de lettres séparent dans l'alphabet les caractères placés dans

une des positions en face de deux lettres repères du clair, c'est ce même nombre de lettres qui séparera les caractères placés en face de ces mêmes lettres repères dans une autre position. Autrement dit, si l'on a les traductions dans deux positions de l'alphabet :

clair	position I	position II
A	q	e
B	p	s
C	e	f
.	.	.

on aura dans l'alphabet base du tableau le même nombre de lettres entre q et p qu'entre e et s, entre p et e qu'entre s et f, etc.

Soient alors les résultats du déchiffrement :

I. — a b c d e f g h i j k l m n o p q r s t u v x y z
II. — D E C K U P X Y G Q R H I A J L B N M T O F Z S V
III. — J S V L K B T O Y F Z Q R P I D M X C U A N G H E

Choisissons au hasard un bigramme dans I, soit ae. Les lettres correspondantes dans II sont DU. L'intervalle de DU dans III correspondra à la fois à celui de DU dans II et de pt dans I, ou de LT dans II; etc... celui de pt dans I est donc égal à celui de LT dans II. Celui de LT dans III est égal à ce dernier, mais égal aussi à celui de dg dans I et de KX dans II. Nous écrirons alors ces intervalles tous égaux sous la forme ci-dessous, et, quand nous aurons considéré un certain nombre d'intervalles égaux, diviseur du nombre de lettres de l'alphabet, et au plus égal à celui-ci, nous retomberons sur notre premier intervalle. Le problème de placement de toutes les lettres ne sera résolu que si notre premier intervalle est choisi de manière à ne pas retrouver le 1er bigramme avant l'emploi de tous les intervalles. S'il en est autrement, si l'on ferme

trop tôt le cycle, on essaiera un intervalle différent avec un autre bigramme

ae, pt, dg, er, tv, gj, rl, vy, jb, lz, yc, bs,
DU, LT, KX, UN, TF, XQ, NH, FS, QE, HV, SC, EM,
zq, cf, sn, qu, fh, ni, ux, hk, im, xo, ka, mp,
VB, CP, MA, BO, PY, AG, OZ, YR, GI, ZJ, RD, IL,
od, ae
JK, DU

Pour avoir l'alphabet, plaçons les bigrammes à la suite l'un de l'autre, dans l'ordre tel que la 1re lettre de l'un soit la même que la 2e lettre de celui qui le précède, ae, er, rl, etc... et considérons la 1re lettre de chaque bigramme

a e r l z q u x o d g j b s n i m p t v y c f h k
D U N H V B O Z J K X Q E M A G I L T F S C P Y R

On voit, en considérant I, II et III, que les lettres a e r l représentent bien deux séquences dans le même ordre DUNH et JKXQ, etc...

On a ainsi obtenu une solution, entre beaucoup, permettant de refaire les opérations que l'on pourrait faire sur les vrais alphabets du chiffreur, alors qu'on ignore en général ceux-ci.

Lorsque, au lieu d'avoir un alphabet repère différent de l'alphabet base du tableau, cet alphabet est le même, et qu'on a un tableau carré avec alphabet incohérent tel que

	M	B	O	K	L	A	C	...
M	m	b	o	k	l	a	c	
B	b	o	k	l	a	c	f	
O	o	k	l	a	c	f	h	
K	k	l	a	c	f	h	w	
L	l	a	c	f	h	w	x	etc..

les deux lignes de bigrammes, majuscules et minus-

cules, présentent la même suite de lettres avec un décalage.

Soient les résultats de déchiffrement :

I. — a b c d e f g h i j k l m n o p q r s t u v x y z
II. — Q P E N U R I L Y M Z O C V S F G X T H J K B A D
III. — E S F G R H J K M B A Z P I D T U L N V X Y O C Q

On forme les séquences de bigrammes de même intervalle

ap, zc, oa, bz, mo, yb, km, ly, xk, jl, ix, vj, hi,
QF, DE, SQ, PD, CS, AP, ZC, OA, BZ, MO, YB, KM, LY,

rv, uh, gr, nu, tg, fn, et, qf, de, sq, pd, cs, ap
XK, JL, IX, VJ, HI, RV, UH, GR, NU, TG, FN, ET, QF

et on en tire l'alphabet, tant du tableau que de la colonne qui le borde à gauche où l'on prend la lettre du clair :

A P D E T G R V J L Y B Z C S Q F N U H I X K M O
q f n u h i .....
e t g r v .....

Rappelons que ce n'est pas forcément l'alphabet du chiffreur.

Reconstitution du mot clef d'un alphabet. — Quand on est sûr *a priori* que l'alphabet du tableau est le même que l'alphabet de la colonne de gauche (lettres du clair), on peut se contenter d'un seul tableau de correspondance pour rétablir l'alphabet.

Soit le tableau déchiffrant :

I. — a b c d e f g h i j k l m n o p q r s t u v x y z
II. — F K L H G M N P Q S T V Y Z J X U I A E C D B R O

Des séquences telles que MNPQ suggèrent l'idée d'un alphabet construit sur un mot clef. Dans ce cas en reconstituant des séquences de lettres de l'alphabet, nous aurons

des chances de reconstituer un ordre des lettres où le mot clef réapparaîtra suivi de la suite des lettres non employées. Partons donc de PQ, qui correspond à hi; HI donne comme intervalle équivalent à celui de hi, dr, etc...

PQ, HI, DR, VY, LM, CF, UA, QS, IJ, RO, YZ, MN, FG, AE, ST, JK, OB, ZX, NP, GH, ED, TV, KL, BC, XU, PQ

d'où l'alphabet (PQ, QS, ST)...

P Q S T V Y Z X U A E D R O B C F G H I J K L M N

ou, en le reversant :

B O R D E A U X Z Y V T S Q P N M L K J I H G F C

Autre procédé pour retrouver l'alphabet de base. — Ces procédés sont surtout intéressants quand on tombe sur des substitutions doubles dans lesquelles les alphabets semblent d'abord incohérents. On a en effet employé de telles substitutions avec des tableaux qu'on modifiait peu à peu avec le temps ou avec le nombre des télégrammes : il est donc bon de chercher alors à se rapprocher le plus possible des conditions où sont placés les correspondants, et de ne point se contenter des tableaux de concordance obtenus pour chaque alphabet qui permettent bien de traduire les premiers cryptogrammes, mais où aucune loi n'apparaît, ce qui nécessite un travail entièrement nouveau pour chaque texte. On n'aboutit d'ailleurs pas toujours à un résultat, car les alphabets peuvent être réellement différents et irréductibles.

La difficulté d'application de la méthode porte presque toujours sur ce fait, qu'un certain nombre de lettres rares manquent au tableau de concordance établi au cours du chiffrement, et ne permettent pas de poursuivre la chaîne des bigrammes. Dans certains cas, on peut tirer parti de remarques sur la constitution des alphabets pour obtenir quand même des solutions.

Soit par exemple la correspondance :

I. — z d r u x o b c f g h i j k e l m a n p y q v s t
II. — A B C D E F G H I J K L M N O P Q R S T U V X Y Z

où l'alphabet en majuscules est l'alphabet du clair, celui en minuscules l'alphabet du cryptogramme. Dans la position relative où nous les avons placés, et en tournant la page de 90° de manière à mettre A en haut, on peut les considérer comme écrits dans un tableau carré, II formant l'alphabet repère, c'est-à-dire la colonne de gauche placée en face du tableau et I jouant le rôle d'une colonne du tableau.

Par hypothèse, nous savons à cause des habitudes du chiffreur que l'alphabet unique du tableau carré est fait sur un mot clef, suivi des lettres non employées placées en ordre direct ou en ordre inverse. Par suite, en dehors du mot clef, on pourra trouver des séquences telles que MNP (ordre direct) ou PNM (ordre inverse), mais on ne pourra pas trouver MPN ni NPM.

Bien entendu, si l'on a le tableau de correspondance complet comme nous l'avons inscrit ci-dessus, la méthode exposée plus haut s'applique. Mais, pour arriver à remédier aux manques, nous allons procéder aux développements ci-après.

Il s'agit d'un tableau carré. Si l'alphabet I était le 1er à gauche du tableau, ses lettres seraient les mêmes que celles de la colonne de lettres repères (où on lit la lettre du clair). Ce n'est pas le cas ici.

Si l'alphabet I était le 2e du tableau, il serait décalé de I par rapport au clair, comme on le voit ci-dessous sur ce schéma :

	1	2	3	4	5	
M	m	p	r	v	t	
P	p	r	v	t	z	
R	r	v	t	z	a	
V	v	t	z	a	m	
T	t	z	a	m	x	etc...

Alors la lettre qui correspondait à A, c'est-à-dire z, se placerait au-dessous de A dans l'alphabet (comme p, qui dans l'alphabet 2 correspond à M, s'écrit au-dessous de M dans l'alphabet MPRV); au-dessous de Z on aurait T (qui traduit z), etc... et l'alphabet serait

A Z T P L I F O E X V Q M J G B D U Y S N K H C R A

Nous n'y voyons pas apparaître de mot clair clef; des séquences telles que FUE, MJG, sont contraires à ce que nous savons de la formation de l'alphabet : hypothèse à rejeter.

Si I était le 3e alphabet, z viendrait à deux rangs au-dessous de A (comme r par rapport à M dans le schéma). On aurait alors après avoir écrit les 13 premières lettres à deux rangs de distance A . Z . P ...., à remplir les intervalles avec les dernières, toujours de 2 en 2. L'alphabet serait :

A J Z G T B P D L U I Y F S O N E K X H V C Q R M A

Il est encore à rejeter (BPD, XHV,...).

Plaçons les lettres de 3 en 3 :

1	2	3	4	5	6	7	8	9	10	11	12	13
A	U	X	Z	Y	V	T	S	Q	P	N	M	L
14	15	16	17	18	19	20	21	22	23	24	25	
K	J	I	H	G	F	C	B	O	R	D	E	

Cette fois nous avons le bon alphabet. Si on ne l'eût pas eu, on aurait continué les essais.

Or, cette méthode s'applique même quand il y a des trous, à condition de faire quelques hypothèses sur la place des différentes têtes de séquences, hypothèses basées sur la constitution de l'alphabet.

Soit la correspondance :

I	g	.	k	m	f	p	q	.	u	.	.	d	y
II	A	B	C	D	E	F	G	H	I	J	K	L	M
	h	b	z	.	c	i	r	l	e	.	.	s	
	N	O	P	Q	R	S	T	U	V	X	Y	Z	

Manquent dans l'alphabet du cryptogramme les lettres a j n o t v x.

Opérons comme pour former l'alphabet avec les lettres juxtaposées; on a des séquences brusquement interrompues :

AGQ ... TRCK ... VEFPZSIULDMY ... NH ... OB.

Elles suffisent à nous montrer que l'alphabet par juxtaposition ne donne pas de mot clef clair, et a des séquences, (SIU, RCK,...) inadmissibles.

Essayons encore les alphabets décalés en ordre croissant, en commençant par la grande séquence.

1	2	3	4	5	6	7	8	9	10	11	12	13
V		E		F		P		Z		S		I

14	15	16	17	18	19	20	21	22	23	24	25
	U		L		D		M		Y		

Cherchons à intercaler T R C K par exemple. Pour ménager entre T et R une séquence alphabétique, il faut y placer S, ce qui donnera ZTSRICUKL. Cela ne peut convenir (ICUK). La solution n'est pas bonne.

Nous faisons grâce au lecteur des essais sur les intervalles 3, 4, et 5.

L'intervalle 6 donne :

1	2	3	4	5	6	7	8	9	10	11	12	13
V				D	S	E				M	I	F

14	15	16	17	18	19	20	21	22	23	24	25
			Y	U	P					L	Z

Déjà DSE, IZV sont de nature à faire rejeter l'hypothèse. Mais où placer

T. . . . . R. . . . . C. . . . . K

On n'aurait encore que des amorces de séquences incohérentes. Essayons l'intervalle 7 :

1	2	3	4	5	6	7	8	9	10	11	12	13
V		Y	Z			L	E			S		
14	15	16	17	18	19	20	21	22	23	24	25	
D	F			I			M	P			U	

Nous avons des séquences qui semblent pouvoir être bonnes. D F . . I . . M P . . U V . Y Z, et des éléments LE et S d'un mot français. Voyons ce que nous pourrions faire de TRCK. En plaçant C devant D, ce qui sera sa place si cette lettre n'est pas dans le mot clef, on a CDF, KMP, et, en comptant par 7 places en remontant à partir de C, RLE, TUV.

V . Y Z . R L E . . S . C D F . . I . K M P . T U .

La séquence AGQ se placera en mettant Q entre P et T, G viendra après F. — H de NH se placera entre G et I, et dès lors l'alphabet sera reformé.

V X Y Z O R L E A N S B C D F G H I J K M P Q T U

Nous fermerons ici cette digression sur la remise des alphabets en ordre; le sujet a été traité en détail par le grand établissement d'études cryptographiques américain de River Bank, dans des notes qui nous ont apporté un secours important au cours de nos études sur ce sujet.

CHAPITRE X

ETUDE D'UN SYSTÈME DE SUBSTITUTION CLASSIQUE
SYSTÈME BAZERIES

Les systèmes de substitution ont donné lieu à de très nombreuses et intéressantes études sur des procédés nouveaux, que leurs auteurs ont présentés souvent comme indéchiffrables. Nous ne développerons dans ce chapitre ni la description de ces procédés ni les méthodes qui ont permis de décrypter beaucoup d'entre eux. Toutefois, pour donner un exemple d'un système fort élégant, et pour indiquer comment la connaissance du matériel employé au chiffrement peut influer sur la résistance des cryptogrammes, en apportant des considérations tout autres que celles, purement théoriques, qui servent souvent de base aux prétentions des inventeurs, nous nous étendrons sur le système Bazeries.

Le capitaine (depuis commandant) Bazeries, lorsqu'il proposa ce système aux administrations publiques, s'était révélé comme un cryptologue extrêmement perspicace, et ses ouvrages en font foi. Il présenta son appareil comme donnant des cryptogrammes indéchiffrables. Pourtant il essuya un refus. Les motifs en furent probablement divers. Il est à croire qu'en particulier la question de résistance des cryptogrammes au décryptement ne fut pas considérée par les commissions d'examen dans les conditions d'emploi parfait où M. Bazeries l'avait établie, mais en tenant compte de circonstances où de nombreux chiffreurs peu exercés auraient à manipuler dans des conditions matérielles difficiles un instrument de maniement délicat. Dans la suite, l'auteur se montra dans ses

œuvres fort dur pour *la routine des services officiels*. On trouvera dans les ouvrages de Viaris une méthode qui permet de considérer comme mal fondée sa prétention à l'indéchiffrabilité. Nous avons également fait état, dans les explications qui vont suivre, de remarques et de procédés, exposés par divers cryptologues, en particulier d'une étude du général Cartier.

L'appareil Bazeries se compose d'un axe sur lequel sont enfilées des rondelles portant des numéros de 1 à 20 : qu'on se figure un cadenas à lettres sans anse. Sur chaque rondelle est gravé un alphabet de 25 lettres (pas de w); un seul de ces alphabets est normal. Les autres sont incohérents et tous différents. On juxtapose ces alphabets en enfilant les rondelles sur l'axe dans un ordre fixé par la clef. Chaque rondelle porte un numéro. On forme en répétant un mot clef juqu'à ce qu'on ait 20 lettres, ou en coupant à 20 lettres une phrase clef, une clef littérale de 20 lettres qu'on transforme en clef numérique en numérotant les lettres suivant leur ordre relatif dans l'alphabet, et on place les rondelles sur l'axe de manière que la suite de leurs numéros reproduise la suite des nombres de la clef. L'appareil est alors prêt à fonctionner : on a le choix entre autant d'ordres différents pour les rondelles qu'on peut faire de permutations avec 20 termes, soit $1 \times 2 \times 3... \times 18 \times 19 \times 20 = 2$ quintillions environ.

Pour chiffrer, on place sur une même génératrice du cylindre formé par la pile des rondelles la suite des 20 premières lettres du texte clair. Comme chaque lettre ne figure qu'une fois sur chaque rondelle, la position de chacune d'elles est parfaitement définie. Si l'on considère le cylindre, et les 25 génératrices suivant lesquelles s'alignent les 25 lettres de chaque alphabet, on lit sur une de ces génératrices le début du texte clair, sur les 24 autres des suites de lettres qui, dans la presque totalité des cas, sont incohérentes. On choisit pour remplacer les lettres du clair les 20 lettres qui figurent sur une génératrice quelconque : on a donc le choix entre 24 représentations différentes. Une fois le début du cryptogramme écrit, on amène sur une génératrice les 20 lettres suivantes du texte clair, et

on les chiffre par les 20 lettres d'une génératrice quelconque, dont la distance à la génératrice du clair sera de préférence différente de celle de la génératrice qui a servi à chiffrer les 20 premières lettres, etc... Pour déchiffrer, on amène les 20 premières lettres du cryptogramme sur une génératrice, et une rapide inspection des 24 autres nous révèle celle où la suite des lettres donne un sens, qui est le texte clair. On continue sur les tranches suivantes.

Le système, avec le nombre des combinaisons clefs et l'arbitraire dans le choix des génératrices, qui donne 24 textes différents possibles pour une même tranche de cryptogramme, présente une sécurité qui semble absolue à l'inventeur. Elle l'est peut-être si l'appareil demeure secret pour le décrypteur. Mais dans le cas où, par suite de circonstances qu'il faut toujours considérer comme normales avant d'adopter un système pour la Guerre ou la Diplomatie, le décrypteur peut avoir une description de l'appareil et la copie des alphabets, la recherche d'une traduction devient possible, car il ne s'agit plus que de trouver la clef, et on peut y parvenir.

Pour les considérations qui vont suivre, nous ne considérerons qu'un appareil à 10 rondelles. On peut obtenir une disposition commode pour l'étude en écrivant les 10 alphabets (2 fois chacun à la suite l'un de l'autre) sur 10 bandes de papier que l'on fait jouer dans les fentes pratiquées dans une grande feuille.

Les 10 alphabets que nous adopterons pour ce cryptographe (appareil à chiffrer) parmi les 20 de Bazeries, sont :

1	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z
2	b	c	d	f	g	h	j	k	l	m	n	p	q	r	s	t	v	x	z	a	e	i	o	u	y
3	a	e	b	c	d	f	g	h	i	o	j	k	l	m	n	p	u	y	q	r	s	t	v	x	z
4	z	y	x	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a
5	y	u	z	x	v	t	s	r	o	i	q	p	n	m	l	k	e	a	j	h	g	f	d	c	b
6	e	v	i	t	z	l	s	c	o	u	r	a	n	d	b	f	g	h	j	k	m	p	q	x	y
7	f	o	r	m	e	z	l	s	a	i	c	u	x	b	d	g	h	j	k	n	p	q	t	v	y
8	g	l	o	i	r	e	m	t	d	n	s	a	u	x	b	c	f	h	j	k	p	q	v	y	z
9	h	o	n	e	u	r	t	p	a	i	b	c	d	f	g	j	k	l	m	q	s	v	x	y	z
10	i	n	s	t	r	u	e	z	l	a	j	b	c	d	f	g	h	k	m	o	p	q	v	x	y

Nous ne nous arrêterons pas à rappeler une étude de Viaris destinée à retrouver l'ordre des alphabets, c'est-à-dire la clef, quand le décrypteur connaît la distance de la génératrice du texte clair à la génératrice du texte cryptographié. Nous ne voyons pas comment, dans la pratique, où le chiffreur ne fera pas même attention à ce détail, un tel cas pourrait se réaliser :

Nous signalerons par contre l'observation suivante de Viaris. Composons la génératrice du clair uniquement de E, les deux génératrices voisines seront (en prenant dans l'ordre des disques 1 à 10) :

f i b d a v z m u z; — soit 1 a, 1 b, 1 d, 1 f, 1 i, 1 m, 1 u, 1 v, 2 z.

g o c c j i l t r l; — soit 2 c, 1 g, 1 i, 1 j, 2 l, 1 o, 1 r, 1 t,

Cet exemple sur deux génératrices montre que la composition alphabétique varie d'une génératrice à l'autre, et définit pour ainsi dire cette génératrice quel que soit l'ordre des rondelles, qui ne peut influer que sur l'ordre des lettres, mais non sur leur présence.

Un e du texte clair ne sera pas, sur une génératrice donnée, représenté par n'importe quelle lettre, même pas par une lettre quelconque choisie entre 10 (10 alphabets), mais par une lettre choisie entre 8 ou 9 seulement (puisque sur plusieurs rondelles on trouvera la même lettre). Avec le cryptographe Bazeries complet à 20 disques, une lettre d'une génératrice donnée arrive à ne pouvoir être remplacée que par une autre lettre à déterminer entre 12 ou 13 seulement sur les 24 restantes de l'alphabet.

Dans les explications qui vont suivre, nous considérerons le cryptographe disposé pour chiffrer; les rondelles empilées suivant une clef inconnue, les 10 lettres du clair sur une même génératrice que nous appellerons ligne 1, la génératrice voisine sera dite ligne 2, etc...

Soit le texte :

ncximzusls yhloertxvz iqjosvejgu cuvhfxxufu
vigeufufxa tykgqbne

Nous avons de sérieux motifs de penser qu'il contient le mot : DIVISION, et nous allons l'y chercher.

Supposons que le mot DIVISION ait été chiffré avec la ligne 2 (génératrice voisine de celle où figure le texte clair); dans ce cas, il aura été chiffré avec les lettres suivant immédiatement, sur chaque rondelle, la lettre du mot clair DIVISION. Nous ne savons sur quelle rondelle on a pris D; si c'est sur la rondelle 1, D sera remplacé par e; si c'est sur la rondelle 2, par f; si c'est sur 3, par f encore, etc..., et, si nous plaçons l'une après l'autre les lettres qui suivent D sur les 10 rondelles, nous aurons :

D e f f c c b g n f f

Faisons le même travail pour toutes les lettres du mot DIVISION. Le tableau des lettres qui, pour les 10 rondelles, suivent chacune des lettres du mot clair, est :

	1	2	3	4	5	6	7	8	9	10
D	e	f	f	c	c	b	g	n	f	f
I	j	o	o	h	q	t	c	r	b	n
V	x	x	x	u	t	i	y	y	x	x
I	j	o	o	h	q	t	c	r	b	n
S	t	t	t	r	r	c	a	a	v	t
I	j	o	o	h	q	t	c	r	b	n
O	p	u	j	n	i	u	r	i	n	p
N	o	p	p	m	m	d	p	s	e	s

On voit alors que si DIVISION a été chiffré avec la 2e ligne, les seules lettres qui peuvent représenter D sont b, c, e, f, g et n. Nous formerons d'après le tableau ci-dessus pour les lettres de DIVISION le tableau des lettres qui peuvent représenter chacune d'elles en ne les faisant figurer qu'une fois chacune, même quand elles figurent plusieurs fois ci-dessus.

D	I	V	I	S	I	O	N
b	b	i	b	a	b	i	d
c	c	t	c	c	c	j	e
e	h	u	h	r	h	n	m
f	j	x	j	t	j	o	o
g	n	y	n	v	n	p	p
n	o		o		o	r	s
	q		q		q	u	
	r		r		r		
	t		t		t		

Promenons sous notre cryptogramme, après avoir écrit les lettres à intervalles égaux à ceux de ce tableau, une feuille de papier portant ce tableau lui-même. Arrêtons-nous à chacune des lettres qui peuvent donner D en clair, c'est-à-dire aux b, c, e, f, g, n; voyons si la première lettre à droite est comprise dans la liste de celles qui peuvent nous donner I en clair. Si non, allons plus loin. Si oui, vérifions la 3e lettre, etc...

Nous ne trouvons pas le moyen de faire coïncider avec une séquence de 8 lettres du cryptogramme une séquence formée de 8 lettres du tableau précédent prélevées à raison d'une par colonne dans l'ordre des colonnes. Nous ne pouvons même pas faire coïncider 4 lettres.

Concluons que le mot DIVISION n'était pas chiffré avec la 2e ligne.

Nous avons pu, pour aller plus vite, charger des aides de faire simultanément ce travail pour chacune des lignes. Or, voici les travaux relatifs à la ligne 5 :

	1	2	3	4	5	6	7	8	9	10
D	h	j	i	z	u	h	k	u	k	k
I	m	b	l	e	m	s	b	t	f	r
V	a	e	e	r	o	l	r	l	h	n
I	m	b	l	e	m	s	b	t	f	r
S	x	z	z	o	q	r	u	b	z	e
I	a	b	l	e	m	s	b	t	f	r
O	s	c	m	k	n	n	z	m	r	x
N	r	s	q	j	e	g	v	x	t	u

et voici le tableau des lettres pouvant représenter DIVISION placé dans une position où il semble pouvoir s'appliquer au cryptogramme.

..... s l s y h l o e r t x v z i q ...

D	I	V	I	S	I	O	N
h	b	a	b	b	b	c	e
i	e	e	*e*	e	e	k	g
j	f	h	f	o	f	m	j
k	*l*	l	l	q	l	n	q
u	m	n	m	*r*	m	r	r
z	r	*o*	r	u	r	s	s
	s	r	s	x	s	*x*	t
	t		t	z	*t*	z	u
							v
							x

Cherchons alors à vérifier, en appliquant la clef à d'autres tranches du télégramme, si la solution est bonne ou s'il ne s'agit que d'une coïncidence. Dans ce dernier cas on continuerait les essais, jusqu'à opérer avec d'autres mots probables si les tentatives de placer DIVISION sur les 24 lignes ne donnaient rien.

Voyons de quelles rondelles viennent les lettres qui nous donnent la solution. h pour D vient de la rondelle 1 (alphabet 1), et, en continuant, nous trouvons la clef :

? 1 3 5 4 6 8 10 7 ?

Nous n'avons eu aucune incertitude, chacune des lettres ne s'étant rencontrée, dans cet exemple, que sur une seule rondelle. Mais si, par exemple, nous avions trouvé que le D était représenté par K, nous eussions eu à hésiter entre les 3 rondelles 7, 9 et 10 qui donnent K sur la 5e ligne quand d est sur la première. On peut donc, si plusieurs lettres donnent des incertitudes, hésiter entre plusieurs clefs. On ferait des essais sur chacune d'elles analogues à celui qui va suivre.

Plaçant les rondelles ou les bandes de papier par les-

quelles nous les représentons dans cet ordre, la 1re tranche nous donne sur la 3e ligne au-dessus de celle où nous lisons le cryptogramme ncximzusls.

? ATROISIE ?

On en déduit le texte : La troisième division se portera demain matin sur Reims. stop. départ à 7 heures, et la clef complète,

2 1 3 5 4 6 8 10 7 9

car dans l'autre combinaison possible (la rondelle 9 en tête), la lettre n du cryptogramme n'est pas à la 3e place par rapport à L du texte clair, comme elle l'est dans la rondelle 2.

Nous avons eu ici un mot probable commode et long. Quand on n'en a pas, on peut chercher simplement un trigramme ou un polygramme fréquent : ement, eraient, ième, les, etc... On peut alors trouver plusieurs solutions, dont les unes s'éliminent *a priori* comme indiquant deux fois l'emploi d'une même rondelle pour une même tranche par exemple, et dont les autres s'éliminent (s'il y a lieu, car le mot peut en effet revenir plusieurs fois et donner plusieurs solutions) au cours des essais sur les autres tranches avec la clef essayée. Nous n'insisterons pas, ayant montré que malgré les quintillions de combinaisons théoriques, il n'était pas impossible de trouver une solution par la méthode du mot probable.

Mais la méthode analytique elle-même peut s'appliquer. Soit le cryptogramme :

sxbapztplf sprzaradoa dmrt

Supposons que la première rondelle enfilée sur l'axe soit celle de l'alphabet 1. Nous essaierons d'y accoler successivement les 9 autres rondelles en plaçant à hauteur de s du 1er alphabet les x des 9 autres, et cherchant chaque fois parmi les bigrammes fournis par les 24 généra-

trices ceux qui sont capables de commencer une phrase française. A ces bigrammes nous essaierons d'accoler une 3e lettre, obtenue en plaçant le b des 8 rondelles restantes sur la même ligne que sx, et ainsi de suite. Ces essais seraient rapides avec l'appareil : nous allons développer le cylindre et en faire un tableau :

Alpb. 1 s t u v x y z a b c d e f g h i j k l m n o p q r
Alph. 2 x z a e i o u y b x d f g h j k l m n p q r s t v

Il n'y a que les bigrammes ve, ef, or qui soient à retenir. Cherchons les trigrammes en considérant tous les autres alphabets, en ne retenant que les 3 lignes correspondant aux bigrammes retenus, et en ayant soin de placer le b sur la même ligne (génératrice) que sx, on a :

1	2	3	4	5	6	7	8	9	10
s	x	b	b	b	b	b	b	b	b
v	e	f	y	z	h	h	h	f	f
e	f	m	p	q	e	y	q	v	v
o	r	x	f	g	r	i	s	t	z

Il n'y a à retenir que org et ori (on peut négliger ort, peu probable au début d'une phrase, quitte à le reprendre si on ne trouve rien autrement) :

1	2	5	3	4	6	7	8	9	10
s	x	b	a	a	a	a	a	a	a
o	r	g	t	e	c	e	t	u	u

Nous supposerons que, pour certains motifs, nous sommes sûrs qu'il ne s'agit pas d'orge dans le cryptogramme. La solution 1, 2, 5... ne donne rien.

1	2	7	3	4	5	6	8	9	10
s	x	b	a	a	a	a	a	a	a
o	r	i	t	e	m	c	t	u	u

On ne peut trouver de tétragramme convenable. Nous renoncerons à placer la 2e rondelle à côté de la première,

et nous essaierons la 3e. Nous passerons sur ces essais pour arriver tout de suite à l'hypothèse d'une clef commençant par 1, 5...

Alph. 1 s t u v x y z a b c d e f g h i j k l m n o p q r
Alph. 5 x v t s r o i q p n m l k e a j h g f d c b y u z

Bigrammes retenus : el, ge, ha, ob, qu (nous négligeons ut, qui pourrait pourtant donner *utile*, pour ne pas alourdir les explications).

Recherchons les trigrammes :

1	5	2	3	4	6	7	8	9	10
s	x	b	b	b	b	b	b	b	b
e	l	p	m	p	e	y	q	v	v
g	e	r	p	n	i	o	o	y	y
h	a	s	u	m	t	r	i	z	i
o	b	i	x	f	r	i	s	t	z
q	u	u	a	d	n	u	u	a	a

Nous avons beaucoup de trigrammes admissibles : ele (éléments) gen (général) hat (hâtez-vous) obs (obstacle). On les essaierait successivement. Pour abréger, commençons les essais par qua; on a 3 solutions possibles... 1. 5. 3..., 1, 5. 9..., 1. 5. 10...

1	5	3	2	4	6	7	8	9	10
s	x	b	a	a	a	a	a	a	a
q	u	a	x	c	u	l	n	t	z

Nous allons continuer sur 1. 5. 3., pour revenir en cas d'échec à 1. 5. 9. et 1. 5. 10., ce qui ira très vite, puisque pour les essais pour 1. 5. 9 et 1. 5. 10, nous aurons déjà les lettres x c u l n z, x c u l n t des colonnes 2 4 6 7 8 9 et 10, et que nous n'aurons qu'à chercher la lettre de la colonne 3, qui sera x (correspondant à a sur la ligne 1).

1	5	3	8	2	4	6	7	9	10
s	x	b	a	p	p	p	p	p	p
q	u	a	n	m	r	k	k	r	m

1	5	3	9	2	4	6	7	8	10
s	x	b	a	p	p	p	p	p	p
q	u	a	t	m	r	k	k	j	m

Continuons sur 1.5.3.9.4...

1	5	3	9	4		2	6	7	8	10
s	x	b	a	p		z	z	z	z	z
q	u	a	t	r		v	i	m	v	a

Nous arrivons à :

1	5	3	9	4	6	8	10	7	2
s	x	b	a	p	z	t	p	l	f
q	u	a	t	r	i	e	m	e	c

En vérifiant sur les autres tranches, nous trouvons que la solution est bonne : quatrième corps est attaqué.

Cette méthode peut conduire à des essais très nombreux ; mais, si l'on veut gagner du temps sans exiger la présence de cryptologues qualifiés, ils peuvent être faits par des aides méthodiques, commençant simultanément l'étude par chacun des alphabets, comme nous l'avons fait pour l'alphabet 1, et, sauf en cas d'erreurs sur le texte comme il s'en produit par exemple lors des réceptions par T. S. F. ils doivent aboutir.

Nous n'accorderons donc pas, malgré les quintillions de combinaisons possibles en théorie sur un appareil à 20 rondelles, une confiance illimitée au cryptographe Bazeries.

Il en est souvent de même pour les appareils ou machines à chiffrer présentées par des inventeurs. Ce n'est qu'après l'examen de la machine elle-même, et après avoir pu apprécier, en chiffrant des textes et en examinant le fonctionnement, les particularités de ce chiffrement, que l'on peut voir si par exemple la dépendance où une lettre se trouve de la précédente par suite de la construction ne vient pas substituer, dans le calcul, à un certain nombre de facteurs 26 (nombre de lettres), des facteurs 1 ou 2, une lettre étant forcément suivie d'une certaine ou de deux certaines autres et non d'une autre quelconque de l'alphabet.

Nous avons donné, avec un appareil supposé à 10 al-

phabets, l'exemple de marche à suivre dans la résolution des cryptogrammes Bazeries. La présence de 20 rondelles, le chevauchement du mot probable sur 2 tranches, l'addition au texte de nulles, l'emploi d'une clef de moins de 20 laissant de côté pour chaque lecture un certain nombre de rondelles suivant une loi donnée, viendraient compliquer la solution et allonger l'exposition. Notre but n'étant que de montrer qu'un système très bon en apparence peut prêter le flanc à des procédés de décryptement relativement simples, nous n'insisterons pas, et nous fermerons ici le chapitre des substitutions où les lettres sont soumises individuellement aux opérations de chiffrement.

CHAPITRE XI

SUBSTITUTIONS PAR POLYGRAMMES

Au lieu de remplacer les lettres d'un cryptogramme une à une par d'autres lettres, uniques, ou par des groupes de lettres ou de chiffres, on peut travailler sur des groupements de deux, trois, etc... lettres du cryptogramme. Les éléments à remplacer, au lieu de n'être qu'au nombre de 26 comme les lettres, sont en nombre beaucoup plus grand, et leur identification devient par suite beaucoup plus compliquée.

Nous indiquerons quelques-uns des procédés classiques employés pour les représentations par polygrammes.

En premier lieu, on conçoit l'emploi d'un tableau à double entrée, où les premières lettres des bigrammes figurent sur une ligne horizontale, les deuxièmes lettres sur une colonne verticale (ou vice versa), et où chaque case renferme un groupe de deux lettres, ou de 3 chiffres, représentant le bigramme défini par la colonne et la ligne.

	A	B	C	D	E	F .....
A	001	002	003	004	005	
B	027	028	029	030	031	
C	053	054	055	056	057	
D	079	080	081	082	083	
E	105	106	107	108	109	

Le bigramme CA est remplacé par 003, DE par 108, etc...

Quant aux bigrammes dont on entreprend la substitution, c'est-à-dire ceux du texte clair, on les formera en

coupant tout simplement le texte en tranches de 2 chiffres; toutefois, pour éviter les répétitions des bigrammes les plus fréquents, on pourra intercaler des lettres nulles dans le texte.

Si l'on tient à ce qu'aucune loi ne puisse apparaître dans la formation du tableau de correspondance (ici AA = 001, AB = 002, AC = 003, etc...) on aura recours à une table chiffrante et à une table déchiffrante. Mais ces tables seront longues, et l'on a inventé des systèmes pour masquer la correspondance qui peut exister entre les lettres des bigrammes et leurs représentations tout en ménageant les facilités de lecture.

On trouve, dans les ouvrages de cryptographie, des tableaux du genre de celui qui suit dont nous ne figurons qu'un fragment :

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
A	xz	kj	yj	hp	pl	el	vb	ci	dw	xn	zl	yp	vn	hh	cc
B	lp	qt	he	rs	ur	cr	zh	gv	wc	hl	yn	kt	wt	mc	kh
C	dx	mn	ao	nh	sf	gi	wl	mn	ah	gr	bz	hs	zu	ym	wu
D	km	yz	ry	fp	tr	ct	xe	jk	ny	po	gj	jr	pe	mo	vb
E	qu	hp	qg	jq	yq	ob	sa	nl	px	op	vs	af	xk	xr	uq

Ces tableaux sont composés de manière qu'un bigramme donné étant traduit par un bigramme, quand on passe du clair au chiffré, ce dernier bigramme, lu comme un bigramme de texte avec sa 1re lettre dans la 1re colonne et sa 2e dans la 1re ligne reproduit le bigramme primitif quand on passe du chiffré au clair. Aussi, en prenant le bigramme AF (A à la colonne de gauche, F à la ligne du haut), on voit qu'il est traduit par el. Quand on considère le bigramme EL (E à la colonne de gauche, L à la ligne du haut), on voit qu'il est traduit par af. De même AO = cc, CC = ao. On trouverait dans le tableau complet AA à la rencontre de la ligne X et de la colonne Z, AB à la rencontre de la ligne K et de la colonne J, etc... Les bigrammes sont donc tous réciproques, et on lit le tableau de la même manière au déchiffrement qu'au chiffrement.

On peut employer un système de réglettes mobiles tel que celui-ci, décrit dans un ouvrage américain :

A B C D E F G H I J K	alphabet fixe
A B C D E F G H I J K L M N O P	alphabets mobiles
M A R S E I L B C D F G H J K M	sur un coulisseau
P A R I S B C D E F G	alphabet fixe

Pour chiffrer un bigramme, on amène la 1re lettre du bigramme, lue sur l'alphabet mobile supérieur, en face de l'A repère de l'alphabet fixe supérieur; on cherche dans ce dernier alphabet la 2e lettre des bigrammes et, sous celle-ci, on lit les deux lettres des deux alphabets inférieurs.

Ainsi le bigramme EE se traduira par CS, EI par HE, EK par KG, AA par MP, etc...

On emploie aussi de simples tableaux carrés, à alphabets généralement intervertis, comme ci-après :

I.	A	B	C	D	E	F	G	H	I	J .....
II.	M	A	R	S	E	I	L	B	C	D .....
III.										
A	P	A	R	I	S	B	C	D	E	F .....
B	A	R	I	S	B	C	D	E	F	G .....
C	R	I	S	B	C	D	E	F	G	H .....
D	I	S	B	C	D	E	F	G	H	J .....
E	S	B	C	D	E	F	G	H	J	K .....
F	B	C	D	E	F	G	H	J	K	L .....

On chiffre un bigramme, lu dans la ligne I et la colonne III, par la lettre lue dans la ligne II sous la lettre de la colonne I, et par la lettre du tableau qui se trouve dans la colonne de la 1re lettre (où a déjà été lue la lettre de la ligne II) et dans la ligne de la 2e lettre. Ainsi IF se traduit par CK, CC par RS, etc...

Substitution orthogonale et diagonale par bigrammes. — Un système qui a été fort employé est le suivant. Avec

une clef, on forme un carré de 25 lettres. Soit la clef Londres :

L o n d r e s
a b c f g h i
j k m p q t u
v x y z

et le carré :

L A J V O
B K X N C
M Y D F P
Z R G Q E
H T S I U

On chiffre chaque bigramme dont les 2 lettres se trouvent dans une même colonne par les 2 lettres qui se trouvent au-dessous de ces 2 lettres (en transportant au besoin la 1re ligne au-dessous de la dernière) AR se chiffre par KT. On chiffre chaque bigramme dont les 2 lettres sont sur la même ligne par les deux lettres à droite : LA se chiffre par AJ. On chiffre chaque bigramme dont les lettres sont sur des lignes et des colonnes différentes par la lettre qui se trouve sur la ligne de la 1re lettre du bigramme et sur la colonne de la 2e, suivie de la lettre qui se trouve sur la ligne de la 2e et la colonne de la 1re (si l'on construit un rectangle sur le bigramme, on chiffre par les 2 lettres qui sont aux deux sommets non occupés du rectangle), AG se chiffre par JR, ON par VC. Lorsqu'en coupant le texte clair en bigrammes, on rencontre un redoublement de lettres, on introduit une nulle dans le texte.

Exemple : adresse..... se décompose en AD RE SK SE et se chiffre JY GZ TX UG.....

On désigne quelquefois ce système sous le nom de substitution orthogonale et diagonale par bigrammes.

Substitution par trigrammes. — Les substitutions peuvent porter sur des groupes de plus de 2 lettres. Pour tra-

vailler sur les trigrammes, on a proposé des tableaux tels que celui qui est figuré ci-dessous :

I.		A B C D E F G H I J K . . . . .
II.		M A R S E I L B C D F . . . . .
III.	IV.	
A	B	P A R I S B C D E F G . . . . .
B	O	A R I S B C D E F G H . . . . .
C	R	R I S B C D E F G H J . . . . .
D	D	I S B C D E F G H J K . . . . .
E	E	S B C D E F G H J K L . . . . .
F	A	B C D E F G H J K L M . . . . .
G	U	C D E F G H J K L M N . . . . .
H	X	D E F G H J K L M N O . . . . .
I	C	E F G H J K L M N O Q . . . . .
J	F	F G H J K L M N O Q T . . . . .
:	:	
:	:	
:	:	

On chiffre par exemple la 1re lettre du trigramme avec l'alphabet II en prenant la lettre du clair dans l'alphabet I, la 2e lettre avec l'alphabet IV en prenant la lettre du clair dans l'alphabet III, la 3e lettre en prenant la lettre placée à la rencontre de la ligne de la 2e lettre dans l'alphabet III avec la colonne de la 3e lettre du clair dans l'alphabet I.

AFI se chiffrera MAK, AFE : MAF, DIC : SCG

On voit que les moyens de réaliser un procédé de chiffrement par polygrammes sont nombreux. En rendant mobile un des alphabets qui figurent au-dessus ou à gauche des tableaux, en le déplaçant suivant une loi comme une réglette de Saint-Cyr, et en faisant dépendre de ce déplacement le choix de la colonne ou de la ligne de la lettre du polygramme chiffrée dans le tableau, on aura des substitutions à double clef. Les complications de ces systèmes peuvent donc conduire à des procédés extrêmement pénibles pour les études de décryptement.

Il semble pourtant qu'ils ne soient pas très employés, peut-être en raison de la nécessité d'employer des tableaux. Seul le procédé qui emploie le petit tableau de 25 lettres paraît avoir été d'un usage courant.

Le décryptement de tous ces systèmes est basé sur l'examen des fréquences. Il y a des tables de fréquence de bigrammes, et c'est sur elles qu'on s'appuiera pour des essais. Toutefois il y a lieu d'examiner avec soin, quand on connaît le principe du procédé employé, et qu'il ne s'agit par exemple que de retrouver une clef, quelles sont les conséquences de la méthode de chiffrement sur la constitution des substitutions. Ainsi dans la substitution par trigramme sous la forme où nous l'avons indiquée, les 2 premières lettres du trigramme sont soumises à une substitution simple, la 3e seule à une substitution à double clef. Il en résulte que l'on peut reconnaître l'emploi des procédés exposés plus haut, lorsque des répétitions de polygrammes ont donné lieu de croire à un chiffrement par bigrammes ou par trigrammes, en faisant un relevé des fréquences soit des lettres de rang pair et de rang impair (bigrammes), où les lettres de rang impair donneront un diagramme de fréquences à peu près normal; soit des lettres de rang $3n$, $3n + 1$, $3n + 2$, où les lettres de rang $3n + 1$ et $3n + 2$ donneront des fréquences à peu près normales.

Exemple de décryptement. — Comme il y a beaucoup plus de bigrammes que de lettres, la question des fréquences ou du pourcentage exigerait, pour pouvoir arriver à des conclusions, des textes beaucoup plus longs ou plus nombreux que ceux qui nous ont suffi pour l'étude des substitutions alphabétiques. Nous donnerons seulement un exemple d'études de décryptement sur le système à substitution orthogonale et diagonale par bigrammes dont nous avons parlé plus haut. Pour ne pas trop allonger le texte, nous avons adopté un cryptogramme assez court. Nous ferons alors des hypothèses assez hardies étant donné le peu de fréquence sur lesquelles elles

seront parfois basées; on nous y autorisera, en ne prenant cet exemple que comme une exposition des principes sur lesquels serait basée une étude mieux assise; mais on devra se persuader qu'en général des textes isolés et aussi courts ne permettront pas de conduire jusqu'au bout une étude dans de bonnes conditions, sauf heureux hasards ou connaissance d'éléments de traduction faciles à déceler (mots probables à syllabes faciles à trouver, par exemple).

Nous ne rappelons que succinctement le détail du procédé de chiffrement. Avec un tableau de 25 lettres, on chiffre les bigrammes soit dans la colonne commune des 2 lettres du bigramme clair, soit dans leur ligne commune, soit par les sommets du rectangle construit sur ces deux lettres :

A N G L E	AT se chiffre tf
T R B C D	AG se chiffre nl
F H I J K	BO se chiffre rp
M O P Q S	
U V X Y Z	

On introduit des nulles dans le clair pour éviter qu'un bigramme soit formé d'une lettre répétée, ainsi que pour séparer les mots si on le juge bon (ponctuations, facilités de lecture, etc...)

Considérons alors un cryptogramme de cette nature. Avant de chercher à identifier les bigrammes simplement en nous servant du texte, voyons l'aide que peut nous donner la connaissance du procédé.

D'après le mode de formation des bigrammes, une lettre du clair ne peut être remplacée que par 5 autres lettres du tableau : les 4 autres de sa ligne et celle de sa colonne qui la suit immédiatement :

x x x A x
x

la fréquence de cette lettre dans le clair n'est donc diluée

que sur 5 lettres du cryptogramme. Si elle est très fréquente, elle entraînera la fréquence de ces 5 lettres ou d'une partie d'entre elles. On peut faire autrement cette remarque : tous les bigrammes du clair contenant une lettre A seront traduits par un bigramme composé de lettres se trouvant sur la ligne ou sur la colonne de l'A, sur ce que l'on peut appeler, d'après une expression employée par M. Foucart dans une étude sur ce système, l'équerre de A : la fréquence de l'A dans le clair entraînera donc dans le cryptogramme la fréquence des lettres qui se trouvent sur cette équerre. Nous ne pourrons pas dire absolument que toute fréquente du cryptogramme correspond à une fréquente du clair en liant ces fréquences par une relation mathématique, parce que plusieurs lettres du clair donnent des bigrammes où entre une même lettre du cryptogramme. Mais, dans la pratique, nous pouvons dire qu'il y a de très fortes chances pour qu'une fréquente du cryptogramme se trouve sur l'équerre d'une fréquente du clair, et nous admettrons pour commencer les recherches que cette fréquente du clair est E.

Si l'on avait des textes très longs, on pourrait même essayer de serrer les solutions en faisant intervenir les comptes de fréquence. Les 8 lettres de l'équerre de l'E seront celles dont les bigrammes entre elles et avec E reproduiront le pourcentage normal de l'E dans le texte clair, chacun de ces bigrammes correspondant à la présence d'un E dans ce dernier : on ferait des essais sur les sommes des combinaisons des lettres les plus fréquentes dans le tableau des bigrammes, pour s'approcher le plus possible de la proportion de 17 %. Mais il n'y a pas lieu de trop chercher dans cette voie lorsque l'on n'a que peu de documents, les questions de calcul de probabilités exposant, avec des éléments insuffisants, à des erreurs grossières.

Soit alors le texte de 136 bigrammes, que nous écrivons par bigrammes séparés :

qa uj zo tc qi eo ie cy mq ei cy eb zb oe gt oa he
mq cz zo gt kh cg qp qa zb hu mq oz qa ym gt mj qm

vf yo yf qa td oz gi dt de gt gl uv cd oz hq oz aq
qa oz vo qi yg zo eo rq cy mz mq fq ef cb cb xp ty
oz ig yo ei qa ye za yj oz aq oe mq cz kz bf ai mq
ig qp to rq ei yn oy gq ce zr oz qa zc cg xr oz zo
cg pq ty ie oz mv tg ty mq kg gi oz ch fb qa vo pg
oz cm rg tg ym yc dt ju de qm ao qm yg na mq qe gu

Faisons le tableau de fréquence des bigrammes, en lisant la 1re lettre dans la ligne qui surmonte le tableau, la 2e dans la colonne de gauche. Les totaux de bas des colonnes indiquent la fréquence de la lettre comme initiale du bigramme, ceux de droite comme 2e lettre.

	a	b	c	d	e	f	g	h	i	j	k	m	n	o	p	q	r	t	u	v	x	y	z	
a						.						.	1	1		8		.					1	11
b			1		1	1						.						.				2	5	
c						.						.						1				1	1	3
d			1			.						.						1						2
e			1	2		.	1	1	2			.		2				.				1		10
f		1			1	.						.						.		1		1		4
g			3			.			3		1	.			1		1	2				2		13
h					1	.					1	.						.						2
i	1				3	.	2					.				2		.						8
j						.						1						.	1			1		3
l						.	1					.						.						1
m			1			.						.				3		.				2		6
n						.						.						.				1		1
o	1				2	.						.						1		2		2	4	12
p						.						.				2		.			1			3
q	2					1	1	1				8			1		2	.						16
r						.						.						.		1		1		2
t				2		.	4					.						.						6
u						.	1	1		1		.						.						3
v						.						1						.	1					2
y			3			.						.						3						6
z			2			.					1	1		13				.						17
	4	1	12	4	8	2	10	3	5	1	3	11	1	16	2	15	3	8	2	3	2	11	9	

Fréquence totale des lettres :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	t	u	v	x
15	6	15	6	18	6	23	5	13	4	3	1	17	2	28	5	31	5	14	5	5	2

y	z	
17	26	= 272

Les lettres les plus fréquentes autres que e (qui ne peut représenter E) sont q, o, z, g, y, m, a, c, t, i. Il y a de fortes chances pour que ce soit parmi ces lettres que se trouvent celles qui sont sur la ligne et sur la colonne de E, et qui donnent par leurs combinaisons des bigrammes où se trouve un E. D'autre part, les bigrammes les plus fréquents sont oz, mq, qa, zo, gt, cy, cg, ei, ig, qm, ty... Pour limiter nos recherches, nous nous appuierons sur une remarque qu'on peut faire dans le tableau normal des fréquences, c'est que presque toutes les séquences fréquentes de E et d'une lettre donnent lieu à deux bigrammes d'une fréquence appréciable, l'un où E est première lettre, l'autre où il est seconde lettre (ES—SE, ER—RE, etc.) et que cette particularité est bien plus rare avec les autres lettres qu'avec E. Comme, dans la formation des bigrammes avec notre méthode, les deux bigrammes inverses du clair sont rendus par des bigrammes inverses du cryptogramme (si ES = ku, SE = uk), nous ne travaillerons au début que sur les bigrammes oz — zo, mq — qm, qa — aq, gt — tg, etc..., laissant d'abord de côté ceux qui, comme yt et cq, n'ont pas donné de bigrammes inverses dans le texte.

Nous essaierons alors d'identifier des bigrammes, d'après leur fréquence, leur position dans le texte, leur accolement avec un bigramme inverse (elle, cette, etc...), en cherchant d'abord les bigrammes où se trouve E. Quand un bigramme est identifié, on cherche à en faire usage pour reconstituer le tableau, de manière à profiter des lettres replacées dans celui-ci pour déchiffrer d'autres bigrammes. Or, si uk s'identifie avec AM, les dispositions du tableau seront, comme forme, l'une des trois suivantes :

```
A        u ..... A        A u .... M k
u        :       :
:        :       :
:        M  ...  k
M
k
```

Les espaces qui sont marqués en pointillés pourront être plus grands ou plus petits, les lignes ou les colonnes pouvant être plus ou moins écartées, sans que le résultat de l'opération de chiffrement soit modifié. Au cours des essais successifs, il s'agira de concilier les différentes hypothèses sur les trois formes possibles dans chaque identification de manière à reformer un seul tableau de 25 cases.

Nous guidant sur les fréquences, nous ferons l'hypothèse : oz = ES. Les fréquences normales qui suivent celles de ES en français portent sur EN et LE. Ici nous avons qa et mq avec même fréquence 8. Le tableau des fréquences normales nous donne une différence plus grande entre EL et LE (EL $= \frac{1}{2}$ LE) qu'entre EN et NE (NE $= \frac{3}{5}$ de EN): Comme aq $= \frac{1}{4}$ de qa, et que qm $= \frac{3}{8}$ mq, nous adopterons qa pour LE. Du reste le premier groupe du cryptogramme est qa; on trouve la forme aqqa = ELLE. Cette hypothèse est donc acceptable.

On aurait alors les possibilités de dispositions suivantes dans le tableau :

```
E  A     E  O     E  M

Q  L     Z  S     Q  N
```

ou :

```
E     E     E
A     O     M
:     :     :
L     S     N
Q     Z     Q
```

ou :

E A . L Q E O . S Z E M . N Q

l'une des trois dispositions pour un des bigrammes devant pouvoir s'arranger avec une pour chacun des autres. On ne peut avoir à la fois deux des dispositions en colonne ou deux des dispositions en lignes, puisque toutes elles imposent la lettre voisine de E et que ce n'est pas la même lettre. Par contre, on peut très bien combiner les trois dispositions en rectangle, en mettant LN sur la même ligne que Q :

E O A M

Z S
Q L N

On en conclut que ml = AN, et on peut porter, comme hypothèse, dans le cryptogramme, les valeurs adoptées ES, SE, EL, LE, EN, NE, AN (les autres bigrammes à tirer de ce tableau par diagonales ne figurent pas dans le texte).

Parmi les combinaisons des lettres sur lesquelles nous avons fait des hypothèses que nous admettons jusqu'à présent, c'est-à-dire sur EOAM que nous supposons être sur la même ligne, notre cryptogramme nous présente deux fois eo et deux fois oe; étant donné le peu de bigrammes figurant au tableau, et à moins qu'il ne s'agisse d'un nom propre à forme particulière répété, et amenant plusieurs fois un bigramme qui sans cela serait rare, nous avons un bigramme fréquent, fait dans une ligne et contenant E. Dans un bigramme ainsi formé, pour qu'une lettre du clair figure dans le cryptogramme, il faut qu'elle soit la lettre du milieu d'un groupe de 3 lettres adjacentes dans le tableau, dont les deux extrêmes sont les autres lettres de deux bigrammes se correspondant dans le clair et le cryptogramme. .AMK. dans une ligne donne mk comme représentation de AM et km comme représentation de MA. Si donc nous supposons que eo représente

un bigramme contenant la lettre E, la colonne O sera adjacente à la colonne E. C'est une nouvelle hypothèse que rien encore ne vient infirmer.

La ligne de l'E pourra alors présenter les permutations diverses entre le groupe EU indissoluble, A, M, et une lettre encore inconnue.

La disposition EOM?A ou EO?MA donnerait eo = AE, groupe peu fréquent comme EA.

La disposition EOA?M ou EO?AM donnerait eo = ME, ce qui n'est pas impossible, étant données les fréquences. Comme la lettre inconnue peut donner une meilleure fréquence que le M (nous avons le t dans la liste des lettres possibles pour l'équerre de l'E), nous ne pouvons pas décider; mais déjà nous savons que ce n'est pas l'A qui viendra à la gauche de l'E.

Parmi les lettres que nous avons considérées, par leurs fréquences et leurs bigrammes, comme pouvant se trouver sur l'équerre de l'E, restent encore gyti. Bien entendu, cette liste n'est pas exclusive; mais c'est une hypothèse.

Or nous avons un bigramme fréquent ei — ie. Si ce bigramme correspond à un bigramme du clair en E, il faudra que I se trouve à côté de E ou au-dessous. Cette dernière place seule est libre. On aura :

E	O	A	?	M
I				
?				
Z	S			
Q		L		N

où les positions de EO et de EI seules sont fixées exactement. Quant au bigramme ei, il ne pourrait correspondre avec les lettres écrites au tableau qu'à ZE ou QE. Il faut alors chercher parmi les lettres non employées la lettre que nous placerons au-dessus de E (ou en fin de colonne), I étant alors immédiatement suivi de Q ou de Z dans la colonne. ei vient trois fois et ie deux fois. Il n'y a que le T qui puisse nous donner de pareilles fréquences (Y et G

ne donnent que de rares bigrammes). La colonne serait alors :

E	ou	E
I		I
Q		Z
Z		Q
T		T

On admettra alors ei = TE, ie = ET, et, si l'on s'en tient aux lettres Y et G comme seules à pouvoir encore entrer dans l'équerre de l'E, comme nous avons un bigramme ao-oa, et que les bigrammes de E avec G sont plus fréquents que ceux de E avec Y, nous supposerons que c'est G qui est dans la branche horizontale de l'équerre. C'est d'ailleurs une hypothèse un peu hasardeuse, car ce bigramme ao pourrait très bien ne pas correspondre à un bigramme en E (sa fréquence est faible, mais la fréquence de EG et de GE est très faible. On trouverait avec A ou O de la même ligne des bigrammes clairs bien plus fréquents).

On doit alors avoir quelque chose comme :

E O M G A	ou	E O G A M
I		I
Q		Z
Z		Q
T		T

les positions réciproques de Z et de Q n'étant pas encore fixées. La lettre que nous gardions inconnue dans la ligne, ce qui nous empêchait d'apprécier la fréquence eo = ME, étant supposée G, et ME étant plus fréquent que GE, c'est M qui vient à la gauche de E, et la ligne de l'E doit être EOGAM.

Revenons alors au cryptogramme, et utilisons nos hypothèses sur ei et eo.

Le commencement donne :

LE uj SE tc qi ME ET cy EN
TE cy eb zb EM....

D'autre part, nous voyons apparaître vers le milieu du cryptogramme la séquence ES EL EM EN, qui nous donne à penser aux mots «les éléments», et nous fait espérer qu'une partie au moins de nos hypothèses sont justes. Le début nous incite à penser à des nombres ordinaux, qui commencent souvent les ordres pris comme exemples dans cet opuscule. Alors ME serait précédé de IE et qi serait IE. Ceci nous fixerait sur la place des différentes lettres de la colonne, où EIQ devraient se succéder. Nous aurons alors comme tableau :

E	O	G	A	M
I				
Q		L	N	
Z	S			
T				

Si le mot ELEMENTS est exact, cz = TS. C viendra donc se placer sous S à côté de T.

Continuant à examiner le début, les groupes

cy ENTE cy eb zb EM

avec la répétition de cy, peuvent correspondre à TRENTE-TROISIÈME. Les bigrammes eb zb avec une première lettre (e et z) venant de la colonne de l'I, et une même deuxième lettre, rendent admissibles deux bigrammes du clair terminés en I. On disposerait alors de nombreux éléments pour le tableau; on aurait à raccorder le résultat déjà acquis :

E	O	G	A	M
I				
Q			L	N
Z	S			
T	C			

avec les nouveaux résultats

T	c		e	O		z	S
R	y		I	b		I	b

L'installation de B au-dessous de O donne satisfaction aux deux derniers. Mais le premier est impossible sous cette forme.

Il n'y a plus de place pour R dans la colonne de T. Nous adopterons alors la disposition T C R Y, et nous aurons :

E O G A M
I B
Q L N
Z S
T C R Y

Nous en tirons gt = ER, cg = RO, to = CE, ye = TA, yg = RA. Reportons ces valeurs (et leurs inverses) dans le cryptogramme.

Nous avons alors le début :

LE uj SE tc IEME ET TRENTE TROISIEME
REG he ENTS SE RE kh RO qp LE.....

Il pourrait s'agir du 16e régiment; alors on aurait tc = IZ, ce qui est impossible, car T et C sont dans la même ligne et I est dans une autre ligne. C'est alors SEPTIEME, tc = PT, et P termine à droite les dernières lignes de notre tableau; uj doit alors être s, de LES, suivi d'une nulle. U sera donc à la même ligne que S. he remplacera IM, H sera donc sur la colonne entre M etN. kh vaudra ND, que nous ne pouvons placer encore, mais cela nous indique que k est à la ligne de N; qp vaudra NT, ce qui nous confirme la place de P.

E O G A M
I B
Q L N — ligne de K
Z S — ligne de U
T C R Y P

LES? SEPTIEME ET 33e REGIMENTS SE RENDRONT
LE SI hu ENESLE APER mj NE vf CAVALE td ES

Ei dt de ERA..... ELLE ES vo IERA iE SE METq TREz EN.....

On a maintenant des éléments pour continuer le tableau et le terminer. Nous avons représenté par les lettres minuscules les passages non traduits du cryptogramme. Parfois il n'y a qu'une lettre douteuse, trois des sommets du rectangle étant déjà connus, ce qui donne une des lettres du nouveau bigramme

E G
: :
I ?

ig = ?E.

Finalement on reconstituerait le tableau

E O G A M
I B D F H
Q J K L N
Z S U V X
T C R Y P

qui a été formé avec la clef CRYPTOGRAMME et la suite de l'alphabet.

C R Y P T
O G A M E
B D F H I
J K L N Q
S U V X Z

Nous rappellerons encore qu'avec des textes courts, le travail peut être beaucoup plus difficile que dans cet exemple. Mais la recherche des bigrammes contenant l'E semble une bonne marche à suivre, surtout si l'on a un mot probable contenant des E à des intervalles faciles à repérer.

CHAPITRE XII

SYSTÈMES DE TRANSPOSITION

Dans les systèmes de transposition, le chiffreur fait une salade des lettres (ou des mots) du texte clair, suivant une loi connue du déchiffreur, et celui-ci, par l'opération inverse, rétablit l'ordre des lettres ou des mots du cryptogramme pour reproduire le clair.

Il en résulte que, sauf le cas d'additions de nulles ou de fautes d'orthographe voulues, les fréquences sont normales.

Clefs de transposition. — Avant d'aller plus loin, nous parlerons des clefs de transposition. Ces clefs ont pour but d'indiquer l'ordre numérique du relèvement de lettres ou de colonnes; ce sont des suites de numéros, de 1 à un autre nombre donné, où aucun nombre ne paraît deux fois, et qui, se suivant dans un ordre différent généralement de l'ordre numérique, indiquent par cet ordre même la loi suivant laquelle doit se faire le relèvement. Ces clefs peuvent être numériques : 5 6 3 9 1 10 2 8 4 7, et se composer de la série des numéros dans l'ordre adopté pour le relèvement. On relèvera d'abord ici l'élément correspondant à 1 de la clef, c'est-à-dire le 5e dans l'ordre de gauche à droite, puis celui qui correspond à 2 de la clef, soit le 7e dans l'ordre de gauche à droite, etc... Mais quand la clef est un peu longue et qu'on ne veut pas la garder par écrit (il est difficile de retenir de mémoire une clef numérique), on a alors recours à une clef littérale, qu'on transforme pour l'emploi en clef numérique.

Un des procédés universellement connus pour trans-

former une clef littérale, mot ou phrase de quelques mots, en clef numérique, est le suivant. On numérote les lettres de la clef suivant l'ordre alphabétique : s'il y a un A, on lui donne le n° 1; s'il y a deux A, on donne le n° 1 à celui qui est le plus à gauche, le n° 2 à l'autre; s'il y a deux A, un B, pas de C, pas de D, un E, on donne aux deux A les n^{os} 1 et 2, au B le n° 3, à l'E le n° 4, etc... S'il n'y a pas de A, on donne le n° 1 à l'exemplaire le plus à gauche de la lettre la plus rapprochée de l'A dans l'ordre alphabétique.

Exemples :

A M B A S S A D E D A L L E M A G N E
1 15 6 2 18 19 3 7 9 8 4 13 14 10 16 5 12 17 11

M I N I S T R E D E L H Y G I E N E
12 8 13 9 16 17 15 2 1 3 11 7 18 6 10 4 14 5

On a ainsi la clef.

On peut suivre, dans le relèvement des éléments, un ordre convenu autre que l'ordre numérique de la clef, mais s'appuyant sur ces numéros (éléments pairs — ordre inverse du plus gros numéro au plus petit, etc...). On peut prendre comme clef littérale l'expression en toutes lettres d'un nombre (cent trente-quatre : 2 3 7 12 13 10 4 8 14 5 9 16 1 15 11 6). On peut, en un mot, user de tous les moyens de dérouter un adversaire qui peut se faire donner la clef par trahison. Mais le principe d'emploi de la clef pour les transpositions, indiqué ici, est reproduit dans maintes méthodes de cryptographie, et doit être connu de tous les cryptologues.

Revenons aux systèmes de transpositions.

On en a inventé des multitudes, et on peut en inventer tant que l'on veut. Il suffit d'adopter une loi commode pour relever une à une la suite de lettres qui forment le texte clair dans un ordre différent de celui de ce texte.

Un numérotage de ces lettres pourrait suffire; on emploie par exemple la mise en tranches de longueur donnée, où

on relève les lettres dans un ordre donné en commençant par une tranche autre que la première. Par exemple, avec une clef numérique 4 2 6 3 7 1 5, on coupera le texte en tranches de 7 lettres; on considérera d'abord l'ensemble des 7 premières tranches et on relèvera la 6e tranche (celle qui correspond au 1 de la clef), lettre à lettre, dans l'ordre 6e, 2e, 4e, 1e, 7e, 3e, 5e, c'est-à-dire dans l'ordre des chiffres de la clef, où le chiffre 1 est le 6e du nombre 4 2 6 3 7 1 5, puis on relèvera la 2e tranche qui correspond au 2e chiffre de la clef, etc... on sautera les tranches ou les lettres manquantes à la fin du texte quand on sera dans la dernière tranche et si celle-ci est incomplète. On pourra aussi relever d'abord dans chaque tranche la lettre portant le no 1, puis dans chaque tranche la lettre portant le no 2, etc... On pourra relever la 1re tranche dans l'ordre des nombres de la clef en commençant à 1, la 2e dans cet ordre en commençant à 2, etc... On voit que ce ne sont pas les conventions pour l'ordre de relèvement qui manquent. Nous indiquerons plus loin la méthode générale pour résoudre les problèmes de cette nature, mais disons tout de suite que, lorsqu'on n'a qu'un document et qu'on ignore comment il a été fait, on a de sérieuses chances de ne point venir à bout de le traduire, étant donnée l'extrême fantaisie qui peut avoir présidé au relèvement des lettres du texte clair.

Transpositions à tableau. — Toutefois, fort souvent, les systèmes de transposition comportent l'emploi d'un « tableau ». Le chiffreur écrit le texte clair, lettre à lettre, dans les cases d'un tableau (on dit parfois d'une grille, bien que ce mot ait ordinairement un sens spécial que nous définirons plus loin), et une certaine loi fixe l'ordre du relèvement des lettres dans les cases. On peut imaginer des formes variées de tableau, un ordre quelconque pour l'inscription et le relevé, tels que saut du cavalier, dessins géométriques, spirales du centre à la circonférence ou réciproquement. Là encore l'imagination peut se donner libre cours.

Il y a pourtant des types de tableaux, très employés, classiques, dont nous allons parler maintenant.

Les lettres y sont écrites par lignes d'une longueur égale (sauf parfois la dernière), de manière à former des colonnes, et on les relève par colonnes, dans un ordre fixé par une clef.

Lorsque la dernière ligne est égale aux autres, on dit que le tableau est « complet ». Quand elle ne l'est pas, le tableau est dit « incomplet ».

Méthode des diviseurs. — On trouvera dans les ouvrages de cryptographie, sous le nom de méthode des diviseurs, des considérations sur les cryptogrammes à tableaux complets. Comme le nombre de lettres est le produit du nombre de lignes par le nombre de colonnes, la longueur des lignes et celle des colonnes sont des diviseurs du nombre de lettres du cryptogramme. Il en résulte pour la longueur des colonnes une première hypothèse dont nous verrons l'avantage quand nous aurons traité le cas général. Ces mêmes ouvrages, sous le nom de transposition double, font allusion au cas où, dans ces tableaux, on relève les colonnes dans un ordre fixé par une clef, et où dans chaque colonne, on relève les lettres non pas de haut en bas dans l'ordre des lignes mais dans un ordre également fixé par une clef, la même ou une autre (On emploie quelquefois le nom de transposition double pour un autre procédé qui doit s'appeler double transposition). Ils parlent de relèvement en diagonales, etc... Ces considérations ne nous semblent pas utiles à reproduire ici : nous ne nous occuperons d'une manière générale que des tableaux relevés par colonnes verticales, qu'ils soient complets ou incomplets. Les considérations exposées à ce sujet pourront guider pour l'étude de tableaux relevés de manière différente, et, finalement, la méthode générale d'étude des transpositions fournira un procédé de recherche applicable à tous les cas.

Transposition simple à tableau. — Nous définissons donc comme suit le procédé, que l'on appelle ordinairement transposition simple :

Pour chiffrer un texte clair en transposition simple,

on choisit une clef, ordinairement littérale, qu'on transforme en clef numérique. On écrit le texte clair en lignes ayant chacune un nombre de lettres égal au nombre de lettres de la clef, les lettres des lignes successives les unes sous les autres, formant des colonnes, et on compose le cryptogramme en écrivant les lettres dans l'ordre où elles se présentent de haut en bas dans chaque colonne, les colonnes étant prises dans l'ordre indiqué par la clef.

Exemple : soit à chiffrer : « La 6e division partira ce soir » avec la clef « MARSEILLE » :

M	A	R	S	E	I	L	L	E
7	1	8	9	2	4	5	6	3
l	a	s	i	x	i	e	m	e
d	i	v	i	s	i	o	n	p
a	r	t	i	r	a	c	e	s
o	i	r						

On aura le cryptogramme suivant, que nous couperons par colonne pour faire comprendre le mécanisme :

airi xsr eps iia eoc mne ldao svtr iii

et qu'on rencontrera ordinairement en tranches de 5 lettres :

airix sreps iiaeo cmnel daosv triii

Pour déchiffrer, on connaît la longueur de la clef et le nombre de lettres du texte. En divisant ce dernier par le nombre de lettres à la ligne (longueur de la clef), on voit combien on a de lignes entières (quotient) et combien il reste de lettres en plus (dernière ligne incomplète). Comme ces lettres appartiennent aux colonnes de gauche du tableau, il est facile de préparer, dans un quadrillage par exemple, un tableau en blanc où les colonnes sont prêtes à recevoir le même nombre de lettres que celles du tableau fait par le chiffreur. On écrit la clef au-dessus.

Ici nous avons 30 lettres, et la clef en a 9. Nous aurons

donc 3 lignes complètes, plus 3 lettres. Nous aurons par suite 3 colonnes de 4 lettres et 6 de 3; les premières sont les 3 colonnes de gauche (7, 1, 8). Nous écrirons alors les 4 premières lettres du cryptogramme l'une sous l'autre dans la colonne 1, les 3 suivantes dans la colonne 2, les 3 suivantes dans la colonne 3, etc... Nous constituerons ainsi un tableau absolument analogue au tableau de chiffrement et nous lirons le texte clair par lignes horizontales.

Décryptement des transpositions simples. — Le décryptement des documents de cette nature repose essentiellement sur la considération de la fréquence des bigrammes. On cherche à juxtaposer deux fragments du cryptogramme provenant de deux colonnes voisines et à reconstituer les bigrammes du texte clair; puis on juxtapose un 3e fragment pour avoir des trigrammes, etc...

Soit le cryptogramme de 78 lettres ·

5
TVCER NSMRY LEIQR EHOQC UDDEA URDSC
10
AIUMR IEUPH AMOUP AEIUR QENIS QUSIE
15
RIICI ZAAEI SNOVE BRS.

Dans cette explication d'une méthode générale, nous ne ferons d'abord aucune hypothèse sur la longueur de la clef. Nous chercherons de proche en proche, comme nous l'avons dit, à accoler des lettres. Pour avoir un bon point de départ, il est recommandé de choisir d'abord les bigrammes qui peuvent le moins prêter à l'équivoque : si nous prenions comme 1re lettre E, nous pourrions essayer avec succès de lui accoler n'importe quelle consonne et plusieurs voyelles, et nous aurions à faire d'innombrables essais. On choisit donc comme point de départ une lettre qui donne peu de séquences : Z, qu'on fait précéder d'une voyelle ou de N; X, qu'on fait précéder d'une voyelle

particulièrement U ou I; J, qu'on fait suivre d'une voyelle; et, de préférence, Q, qu'on fait suivre de U.

C'est la lettre Q que nous prendrons ici. Elle apparaît quatre fois dans le cryptogramme, où nous trouvons 7 U.

Chacun des essais est basé sur la remarque suivante: comme le texte clair est écrit par lignes, si nous amenons la juxtaposition d'une lettre d'une ligne dans une première colonne quelconque avec la lettre de la même ligne de la colonne voisine dans le tableau du chiffreur, les lettres au-dessus et au-dessous dans la 1re colonne devront également retrouver leur voisine du texte clair dans la colonne voisine. Si donc nous prenons une séquence de lettre du cryptogramme renfermant la lettre Q, une autre renfermant la lettre U, et si les deux lettres choisies sont celles qui doivent nous donner la solution, les autres lettres des deux séquences, juxtaposées, doivent donner des bigrammes acceptables dans un texte clair. Une difficulté apparaît, celle de limiter les séquences aux lettres d'une seule colonne, et de ne pas prendre à la fois des lettres de la colonne où figure Q et des lettres d'une autre colonne. Nous verrons comment cette difficulté diminue au cours du travail : au début, elle est réelle, et oblige à une grande prudence dans les essais.

Considérons donc Q du 3e groupe, et plaçons en face d'un fragment de colonne comprenant cette lettre des éragments de colonnes contenant les U successifs, Q et U ftant en regard :

1	2	3	4	5	6	7
Y H	Y D	Y S	Y M	Y H	Y P	Y N
L O	L D	L C	L R	L A	L A	L I
E Q	E E	E A	E I	E M	E E	E S
I C	I A	I I	I E	I O	I I	I Q
Q U	Q U	Q U	Q U	Q U	Q U	Q U
R D	R R	R M	R P	R P	R R	R S
E D	E D	E R	E H	E A	E Q	E I
H E	H S	H I	H A	H E	H E	H E
O A	O C	O E	O M	O I	O N	O R
Q U	Q A	Q U	Q O	Q U	Q I	Q I

Supposant que nous avons de bonnes raisons de croire que la lettre Q du bas des colonnes est dans la même colonne que celle que nous considérons, nous éliminerons les combinaisons 2 4 6 7 où cette lettre n'est pas suivie de U. Nous nous réservons d'ailleurs, si nous n'obtenons de résultat avec aucune des trois autres, de les reprendre, en coupant la colonne, en bas, au-dessus de cette lettre.

Le bigramme II nous pousserait à écarter la combinaison 3. Cependant il peut être produit par la fin d'un mot et le début d'un autre. Pour décider entre les trois hypothèses nous aurons recours à un procédé déjà signalé comme capable de donner des indications utiles (nous ne disons point des certitudes) et nous ferons le total des indices de fréquence des bigrammes relevés dans le tableau qui figure au chapitre I.

YH — 0	YS — 0	YH — 0
LO — 4	LC — 0	LA — 12
EQ — 1	EA — 8	EM — 20
IC — 1	II — 0	IO — 10
QU —	QU —	QU —
RD — 4	RM — 3	RP — 4
ED — 21	ER — 19	EA — 8
HE — 6	HI — 0	HE — 6
OA — 0	OE — 0	OI — 10
QU —	QU —	QU —
TOTAL. . 37	30	70

(On n'a pas inscrit les fréquences de QU qui sont égales dans les 3 colonnes). Nous adopterons donc, pour continuer les essais et tâcher de former des trigrammes, la combinaison fournie par Q du 3e groupe avec U du 9e, et nous considérerons que la plus grande partie des 3e, 4e, 9e et 10e groupes ne sont plus disponibles pour de nouveaux essais, étant déjà employés en bigrammes.

Considérons nos bigrammes. L'M du troisième sera probablement suivi d'une voyelle, ou des consonnes B, M, P (Voir, tableau des bigrammes, les lettres suivant M),

les bigrammes QU seront suivis d'une voyelle, OI probablement d'une consonne. Nous chercherons dans le cryptogramme une séquence du type .. voyelle ou M, ou B, ou P . voy ... cons. voy., ou, en représentant les voyelles par v, les consonnes par c, et ne tenant pas compte des deux premières lettres dont la nature est douteuse :

v . v . . . c v

(si nous n'obtenons pas de résultat, nous remplacerons la 1re voyelle par M, B, P). Nous trouvons, en respectant les groupes déjà employés :

E A U R D S C A
E N I S Q U S I
A E I S N O V E

En juxtaposant ces séquences, et les deux lettres qui les précèdent, à nos bigrammes, nous avons :

1	2	3
YH D	YH R	YH Z
LA D	LA Q	LA A
EM E	EM E	EM A
IO A	IO N	IO E
QU U	QU I	QU I
RP R	RP S	RP S
EA D	EA Q	EA N
HE S	HE U	HE O
OI C	OI S	OI V
QU A	QU I	QU E

Au simple examen des trigrammes, les séries 1 et 3 semblent à éliminer, à cause des trigrammes IOA, RPR pour 1, IOE pour 3. D'autre part, le trigramme de tête de chaque colonne est inadmissible ; cela n'importe que pour la solution juste, et nous ne pouvons faire état de cette particularité dans les combinaisons 1 et 3, mais dans la combinaison 2 nous en tiendrons compte pour supposer

que nous avons trop étendu vers le haut notre séquence d'essai et nous laisserons ce trigramme de côté pour la suite.

Bien que ce premier examen puisse sembler suffisant, nous allons avoir recours à l'épreuve des fréquences, en considérant la somme des fréquences des bigrammes finaux de nos trigrammes puisque nous n'avons pas de tableau de fréquence des trigrammes.

1		2		3	
AD	1	AQ	1	AA	1
ME	19	ME	19	MA	3
OA	0	ON	28	OE	0
UU	0	UI	8	UI	8
PR	4	PS	4	PS	4
AD	1	AQ	1	AN	18
ES	42	EU	13	EO	0
IC	1	IS	8	IV	2
UA	7	UI	8	UE	8
TOTAL. .	75		90		44

Nous adopterons la combinaison 2 pour continuer les essais (on rappelle qu'en cas de totaux très voisins, il est bon de donner la préférence à la combinaison qui offre beaucoup de fréquences moyennes, plutôt qu'à celle qui ne l'emporte au total que grâce à une unique fréquence très forte contrebalançant la faiblesse extrême des autres).

Nos trigrammes sont alors :

L A Q
E M E
I O N
Q U I
R P S
E A Q
H E U
O I S
Q U I

La présence des deux lettres Q à un intervalle de six rend désirable la découverte d'une séquence contenant 2 U à 6 d'intervalle.

Nous en avons deux : UDDEAU et UMRIEU.

Formons des tétragrammes :

1				2			
L	A	Q	U	L	A	Q	U
E	M	E	D	E	M	E	M
I	O	N	D	I	O	N	R
Q	U	I	E	Q	U	I	I
R	P	S	A	R	P	S	E
E	A	Q	U	E	A	Q	U
H	E	U	R	H	E	U	P
O	I	S	D	O	I	S	H
Q	U	I	S	Q	U	I	.

Nous ne disposons plus d'une lettre pour mettre sur pied le dernier tétragramme de la combinaison 2, l'A qui commence le 9e groupe, et qui devrait prendre cette place, étant employé comme 2e lettre dans le 1er tétragramme. Il faudrait donc, en acceptant cette combinaison, sacrifier la première ou la dernière ligne. Nous préférons adopter la combinaison 1, qui ne contient d'ailleurs pas de tétragramme choquant.

Si nous considérons maintenant notre cryptogramme, nous voyons que nous en avons extrait 4 tranches de 9 lettres, qu'il commence par une tranche de 10 lettres intacte, qu'entre les deux tranches LEIQREHOQ et UDDEAURDS il reste une lettre toute seule ainsi qu'entre les deux tranches AMOUPAEIU et QENISQUSI. Ces lettres ne peuvent rester inutilisées, il faut les rattacher à la tranche qui les précède, en allongeant le tableau par en bas, ou à celle qui les suit en l'allongeant par en haut. Comme nous en avons déjà rogné une ligne en haut, c'est en bas que nous essaierons, et nous ajouterons un nouveau tétragramme, en prenant la 10e lettre de nos séquences actuellement limitées à 9 : C R E C, tétragramme acceptable.

Le cryptogramme comprend alors : 1 tranche de 10 non employée, 2 tranches de 10 employées, 1 tranche de 10 non employée, 2 tranches de 10 employées et 18 lettres qui ne peuvent correspondre qu'à deux tranches de 9, puisque les colonnes longues n'ont jamais qu'une lettre de plus que les colonnes courtes. Ces deux tranches de 9 correspondront aux deux seules colonnes courtes du tableau, et seront donc à droite de ce dernier, à côté l'une de l'autre.

En les juxtaposant, nous aurons deux solutions possibles :

R	I
I	S
I	N
C	O
I	V
Z	E
A	B
A	R
E	S

I	R
S	I
N	I
O	C
V	I
E	Z
B	A
R	A
S	E

La somme des fréquences des bigrammes donne 109 pour la combinaison de gauche, 63 pour celle de droite. Nous adopterons donc celle de gauche.

Restent deux colonnes à placer, à droite ou à gauche de notre faisceau de 4, ou à gauche de notre faisceau de deux colonnes courtes, ou à droite de ce faisceau, mais en mettant les lettres en concordance non plus avec celles de la même ligne, mais avec celles de la ligne inférieure de la colonne courte. Le texte en effet continue d'une ligne à l'autre, et des bigrammes du texte clair commencent par les lettres de la dernière colonne du tableau, mais ils finissent dans la 1re colonne à la ligne au-dessous. Ceci est à retenir, car notre lettre origine des essais peut appartenir à la dernière colonne, et il faudra en tenir compte lorsque, comme nous l'avons fait, on sera amené à délimiter la longueur des colonnes dans le cryptogramme.

Continuons. Les deux bigrammes QU des 1re et 6e lignes

du tableau des tétragrammes appellent des voyelles. Les deux colonnes à placer sont :

TVCERNSMRY et AIUMRIEUPH

Il ne saurait y avoir de doute, et nous avons terminé la reconstitution du tableau :

L	A	Q	U	A	T	R	I
E	M	E	D	I	V	I	S
I	O	N	D	U	C	I	N
Q	U	I	E	M	E	C	O
R	P	S	A	R	R	I	V
E	A	Q	U	I	N	Z	E
H	E	U	R	E	S	A	B
O	I	S	D	U	M	A	R
Q	U	I	S	P	R	E	S
C	R	E	C	H	Y		

La clef, que l'on retrouve en considérant l'ordre dans lequel les colonnes étaient placées dans le cryptogramme, était numériquement 2 5 6 3 4 1 7 8.

Le problème est résolu, car nous aurons le moyen de déchiffrer les cryptogrammes faits avec la même clef. Toutefois, certains cryptologues tiennent à retrouver la clef littérale dont a été tirée la clef numérique. C'est surtout une affaire d'intuition, où l'on essaie des combinaisons de lettres se succédant de manière à donner une clef numérique analogue à celle qu'on possède et donnant des bigrammes et trigrammes acceptables. Ici nous avions la clef « Bordeaux ».

Emploi du mot probable. — Nous avons exposé ci-dessus le procédé analytique de décryptement des transpositions simples.

La connaissance ou l'hypothèse de l'existence d'un mot probable facilite énormément les recherches. On y trouve au besoin un point de départ pour les essais. Des cryptogrammes en effet peuvent ne pas contenir la lettre Q,

ou bien le bigramme QU, trop connu des décrypteurs, peut être masqué et remplacé par exemple par K (En allemand, le bigramme commode de départ est CH. Mais il existe un signal Morse pour ce bigramme, souvent C et H sont groupés systématiquement et l'ensemble ne compte que pour une lettre, et ne figure que pour une lettre dans les colonnes). Quand on hésite sur la séquence à juxtaposer aux colonnes obtenues, le mot probable est une aide puissante. Nous n'avons pas voulu en faire état, mais le lecteur habitué à nos exemples voyait, dès les trigrammes, se dessiner le début LAQ.... IEME DIVISION, qui lui donnait et la longueur des lignes (par suite le nombre de colonnes) et le début de toutes les colonnes. Il faut donc, dès qu'on peut faire des hypothèses sur un mot dont on n'a que des fragments, les faire et les utiliser. En particulier, si les lettres du mot probable ne figurent qu'une fois dans le cryptogramme, leur simple juxtaposition résout le problème.

Limitation des essais. — L'exposé ci-dessus nous a montré que la grosse difficulté est de déterminer les limites des séquences à juxtaposer. Si, par exemple, on est certain que la lettre U qu'on allait essayer de juxtaposer à Q est dans la partie inférieure d'une colonne tandis que Q est dans les premières lignes, on ne perdra pas son temps à faire l'essai. Par conséquent, tout ce qui permet des hypothèses menant à des essais simples et rapides sur la longueur et les limites des colonnes est une aide pour le décrypteur.

Parmi ces circonstances heureuses, nous citerons d'abord la certitude qu'on a affaire à un tableau complet. Si avec cette certitude, nous trouvons un cryptogramme de 96 groupes, le tableau aura énormément de chances, étant donné qu'on évite ordinairement les clefs de moins de 5 lettres et de plus de 30, d'avoir ou 6 colonnes de 16 lettres, ou 8 de 12, ou 12 de 8, ou 16 de 6, ou 24 de 4. Cela nous fera 5 essais à faire, car 96 a des diviseurs relativement nombreux; mais, ayant coupé notre document en 8 tranches de 12 lettres par exemple, nous n'aurons

qu'à essayer dans chaque ligne formée par la juxtaposition de ces colonnes de former des mots, sans nous demander : les lettres que nous nous efforçons de juxtaposer sont-elles bien celles d'une même ligne? et sans craindre un décalage de ligne d'une colonne à l'autre. En écrivant les colonnes sur des bandes de papier, et en s'aidant des fréquences comme plus haut, l'opération est généralement facile.

Nous aurons encore une heureuse chance si, ne pouvant compter sur un tableau complet, nous connaissons le nombre de colonnes du tableau : cela peut arriver dans la réalité, par exemple si un chiffreur imprudent a opéré en notre présence, trop loin pour que nous puissions lire son travail, mais à distance telle que nous ayons pu distinguer et compter les colonnes.

Soit le cryptogramme suivant de 52 lettres :

ASTNS TUUSA ANUOP MTDEZ LCECO UDEAT
SEDDR RREMC QBOMP ECEEO NI

Nous savons que le tableau a 9 colonnes. En divisant 52 par 9, nous trouvons qu'il a 5 lignes complètes et 1 ligne de 7. Il y a donc 7 colonnes longues de 6 lettres, et 2 colonnes courtes de 5. Si nous savions à quelle place, dans le cryptogramme, figurent ces colonnes courtes, nous couperions ce texte en tranches de 6 et de 5 lettres qui reproduiraient les colonnes du tableau, et nous n'aurions plus qu'à en retrouver l'ordre en les écrivant par exemple sur des bandes de papier et nous aidant, pour apprécier la valeur d'un essai de juxtaposition, des fréquences de bigrammes comme nous l'avons vu plus haut.

Nous ne connaissons pas la place des colonnes courtes, mais on peut fixer des limites pour chaque colonne.

Supposons en effet que sur le vrai tableau, celui du chiffreur, les deux colonnes courtes aient été relevées les dernières. En coupant notre cryptogramme en 7 colonnes longues suivies de deux courtes, nous aurions la copie des colonnes du vrai tableau :

A	U	U	E	O	S	R	O	E
S	U	O	Z	U	E	E	M	E
T	S	P	L	D	D	M	P	O
N	A	M	C	E	D	C	E	N
S	A	T	E	A	R	Q	C	I
T	N	D	C	T	R	B		

Mais notre hypothèse peut être fausse et les colonnes courtes peuvent être ailleurs. Si, au lieu d'être une colonne longue, la 1re colonne relevée, qui commence par A, était une colonne courte, la lettre T qui la termine sur ce tableau passerait en tête de la colonne suivante, celle du bas de cette colonne en tête de la 3e, etc...

Si les deux colonnes courtes avaient été relevées les premières, les 2 dernières lettres de la 2e colonne passeraient à la 3e, les 2 dernières de la 3e à la 4e, etc...

Si la 1re colonne étant longue, la 2e est courte, un passage de lettre d'une colonne à l'autre se produira, mais nous avons considéré les deux cas extrêmes des colonnes courtes en queue et des colonnes courtes en tête, et par suite les déplacements de lettres maxima.

Si donc nous établissons le tableau suivant :

	a	t	e	a	r	q	
t	n	d	c	t	r	b	c
A	U	U	E	O	S	R	O	E
S	U	O	Z	U	E	E	M	E
T	S	P	L	D	D	M	P	O
N	A	M	C	E	D	C	E	N
S	A	T	E	A	R	Q	C	I
T	N	D	C	T	R	B		

le tableau en majuscules représentera les colonnes dans un des cas extrêmes, le tableau composé par la partie du tableau en majuscules au-dessus du trait plein, et par le « chapeau » en minuscules, représentera les colonnes dans

l'autre cas extrême (en considérant chaque colonne isolément et sans que, bien entendu, les lettres en soient placées par lignes horizontales) et les lettres comprises dans la 1re ligne et le chapeau seront les seules qui pourront se trouver sur la 1re ligne du vrai tableau.

On ferait un raisonnement analogue pour la 2e ligne, avec un « chapeau » limité à une lettre au-dessous de la lettre du haut de chaque colonne, puisque la lettre de la 2e ligne est à un intervalle au-dessous de celle de la 1re ligne.

On arrive ainsi à réduire de beaucoup les essais. La lettre Q, du chapeau, si elle est sur la 1re ligne, ne pourra être suivie que de l'un des deux U de la 1re ligne en majuscule.

Faisons alors les essais :

Q	U			Q	U	
B	U	0		B	O	2
O	S	7		O	P	1
M	A	3		M	M	1
P	A	6		P	T	1
E	N	39		E	D	21
		55				26

Nous adopterons la 1re solution et soulignerons le U correspondant. Mais pour que q et *U* puissent se juxtaposer il faut une disposition des colonnes longues et courtes telles que q et U soient sur la même ligne. On l'obtiendra en plaçant les 2 colonnes courtes entre la colonne de U et celle de q, par exemple :

A	*U*	U	D	E	A	R	Q	C
S	U	O	E	C	T	R	B	E
T	S	P	Z	O	S	R	O	E
N	A	M	L	U	E	E	M	O
S	A	T	C	D	D	M	P	N
T	N			E	D	C	E	I

Nous ne savons pas lesquelles des colonnes entre U et Q sont réellement les courtes. Toutefois nous sommes

sûrs que celles de *U* et Q et celles qui leur sont extérieures dans le tableau sont sûrement longues. En rangeant ces dernières à gauche, et les autres douteuses à droite, nous avons :

					e	a		
				d	c	t	r	
Q	U	A	C	U	E	O	S	R
B	U	S	E	O	Z	U	E	R
O	S	T	E	P	L	D	D	E
M	A	N	O	M	C	E	D	M
P	A	S	N	T	E	A	R	C
E	N	T	I	D	C	T		

A considérer les 5 colonnes où, nous en sommes sûrs, les lettres sont bien sur leurs lignes, nous voyons apparaître les mots OBUS et POST :

U	Q	U	A
O	B	U	S
P	O	S	T
M	M	A	N
T	P	A	S
	E	N	T

et nous pouvons faire l'hypothèse que la colonne UO.... a 6 lettres et que le fragment de dernière ligne est DENT.

Pour chercher la colonne suivante, nous prendrons le mot probable POSTE, et nous chercherons un E à la 3e ligne. En prenant le restant du tableau avec le chapeau de la 3e ligne :

TABLEAU

		a		
	c	t	r	
E	O	S	R	
Z	U	E	R	
L	D	D	E	
C	E	D	M	
E	A	R	C	
C	T			

nous voyons que nous n'avons que 2 E capables de venir en 3e ligne, celui de S E D, et celui de R R E.

En essayant la colonne SED, nous voyons se dessiner à la 4e ligne le mot « commande »... seul l'O de la colonne CEEO peut nous le fournir :

C	U	Q	U	A	T
E	O	B	U	S	S
E	P	O	S	T	E
O	M	M	A	N	D
N	T	P	A	S	D
I	D	E	N	T	R

En prenant le 1er C de la colonne EZLCEC qui seul peut convenir, on voit apparaître suffisamment d'éléments pour finir la traduction :

R	E	C	U	Q	U	A	T	O
R	Z	E	O	B	U	S	S	U
R	L	E	P	O	S	T	E	D
E	C	O	M	M	A	N	D	E
M	E	N	T	P	A	S	D	A
C	C	I	D	E	N	T		

Nous avons ainsi montré comment on peut, connaissant le nombre de colonnes du tableau, accélérer les recherches, en limitant, lorsqu'on a choisi la première lettre

d'un bigramme dans le tableau, la zone où chercher la seconde.

Cette méthode a une application intéressante lorsqu'on connaît un mot du cryptogramme.

Plusieurs fois pendant la guerre, les postes T. S. F. ont intercepté des conversations de ce genre :

Poste X à Poste Y. — ISSTE PNLES UOSCO AFMER UEORN OPRTC UTPEY G.

Poste Y à Poste X. — Télégramme brouillé. Quel est le mot avant Foug?

Poste X à Poste Y. — Nancy Toul.

Nous devons donc trouver dans le cryptogramme les lettres de ces noms. Un certain nombre de ces lettres ne se trouvent qu'une fois, plaçons-les aux intervalles qu'elles doivent occuper, en les mettant en colonne avec les lettres voisines :

O . T E . . . N
A . C Y . . . L
F . U G . . . E

Nous voyons que dans le cryptogramme C et Y sont à intervalle de 5; les colonnes auront donc ou 4, ou 5, ou 6 lettres. D'ailleurs, d'après la série Nancy—Toul—Foug, ou l'Y et le G sont dans la même colonne, la clef a 8 lettres, ce qui nous amène (36 lettres divisé par 8) à 4 lignes complètes et 1 ligne de 4, soit 4 colonnes de 5 et 4 colonnes de 4.

Prolongeons alors nos colonnes ci-dessus vers le haut :

S . P T . . . E
C . R P . . . P
O . T E . . . N
A . C Y . . . L
F . U G . . . E

En nous reportant au cryptogramme, nous voyons que cette dernière colonne doit être arrêtée à L, car il ne res-

terait que 3 lettres pour la colonne suivante avant SCO. Pour compléter NANCY et FOUG, nous ferons appel à la séquence EORNO. La nécessité de trouver T, O et U de Toul en bas de colonnes, et la coupure des tranches déjà prélevées sur le cryptogramme, donne immédiatement la solution : « Septième corps se portera sur Nancy, Toul, Foug. »

Mais on peut ne pas trouver autant de lettres faciles à placer sans hésitation parce qu'elles ne figurent qu'une fois dans le document.

Soit le cryptogramme de 47 lettres :

RTEUR DLNLB TGRIL EINTA IDAEE YNARR IRMUD EAHAA TRIQE EB.

où nous soupçonnons la présence du nom de village : Trambly. Servons-nous de cette hypothèse pour chercher à déterminer la longueur de la clef. D'après ce que nous savons des habitudes de l'autorité qui a donné cette clef au chiffreur, elle ne doit pas avoir plus de 10 lettres, ni moins de 5.

Nous considérerons d'abord comment avec des clefs de 6, 7, 8, 9, 10 lettres on peut construire un tableau contenant 47 lettres; puis nous verrons si dans ce tableau nous pouvons, avec les éléments du cryptogramme, installer le mot Trambly, en nous servant des lettres b et y (y ne vient qu'une fois dans le document, b y figure deux fois. — Nous ne ferons pas emploi de l'm, qui ne vient qu'une fois, pour ne pas retomber sur le cas précédent. En réalité, on en ferait naturellement usage.)

Le cryptogramme de 47 lettres se composera :

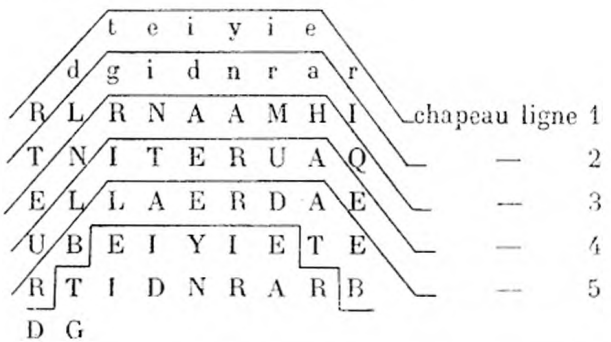
En clef de	6	lettres, de	5	colonnes de	8	lettres et	1 de 7
—	7	—	5	—	8	—	2 de 6
—	8	—	7	—	6	—	1 de 5
—	9	—	2	—	6	—	7 de 5
—	10	—	7	—	5	—	3 de 4

Les intervalles des deux b à y sont de 16 et 21 lettres.

Ces intervalles peuvent-ils être réalisés (pour que b et y soient juxtaposés) :

En clef de 6, celui de 16, par 2 colonnes de 8; celui de 21 : non.
En clef de 7, celui de 16 : non; celui de 21 : 3 de 7.
En clef de 8, celui de 16 : non; celui de 21 : non.
En clef de 9, celui de 16 : 1 de 6 et 2 de 5; celui de 21 : 1 de 6, 3 de 5.
En clef de 10, celui de 16 : non; celui de 21 : non.

Essayons la clef de 9, et mettons notre cryptogramme sur 2 colonnes de 6 lettres et 5 de 4 :



Faisons le chapeau, en supposant que le cryptogramme commence par les 5 colonnes courtes.

Nous voyons que Y pourrait être à la 1re ligne, mais alors pas de B à y juxtaposer. Il pourrait être à l'avant-dernière et nous avons un B à la même ligne, plus un L à la ligne d'au-dessus que nous pouvons faire descendre, en amenant 1 colonne de 6 et 2 colonnes de 5 à séparer B et Y :

R	D	T	I	D	N	R	A	R
T	L	G	N	A	A	M	H	I
E	N	R	T	E	R	U	A	Q
U	L	I	A	E	R	D	A	E
R	B	L	I	Y	I	E	T	E
		E						B

Mais, comme les contours nous l'indiquaient (et cela rendait inutile dans la pratique la constitution de ce dernier tableau), si dans le contour du chapeau de la ligne 4 nous trouvions TRABLY, nous ne pouvions y faire entrer l'M. Pour le même motif, nous ne réussirons pas avec le 2e B, lorsque nous aurons amené Y sur la même ligne en disposant les colonnes intermédiaires en 3 colonnes de 5 et 1 de 6 :

R	L	G	I	D	N	M	H	I
T	N	R	N	A	A	U	A	Q
E	L	I	T	E	R	D	A	E
U	B	L	A	E	R	E	T	E
R	T	E	I	Y	I	A	R	B
D					R			

L'examen des chapeaux pouvait donc nous éviter l'établissement de ces deux tableaux.

La clef de 9 ne donne donc rien.

Essayons la clef de 7 :

		r	a	n	u	
	l	i	i	a	d	t
R	N	L	D	R	E	R
T	L	E	A	R	A	I
E	B	I	E	I	H	Q
U	T	N	E	R	A	E
R	G	T	Y	M	A	E
D	R	A	N	U	T	B
L	I	I	A	D		

Nous savons que nous ne pouvons amener le 1er B à se juxtaposer à Y. Quant au second, la dernière lettre du texte, le contour inférieur nous montre immédiatement qu'il peut s'y juxtaposer. Le seul L que nous puissions prendre pour le trigramme est celui de la 1re colonne. Le B devra donc être abaissé de 1 ligne et l'Y de 2, ce

qui est possible en laissant l'L à sa place, puisque nous avons 2 colonnes entre L et B pour donner les 2 lettres du chapeau. Quant au reste du nom TRAM, nous en avons également les éléments dans les limites des abaissements possibles, et sur des colonnes différentes, mais la nécessité de garder 2 colonnes courtes ne permet pas de descendre *à la fois du maximum* toutes les lettres du contour; il faudra que notre mot soit sur deux lignes et on aura le tableau :

R	N	I	A	N	U	T
T	L	L	I	A	D	R
E	B	E	D	R	E	I
U	T	I	A	R	A	Q
R	G	N	E	I	H	E
D	R	T	E	R	A	E
L			Y	M	A	B

La reconstitution de l'ordre des lettres de TRAMBLY donne le cryptogramme (clef Rosalie).

U	N	T	R	A	I	N
D	A	R	T	I	L	L
E	R	I	E	D	E	B
A	R	Q	U	A	I	T
H	I	E	R	E	N	G
A	R	E	D	E	T	R
A	M	B	L	Y		

Nous arrêterons ici ces exemples de travaux sur les transpositions simples où nous nous sommes efforcé d'attirer l'attention du lecteur sur de nombreuses remarques pouvant faciliter l'obtention du résultat. On peut estimer que pour réussir dans la résolution de problèmes relatifs aux transpositions, il faut beaucoup plus d'expérience et d'aptitude spéciale que pour les problèmes de substitutions relativement simples que nous avons exposés. Les débutants semblent généralement ne pas

savoir « par quel bout » prendre une transposition, lorsqu'ils n'ont ni mot probable, ni q suivis d'u, ni indication sur la longueur de la clef. Nous ne saurions trop recommander de faire des hypothèses, d'essayer quelque chose et de ne pas rester à contempler le cryptogramme pendant des journées entières. Souvent un point de départ faux conduit à des considérations ou à des juxtapositions de lettres qui mettent sur la bonne voie.

L'emploi des bandes de papier sur lesquelles on écrit les colonnes hypothétiques, et qu'on cherche à juxtaposer, fait souvent apparaître des groupements de lettres intéressants qui amorcent les solutions.

Il faut remarquer que, lorsqu'on connaît les habitudes des chiffreurs en ce qui concerne la clef, il est bon de se rendre compte immédiatement des longueurs extrêmes des colonnes. Par exemple, si le chiffreur a l'habitude des clefs de 15 à 25 et qu'on ait un texte de 150 mots, on saura que les colonnes ont environ de 10 à 6 lettres. De très longues séquences de consonnes, qui d'après les fréquences normales doivent être très fréquemment suivies de voyelles, amèneront probablement une séquence où les voyelles seront en majorité, et on la cherchera dans le cryptogramme. Deux ou trois m dans une séquence de 10, et des m, b, ou p à des intervalles égaux à ceux des m seront intéressants à rapprocher si les colonnes ont plus de 10 lettres, et ne le seront plus si les colonnes sont très courtes, parce qu'il y aura peu de chances que les colonnes se juxtaposent dans le même ordre pour le premier m, qui vient d'une colonne, et le dernier, qui vient d'une autre.

Dès qu'on aura des trigrammes à peu près certains, on fera des hypothèses sur la longueur des colonnes et le début des tranches qui y correspondent, ce qui permettra de chercher vers la 3e lettre de la tranche hypothétique le u qu'on cherche pour le juxtaposer à un q, supposé à la 3e ligne du tableau, et de laisser de côté les u occupant dans les tranches des places trop éloignées, etc... et dès qu'on verra apparaître des éléments de mots probables, il faudra en faire état. La connaissance des questions qui

peuvent intéresser les correspondants, de la carte pour les opérations de guerre, des noms des personnalités politiques pour la diplomatie, etc..., est bien plus nécessaire, pensons-nous, quand on travaille sur des systèmes de transposition que sur des systèmes de substitution, à égalité de complication des procédés dans les deux systèmes, et c'est pour cela qu'à notre avis les procédés de transposition sont en général plus sûrs que les systèmes de substitution, lorsque l'on veut pouvoir faire chiffrer à des gens peu idoines des communications nombreuses.

Grilles. — Nous passerons à un autre système de transposition classique, celui où l'on emploie des grilles (1).

La grille est un morceau de carton présentant des ouvertures telles que, si on l'applique sur une feuille de papier, certaines parties de cette feuille sont visibles à travers les ouvertures ou trous et d'autres sont cachées. Supposons que l'on écrive à travers les trous une phrase, par lettres ou par mots, puis qu'on enlève la grille et qu'on complète les lignes de la feuille de papier, entre les inscriptions faites à travers les trous, au moyen de lettres ou de mots bien choisis : il pourra être impossible de distinguer les inscriptions faites à travers la grille de celles qu'on aura faites ensuite, et ainsi les mots ou lettres du message clair seront noyés dans une série de lettres ou de mots qui empêcheront de retrouver le sens. La feuille de papier ainsi traitée sera envoyée au correspondant, qui, muni d'une grille analogue à celle qui a servi au chiffreur, l'appliquera sur le document et lira à travers les trous la phrase intéressante, tous les caractères ajoutés après coup étant cachés.

On ne peut employer un système de ce genre avec le télégraphe qu'à condition d'écrire le texte du cryptogramme sur un papier quadrillé ou repéré de manière à

(1) On emploie quelquefois, à tort, selon nous, le nom de grille pour de simples tableaux de transposition, particulièrement en chiffres plutôt qu'en lettres.

replacer chaque lettre à la place même où elle se trouvait sur la minute du chiffreur.

Sous cette forme, la méthode exige l'envoi de tout le texte inutile qu'on a écrit après l'enlèvement de la grille pour noyer le texte utile. Ce n'est donc pas très pratique surtout pour les télégrammes.

L'ordre dans lequel on écrit les caractères dans les cases peut être fixé par une convention : lignes, colonnes, ou numéros au-dessus des cases pour fixer l'ordre de leur emploi.

Afin de diminuer le nombre des nulles, on aurait intérêt à employer le plus grand nombre de cases utiles, de trous dans la grille. Mais si les lettres, écrites dans ces trous, sont trop rapprochées et dans un ordre simple, par lignes par exemple, on arrivera à deviner les mots malgré les lettres nulles qu'ils renfermeront. C'est pour cela qu'on emploie parfois des numérotages des trous qui changent de lignes et de colonnes les lettres successives d'un mot. On peut même, en employant simplement un tableau de cases numérotées, et appliquant dessus un papier transparent, écrire les lettres du texte clair dans l'ordre des numéros en employant toutes les cases. Le cryptographe employé dans l'armée française en 1886, formé de réglettes sur lesquelles étaient inscrits des numéros, et qu'on plaçait dans un ordre correspondant à une clef, indiquait par la succession de ses numéros l'ordre dans lequel on devait relever les lettres du texte clair écrites dans un tableau quadrillé.

Dans cet ordre d'idées, on emploie parfois les grilles uniquement pour déterminer l'ordre de relèvement des lettres d'un texte, écrites par lignes dans les trous d'une grille et relevées par colonne. Cela revient à faire un tableau de transposition où des blancs existent dans les lignes et les colonnes, et où par suite la juxtaposition des colonnes voisines devient fort difficile. On ne s'occupe plus de nulles, et on envoie par télégraphe le texte ainsi relevé.

Exemple :

L . A T R . O . I
S I . E . M E . D
. I V I S . I O .
N .

LSNII AVTEI RSMOE IOID.

Le résultat obtenu par le procédé du tableau de cases numérotées indiqué un peu plus haut, c'est-à-dire l'emploi utile de toutes les cases et la suppression des nulles, peut être obtenu aussi par l'emploi simultané de plusieurs grilles, percées de trous différents ne se correspondant jamais, et telles que si on les applique successivement sur un même quadrillage toutes les cases auront finalement été découvertes et employées lorsque toutes les grilles auront été mises en place successivement. On commence à écrire dans les trous de la première grille placée seule; on l'enlève; puis on place la deuxième et on écrit dans ses trous, qui découvrent des parties couvertes par la première grille et couvrent toutes les cases découvertes par celle-ci. On fait de même avec la troisième grille, qui découvre des cases restées blanches, etc... A la fin, après emploi de la dernière grille, on a un mélange de lettres appartenant à des parties successives du texte, qu'on peut relever et envoyer, et qui n'est pas encombré de nulles inutiles.

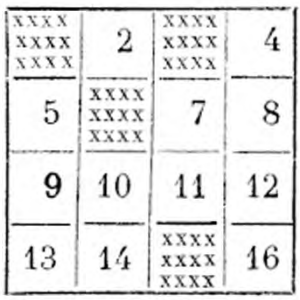
Nous n'insisterons pas sur le déchiffrement de ces systèmes; il rentre dans le cas général que nous étudierons plus loin, le mélange des lettres n'obéissant qu'à des conventions absolument arbitraires. Mais, comme suite à l'emploi de grilles multiples venant tour à tour découvrir toutes les cases de la feuille de chiffrement, nous examinerons le cas des grilles tournantes.

Une grille tournante est une grille généralement carrée, percée de telle manière que, lorsqu'on la place sur un tableau de chiffrement dans des positions successives résultant pour la grille carrée de rotations de 90° chaque fois, toutes les cases du tableau ont été successivement

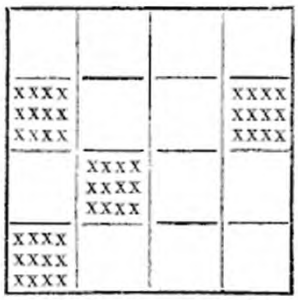
découvertes une fois chacune. Les cases ouvertes dans la grille sont donc égales en nombre au quart du total des cases.

L'emploi d'un semblable appareil entraîne un certain nombre de conséquences. Considérons une grille de 4 cases de côté dans ses quatre positions :

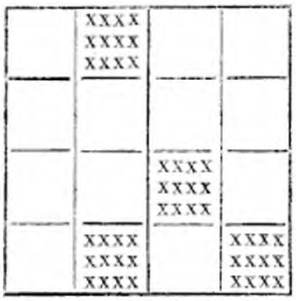
I



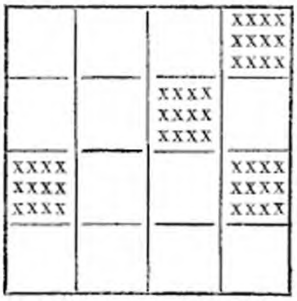
II



III



IV



et numérotons les cases de 1 à 16 par lignes horizontales; on voit comme cases découvertes :
position 1 : 1, 3, 6, 15;
position 3 : 16, 14, 11, 2.

Chaque case ouverte de la position 1 a une symétrique dans la position 3, si bien qu'à la succession de lettres 1 — 3 — 6 — 15 correspond une autre succession 2 — 11 — 14 — 16. Le fait de reconnaître un tétragramme du clair dans les 4 cases 1 — 3 — 6 — 15 entraîne donc le fait d'en reconnaître un autre dans les cases dont les numéros

font individuellement des totaux de 17 avec les numéros des premières, mais en les prenant en ordre inverse (le tétragramme se lira dans l'ordre 2 — 11 — 14 — 16, tandis que pour avoir des totaux de 17 il faut lire dans l'ordre 16 — 14 — 11 — 2). Les positions 2 et 4 donnent lieu aux mêmes observations.

Or la grille comporte un texte de 16 lettres, coupé pour le chiffrement en tranches de 4. Si donc nous arrivions à distinguer dans le cryptogramme les lettres provenant d'une des 4 tranches du texte clair, nous devons trouver par symétrie les lettres provenant de la tranche conjuguée. Tout bigramme acceptable de la première tranche doit avoir comme correspondant un bigramme acceptable.

Soit donc le texte :

NVCOS RITIY SXEII ETEMO STUNR OSNEU DAIEL P.

chiffré à l'aide d'une grille tournante, et où nous soupçonnons la présence du mot division. Nous adoptons un mot probable ; sinon on aurait recours à des essais successifs comme pour un tableau de transposition dans lequel on n'aurait pas d'entrée évidente, mais cela ne serait pratique qu'avec un peu plus de matériaux. Remarquons qu'avec les grilles il est fréquent d'avoir un texte plus long que le nombre de cases de la grille, et qu'alors on coupe le texte en tranches égales à ce nombre de cases, en complétant la dernière avec des nulles. La possession de documents ayant toujours une longueur égale à des multiples d'un même nombre, deuxième puissance d'un nombre donné, révèle des chiffrements par grille tournante.

Nous allons, pour appliquer plus facilement la symétrie que nous avons signalée, d'après laquelle chaque case d'une des positions 3 et 4 est la symétrique d'une case d'une des positions 1 et 2, écrire ce cryptogramme sur 2 lignes symétriques ; la deuxième étant formée du texte de la première lu de la fin au commencement.

NVCOS RITIY SXEII ETEMO STUNR OSNEU
PLEIA DUENS ORNUT SOMET EIIEX SYITI
DAIEL P
RSOCV N

Chaque bigramme formé avec 2 lettres successives du clair dans une des lignes correspond dans l'autre ligne à un autre bigramme du clair, lu à l'envers.

Plaçons maintenant le cryptogramme sur un tableau de 36 cases qui reproduira le tableau de chiffrement :

N	V	C	O	S	R	1	2	3	4	5	6
I	T	I	Y	S	X	7	8	9	10	11	12
E	I	I	E	T	E	13	14	15	16	17	18
M	O	S	T	U	N	19	20	21	22	23	24
R	O	S	N	E	U	25	26	27	28	29	30
D	A	I	E	L	P	31	32	33	34	35	36

Nous savons qu'il y a 9 cases ouvertes, soit probablement 1 ou 2 à chaque ligne. Les lettres successives b'un même mot ne doivent donc probablement pas être éloignées de plus d'une ligne, de plus de 6 places.

Cherchons les lettres du mot division supposé dans le texte clair.

Nous n'avons qu'un D — 31. Le 1er I est I^{33}, puis vient I^{7} qui est bien loin.

Le bigramme symétrique de DI est OR, acceptable. Comme DI est la dernière ligne, la suite a été chiffrée dans une nouvelle position de la clef. Nous remarquerons tout de suite que dans cette nouvelle position, les cases ouvertes sur 31 et 33 se sont transportées sur 36 et 24; mais que, par suite de la construction de la grille, les cases 16 et 6, qui devront être ouvertes dans la 3e position, et les cases 1 et 3, qui devront être ouvertes dans la 4e, sont certainement fermées; si donc nous trouvions un V dans les cases 1, 3, 6, ce ne serait certainement pas celui que nous cherchons.

Nous avons V^{2}. Pour l'I suivant, nous hésitons entre

I^7 et I^9; pour S, nous ne disposerons que de S^2; puis, nouvelle hésitation entre I^{14} et I^{15}, et probabilité pour O^{20} et N^{24}.

Voyons ce que donnent les symétriques de ces diverses hypothèses :

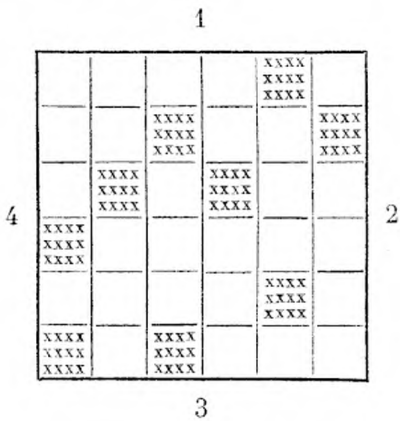
$V^2\ I^7\ S^{11}\ I^{14}\ O^{20}\ N^{24}$ = ETUOUL

$V^2\ I^9\ S^{11}\ I^{15}\ O^{20}\ N^{24}$ = ETTONL

On voit que la solution est :

$V^2\ I^7\ S^{11}\ I^{15}\ O^{20}\ N^{24}$ = ETTOUL

Nous avons reconstitué la grille à une case près. En la présentant sur le tableau, et la ramenant à la première position, nous voyons immédiatement que la case à ouvrir est la case 29, et nous avons :



avec le texte : 6e division se portera sur Nancy et Toul.

Avec un mot probable, relativement long par rapport à la grille, nous sommes arrivés assez vite au but. Quand les données sont moins avantageuses, il faut avoir soin d'utiliser à plein tous les éléments d'étude : il faut, dès que l'on a fait une hypothèse sur la grille, vérifier si, dans l'une quelconque des 4 positions, cette hypothèse peut donner lieu à une remarque utile. En particulier, il faut avoir soin de restreindre le champ des hypothèses

ultérieures en remarquant quelles sont les cases qui découvriront *dans une autre position* les trous que l'on vient de déceler dans la grille, et en tenant compte de ce que, par suite, *ces cases sont couvertes* dans la position actuelle et ne peuvent fournir aucun élément du texte clair dans ladite position.

Enfin, il faut se rappeler, en travaillant sur les grilles, que l'emploi de nulles y est très fréquent, et peut amener des bigrammes incohérents.

Anagrammes. — En dehors de ces cas particuliers, nous ne savons résoudre les systèmes de transposition que par la juxtaposition *a priori* des lettres qui s'y trouvent pour former des mots, au mieux, et sans procédé spécial, c'est-à-dire par la formation d'un anagramme constituant un texte clair.

Quand on ne dispose que d'un seul cryptogramme pour ce travail, on peut parfois former plusieurs anagrammes sans que rien vienne indiquer quel est le bon.

Quand on dispose d'un texte de vérification, on peut échapper à cet écueil. La plupart des procédés de transposition sont tels que si l'on opère sur deux textes de même longueur, chaque lettre de l'un subit exactement les mêmes tribulations que la lettre qui occupe, dans l'autre, le même rang à partir du début, et se trouve à la même place dans le cryptogramme. Dès que les textes sont de longueurs différentes, les lettres de l'un subissent des opérations qui les envoient souvent fort loin de la place qu'occupent dans l'autre cryptogramme les lettres de même rang de l'autre texte clair. On ne peut donc, dans la généralité des cas, travailler utilement que sur des cryptogrammes ayant un même nombre de lettres, pour vérifier sur l'un toute hypothèse faite sur l'autre.

Soient par exemple les deux cryptogrammes :

NNYCT OUAIL PPDLU ATEOR R
BUGRI LAOQS ATAUA NVTRS D

Dans le premier, nous voyons dans les premiers grou-

pes qu'une partie des lettres forme les mots NANCY et TOUL.

Il reste alors IPPDLUATEORR.

Étant données la présence de noms de pays, et les lettres dont nous disposons, nous ferons encore comme anagramme DE et POUR. Il reste IPLATR = IL PART.

Mais part-il de Nancy pour Toul, ou de Toul pour Nancy? La présence du 2e cryptogramme nous renseignera :

IL PART DE nous donne, en plaçant dans le même ordre les lettres correspondantes : QUAND VA T.

Les lettres correspondantes à TOUL donnent ILAS.

Celles qui correspondent à NANCY donnent BOURG et à POUR = TRAS.

On doit donc lire : Quand va-t-il à Strasbourg?

et : Il part de Toul pour Nancy.

Quand on a plusieurs cryptogrammes de même longueur, on peut utiliser pour former les anagrammes les considérations connues sur les sommes des fréquences pour essayer des bigrammes, et traiter le problème sans avoir besoin du mot probable, en partant dans un des textes d'un bigramme probable et en vérifiant sur les autres textes.

Dans le cas des transpositions à tableau, le déplacement des lettres d'un cryptogramme à l'autre, lorsque les textes ne sont pas de la même longueur, est soumis à des lois assez simples pour qu'on puisse faire état de deux cryptogrammes de longueurs différentes.

Les lettres supplémentaires s'ajoutent au bas des colonnes dans un chiffrement à tableau classique comme celui que nous avons examiné. Deux ou trois lettres de plus à un des textes qu'à l'autre pourront donc n'apporter aucune perturbation à toute une série de colonnes, et si ce sont les premières relevées, les lettres à une même distance du début des deux textes clairs seront à une même distance du début du cryptogramme. Si l'un des textes est double, triple de l'autre, les colonnes seront deux fois, trois fois plus longues. S'il y a 10 colonnes par exemple, les lettres de la première ligne seront pour les 2 crypto-

grammes dans le voisinage des séparations en 10 tranches égales à une lettre près. On possède donc, lorsqu'on a des mots probables pour le commencement ou la fin des textes par exemple, le moyen de limiter dans chaque cryptogramme les recherches à des régions définies et qui se correspondent. Mais tout ceci, dans la pratique, est d'un emploi bien limité.

Recherche de la clef. — Lorsqu'on a pu reconstituer un texte clair par anagramme, il est de la plus haute importance de reconstituer la clef, puisqu'elle permettra de traduire des cryptogrammes dont la longueur sera différente de celle du texte reconstitué. L'opération diffère suivant le procédé de chiffrement, et il faut analyser en détail le procédé de passage du texte clair au texte chiffré.

Pour donner brièvement l'idée de la manière dont on peut conduire une étude de ce genre, supposons qu'on connaisse le procédé employé pour chiffrer, et qu'on n'ait qu'une clef à retrouver. Ce procédé sera par hypothèse le suivant : Au-dessus du texte clair, on écrit les répétitions d'un mot clef et on relève successivement les lettres du clair correspondant à une même lettre de la clef, les lettres de cette clef étant prises dans un ordre donné (alphabétique par exemple). On obtient ainsi un cryptogramme que nous appellerons cryptogramme primitif. On le traite ensuite avec le même mot clef comme on a traité le clair, pour avoir le cryptogramme final.

Exemple :

1re opération	A M I E N S A M I E N S A M I E N S A
	L a c i n q u i è m e d i v i s i o n
Crypto primitif	L U I N I M S C E I A I V N E I Q D O
2e opération	A M I E N S A M I E N S A M I E N S A
	L u i n i m s c e i a i v n e i q d o
Crypto final	L S V O N I I I E E U C N I A Q M I D

Nous supposerons, possédant un texte de 46 lettres

chiffré par ce procédé, que nous avons reconstitué l'anagramme, et nous chercherons la solution de la question suivante : étant donnés le cryptogramme et le texte clair, retrouver la clef.

Supposons le problème résolu, la clef étant Bordeaux. Remplaçons chaque lettre par le numéro qu'elle occupe dans le texte en partant du début, et faisons subir à la suite de nombres ainsi obtenue les deux opérations successives. Nous retrouverons ainsi la place qu'occupe dans le cryptogramme chaque lettre du clair.

B O R D E A U X B O R D E A U X
01 02 03 04 05 06 07 08 09 01 11 12 12 14 15 16
B O R D E A U X B O R D E A U X
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
B O R D E A U X B O R D E A
33 34 35 36 37 38 39 40 41 42 43 44 45 46

Cryptogramme primitif : 06, 14, 22, 30, 38, 46, 01, 09 etc...

B O R D E A U X B O R D E A U X
06 14 22 30 38 46 01 09 17 25 33 41 04 12 20 28
B O R D E A U X B O R D E A U X
36 44 05 13 21 29 37 45 02 10 18 26 34 42 03 11
B O R D E A U X B O R D E A
19 27 35 43 07 15 23 31 39 08 16 24 32 40

Cryptogramme final : 46 12 29 42 15 — 40 06 17 36 02 — 19 39 30 41 13 — 26 43 24 38 04 — 21 34 07 32 14 — 25 44 10 27 08 — 22 33 05 18 35 — 16 01 20 37 03 — 23 09 28 45 11 — 31.

Analysons les opérations successives. Le cryptogramme primitif est constitué par des tranches de nombres qui diffèrent entre eux de 8, longueur de la clef. Cette progression de 8 d'un nombre au suivant n'est rompue qu'aux changements de lettre de la clef. Pour constituer le cryptogramme final, on forme des tranches ou séquences

renfermant chacune une lettre de chaque tranche du cryptogramme primitif, ces lettres se suivant dans le même ordre. Il y a parallélisme entre ces séquences; si la première lettre de l'une, correspondant à l'A du premier mot clef, Bordeaux, par exemple, diffère de 8 ou de 16 de la première lettre d'une autre correspondant à l'E ou au D, les autres lettres, correspondant à l'A des mots clefs successifs, diffèrent de 8 de ou 16 des lettres de même rang de la séquence, correspondant aux E et aux D des mots clefs (sous réserve de rupture de la progression dans le cryptogramme primitif). Si bien qu'en ajoutant 8 ou un multiple de 8 aux différents nombres d'une séquence, on doit retrouver la succession des nombres d'une autre, ou du moins une partie de cette succession. Partant de cette remarque, constatons qu'inversement si, sur une tranche du cryptogramme fait avec une clef de longueur inconnue, nous faisons des essais successifs en ajoutant à chaque nombre de cette tranche une même quantité, et si nous retombons ainsi sur une autre tranche du cryptogramme, nous aurons trouvé probablement la longueur de la clef. Supposons que nous ignorions ici cette longueur, et essayons d'ajouter 7, 8, 9, 10, etc... à chacun des chiffres d'une tranche d'un cryptogramme, par exemple aux 20 derniers nombres :

	44	10	27	08	22	33	05	18	35	16
+ 7	51	17	34	15	29	40	12	25	42	23
+ 8	52	18	35	16	30	41	13	26	43	24
+ 9	53	19	36	17	31	42	14	27	44	25
	01	20	37	03	23	09	28	45	11	31
+ 7	08	27	44	10	30	16	35	52	18	38
+ 8	09	28	45	11	31	17	36	53	19	39
+ 9	10	29	46	12	32	18	37	54	20	40

. . . . . .

nous voyons apparaître à la ligne correspondant à + 8 des séquences du cryptogramme :

18.35.16. — 30.41.13.26.43.24. — 09.28.45.11.31. — 17.36. — 19.39. —

Nous avons 46 lettres au texte, et 8 à la clef; les tranches auront donc 6 lettres pour les 6 premières lettres de la clef, 5 pour les 2 dernières. Les successions reconstituées de 6 et de 5 lettres conformes à celles que l'on peut tirer intégralement du cryptogramme final seront alors probablement des tranches entières correspondant à une lettre de la clef, 18.35.16 sera une fin de tranche, 17.36 sera un début de tranche puisqu'il suit une tranche complète.

Mais une séquence du cryptogramme final doit avoir, à quelques exceptions près, ses nombres égaux à ceux de la séquence qui correspond à la lettre précédente du mot clef, augmentés de 8. La séquence correspondant à la lettre à gauche de celle qui donne 30.41.13.26.43.24 doit donc être 22.33.05.18.35.16. Nous avons bien cette séquence dans le cryptogramme. On reconstituera ainsi de proche en proche l'ordre des tranches, et on retrouvera la clef numérique dont on a déjà la longueur.

Revenant à notre problème, dont les données sont le texte clair, où figurent les lettres qui s'y trouvent dans l'ordre 01, 02....46, et le cryptogramme, où ces lettres sont mélangées, on voit comment, en remplaçant les lettres du cryptogramme par le numéro que chacune d'elles porte dans le clair, ce qui donnera 46.12.29...11.31, on pourra essayer d'additionner un même nombre à une séquence du cryptogramme pour retrouver une autre séquence. Les difficultés peuvent, dans la pratique, provenir de plusieurs sources. On pourra difficilement identifier une lettre du clair, un A par exemple, avec un A donné du cryptogramme s'il y a plusieurs A, et par suite l'ordre de numérotage du cryptogramme sera douteux et les séquences seront brouillées. Cet obstacle sera surmonté si l'on a plusieurs anagrammes de même longueur, les incertitudes de l'un étant tranchées par l'autre. On se trouvera également dans un cas désavantageux si la clef est longue et si les ruptures de séquences dans le cryptogramme primitif sont très nombreuses avec des séquences très courtes. Mais le principe de la méthode reste le même.

Nous n'étendrons pas plus loin cette étude, et nous ne

la généraliserons pas. Nous avons voulu montrer comment on pouvait analyser un procédé de transposition, et, supposant le problème résolu, étudier les moyens de trouver la clef inconnue au moyen d'un cryptogramme, quand on possédait la traduction du cryptogramme. C'est cette dernière condition qui est ordinairement la plus difficile à réaliser. Les imprudences de chiffreur apportent quelquefois à ce sujet un secours important au décrypteur, mais c'est surtout sur la connaissance de la langue du document et sur une grande expérience technique, que celui-ci doit compter pour réussir des anagrammes.

Nous avons dit que les transpositions, surtout du type grilles, pouvaient s'appliquer non seulement aux lettres, mais aux polygrammes ou aux mots. Nous n'insisterons pas sur ces questions : certains romans historiques font état, par exemple, de messages ou 3 mots sur 4 sont nuls, le texte avec les nulles formant un sens, et les seuls mots utiles $= n$, $n + 4$, $n + 8$ etc., en formant un autre. Les mélanges des mots d'un texte clair donnent souvent des cryptogrammes très suffisamment incompréhensibles pour fournir des problèmes intéressants; il faut presque toujours s'adresser à la méthode de l'anagramme, heureux si un second texte permet de vérifier les hypothèses faites sur le premier.

CHAPITRE XIII

SUPERPOSITIONS DE PROCÉDÉS

Lorsque des correspondants ne trouvent pas que la sécurité obtenue par un chiffrement du texte est assez grande, ils font souvent subir au premier cryptogramme, considéré comme un texte clair, un deuxième chiffrement, qu'on appelle quelquefois surchiffrement. Lorsque les deux procédés sont bien choisis, il en résulte en effet un fort accroissement de sécurité; mais, parfois, le résultat est illusoire, et la sécurité n'est qu'égale à celle qu'offrait le premier procédé, sinon même inférieure.

Nous n'avons pas la prétention d'examiner tous les systèmes possibles. D'ailleurs, ce ne sont plus là des études introductives à la cryptographie, mais des études cryptographiques exigeant des connaissances assez étendues et l'habitude d'analyser des cryptogrammes. Nous prendrons donc seulement quelques exemples, pour indiquer dans quel ordre d'idées ces méthodes sont établies, doivent être critiquées avant adoption, et peuvent donner lieu à des recherches des décrypteurs.

Substitution simple. — Un texte étant chiffré avec une substitution simple, le surchiffrement avec une autre substitution simple ne donne comme résultat qu'une substitution simple. Si A est représenté par E dans le premier cryptogramme et que le second tableau de substitution fasse remplacer E par N, A du clair sera représenté par N du cryptogramme.

Ce n'est donc pas sans étonnement que l'on trouvera dans un volume édité en 1922 un procédé de ce genre décrit comme préférable aux procédés connus « qui ne

donnent pas une sécurité absolue ». A la fin du code Rudolf Mosse on recommande l'emploi du procédé suivant : écrire le texte à chiffrer au moyen d'une écriture stéganographique (semblable à l'alphabet dit des francs-maçons, où les lettres se composent de deux ou trois traits appartenant aux côtés d'un carré ou d'un triangle) où il y a un caractère par lettre de l'alphabet, retourner la page la tête en bas, ce qui met les caractères stéganographiques la tête en bas, et leur fait, dans cette position, représenter d'autres lettres de l'alphabet que lorsqu'ils ont la tête en haut, traduire ces caractères dans cette nouvelle position et écrire le texte ainsi obtenu.

On fait trois substitutions simples, le retournement des caractères la tête en bas n'étant qu'une substitution.

Substitution simple et substitution à double clef. — La superposition des substitutions simples aux substitutions doubles, quel que soit l'ordre de l'opération, peut faire disparaître, dans les cas où l'on se contente d'alphabets normaux pour la substitution double, tous les avantages que ces alphabets offraient au décrypteur. Il ne trouve que des alphabets incohérents lorsque, ayant découvert la longueur de la clef comme pour une substitution à double clef ordinaire, il cherche à découvrir la traduction en clair des lettres du cryptogramme.

Double substitution à double clef. — En employant successivement des substitutions à double clef, ayant des clefs de longueur donnée, on arrive dans le cas général à obtenir, après la deuxième substitution, une substitution à double clef ayant une période égale au plus petit commun multiple de la longueur des deux clefs.

Soit en effet d'abord le cas où les deux clefs ont la même longueur. Chiffrons, en système de Gronsfeld, un texte avec la clef 1324 puis surchiffrons-le avec la clef 0142. Nous avons :

Clair : L a p r e m i e r e d i v i s i o n
1er chiffrement : M D R V F P K I S H F M U L U M P Q
2e chiffrement : M E V X F Q O K S I J O U M Y O P R

On obtient le même résultat que si l'on avait chiffré le texte clair avec la clef 1466, de même longueur que les deux clefs primitives. On remarquera que le chiffrement successif des textes revient à chiffrer les deux clefs l'une par l'autre (1324 chiffré avec la clef 0142 devient 1466) et à appliquer la clef nouvelle au texte clair. On peut ainsi, quand on opère sur des clefs littérales, se servir de deux chiffrements successifs avec des clefs claires pour aboutir à un chiffrement avec une clef incohérente, résultant du chiffrement d'une des clefs au moyen de l'autre avec le tableau carré adopté.

On voit facilement que le texte obtenu en chiffrant avec une clef de 4 et en surchiffrant avec une clef de 6, ou vice versa, donnerait une période de 12. Nous le montrerons encore sur des clefs du système de Gronsfeld.

Soient les clefs : 1 3 2 4, et 1 0 1 2 0 3.

En les appliquant successivement, les décalages de l'une par rapport au texte clair (lettre du texte $+ n$) s'ajoutant aux décalages de l'autre (lettre du texte $+ n + n'$), on a :

1	3	2	4	1	3	2	4	1	3	2	4	1	3	2	4	1	3
1	0	1	2	0	3	1	0	1	2	0	3	1	0	1	2	0	3
2	3	3	6	1	6	3	4	2	5	2	7	2	3	3	6	1	6

Donc, une période de 12. Or, nous savons que le système de Gronsfeld, dans son principe, est absolument analogue au système de Vigenère; on désigne les alphabets à prendre, pour chiffrer chaque lettre, par un intervalle numérique au lieu de les désigner par leur lettre initiale. Notre raisonnement est donc général. Avec des nombres de lettres des clefs premiers entre eux, on peut obtenir des périodes fort longues, et par suite des cryptogrammes difficiles à déchiffrer s'ils sont à un exemplaire unique. Nous ne revenons pas sur les questions du déchiffrement des substitutions doubles à clefs très longues.

Double transposition. — Comme nous avons dit que les transpositions pouvaient affecter des formes très diverses,

et que la convention adoptée pouvait amener à un mélange qui semble échapper à toute loi autre que celle d'un numérotage de lettres établi au hasard par les correspondants, l'opération de mélanger à nouveau les lettres déjà mêlées par un premier chiffrement ne modifiera rien aux principes que nous avons donnés pour étudier les transpositions. On peut appliquer plusieurs fois un procédé simple de transposition, par exemple le système à tableau, et faire 2, 3, etc... transpositions par tableau successives. Sans doute quelques chiffrements par transpositions à loi simple successives pourraient-ils donner lieu à une étude méthodique comme celles que nous avons présentées plus haut. Mais dans la plupart des cas il faudra recourir à la recherche de l'anagramme comme unique méthode de décryptement.

Transposition et substitution. — Restent alors les combinaisons des substitutions et des transpositions. Elles peuvent affecter des formes diverses. Nous en citerons quelques-unes.

En écrivant le texte sur un tableau d'un nombre de lettres donné à la ligne, et considérant les bigrammes formés dans chaque colonne par deux lignes successives pour leur faire subir des substitutions par bigramme, on a une première classe de systèmes :

Exemple : L a q u a t r i e m
e d i v i s i o n

On considère les bigrammes LE. AD. QI. UV. AI. TS. etc..., et on les chiffre. On voit que la fréquence des bigrammes n'intervient plus et que la découverte du sens de quelques-uns ne permet plus de former des hypothèses sur ceux qui les précèdent ou les suivent.

Quand on emploie les substitutions à représentations par groupe de lettres ou de chiffres, on peut, après une transposition assez simple convenablement choisie, revenir à une représentation de chaque groupe par une seule lettre et éviter ainsi la transmission de cryptogrammes

sensiblement plus longs que le texte clair. Soit, par exemple, la substitution faite avec ce tableau :

	Z	Y	X	V	T
M	A	B	C	D	E
N	F	G	H	I	J
O	K	L	M	N	O
P	P	Q	R	S	T
Q	U	V	X	Y	Z

Texte : L a q u a t r i e m
1er crypto. : OY MZ PY QZ MZ PT PX NV MT OX

Texte : e d i v i s i o n
1er crypto. : MT MV NV QY NV PV NV OT OV

Faisons maintenant une transposition quelconque, soit au moyen d'un tableau, soit simplement en laissant la première et la dernière lettre seules et en groupant la dernière lettre de chaque bigramme avec la première lettre du suivant. Remplaçons chaque nouveau bigramme par la lettre qu'il représente au tableau :

O YM ZP YQ ZM ZP TP XN VM TO XM TM
O B P V A P T H D O C E

VN VQ YN VP VN VO TO V
I Y G S I N O V

et l'on aura le cryptogramme OBPVA PTHDO CEIYG SINOV.

Les combinaisons de substitution et de transposition les plus fréquemment rencontrées comportent l'emploi d'une transposition à tableau. Étant donné que, dans la substitution, la lettre du clair peut être représentée par un ou deux caractères, que la substitution peut être simple ou double, que dans le cas des représentations par deux caractères, la transposition peut être faite avant ou après la substitution, laissant subsister l'individualité de chaque

groupe ou le partageant en deux, les procédés sont extrêmement nombreux. Nous en citerons quelques-uns en indiquant, mais seulement d'une façon sommaire, quelles remarques peuvent être utilisées pour trouver la solution.

En général, on a bien peu de chances de retrouver les clefs quand on travaille sur un document unique. Mais nous rappellerons que des exemples nombreux permettent de tenir compte dans une large mesure de la possession de plusieurs cryptogrammes de même longueur, de cryptogrammes ayant des débuts analogues, et même parfois du texte clair de certains cryptogrammes.

La plus grande difficulté est souvent de trouver le nombre de colonnes du tableau de transposition. Des cryptogrammes ayant même début du clair, permettant de reconnaître les hauts de colonnes, donnent parfois la longueur d'une ou plusieurs colonnes : on en tire des hypothèses sur la composition possible du tableau d'après le nombre de lettres en considérant les longueurs de clefs qui comportent les colonnes de longueur égale à celles que l'on possède, les autres étant plus courtes ou plus longues. L'examen des autres cryptogrammes de même clef permet d'éliminer certaines solutions admises d'abord à l'examen. On peut même parfois ranger ainsi les colonnes en longues et courtes, et avec plusieurs cryptogrammes de longueur différente, où le nombre des colonnes longues diffère, on peut arriver quelquefois à reconstituer presque l'ordre des colonnes. D'autres remarques, comme nous le verrons, peuvent aider dans cette recherche.

Substitution simple à représentation mono-alphabétique et transposition. — Pour les cryptogrammes obtenus par substitution simple lettre à lettre et transposition à tableau, l'ordre des deux opérations n'influe pas sur le résultat; on peut substituer avant de mettre en tableau, ou ne substituer que sur le premier cryptogramme obtenu en relevant le tableau.

Un tel cryptogramme présente un tableau de fréquences analogue à celui d'une substitution simple, et, dans la

plupart des cas, on y trouve l'E du clair sans difficulté. Mais les groupements caractéristiques manquent pour trouver les bigrammes dont la formation permet la juxtaposition de deux colonnes voisines.

Si l'on connaît le nombre de colonnes du tableau, on pourra essayer la méthode du mot probable, avec des considérations de la nature de celles que nous avons présentées dans le chapitre « Transposition », en établissant un tableau d'un nombre égal de colonnes par colonnes successives, et en déterminant (Voir la théorie du « chapeau ») la zone où la variation de place des colonnes peut emmener les lettres du mot probable. Les fréquences des caractères du cryptogramme serviront de guide pour tâcher d'identifier les lettres du mot probable avec ces caractères.

Sauf au cas où le mot probable est très caractéristique, soit par des lettres très fréquentes, soit mieux par des lettres rares, cette identification et la détermination de la région du tableau qui doit correspondre au mot probable, sont fort malaisées. Le procédé de chiffrement dont il s'agit, quoique très simple, donne donc, surtout avec des clefs longues et des cryptogrammes courts, une réelle sécurité.

Substitution simple par groupes et transposition. — Pour étudier les cryptogrammes établis par substitution en groupes numériques et transposition, en supposant que la transposition ait été effectuée après la substitution et sépare les éléments des groupes (sinon nous sommes dans le cas précédent), nous supposerons d'abord que la substitution est faite avec le tableau ci-dessous :

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

Chaque lettre est chiffrée par le numéro de la colonne suivi de celui de la ligne, et nous chercherons à élucider ce qui a rapport à la transposition.

Après cette dernière opération nous aurons un cryptogramme qui ne contiendra que les 5 premiers chiffres, ce qui lui donnera un aspect caractéristique.

On fera bien de commencer par compter les fréquences de chaque chiffre.

A ce sujet faisons une remarque. Comptons la somme des fréquences des lettres qui constituent chaque ligne et chaque colonne du tableau :

a :	7	b :	1	c :	4	d :	4	e :	17	TOTAL :	33
f :	1	g :	1	h :	0	i :	7	j :	0	—	9
k :	0	l :	5	m :	3	n :	9	o :	7	—	24
p :	3	q :	1	r :	7	s :	7	t :	7	—	25
u :	7	v :	2	x :	0	y :	0	z :	0	—	9
TOTAUX :	18		10		14		27		31		

Les 1 du cryptogramme proviendront, soit du chiffre de la ligne (2e chiffre du groupe), soit du chiffre de la colonne (1er chiffre du groupe), leur fréquence normale sera donc proportionnelle à 33 + 18 = 55.

De même, la fréquence des 2 serait proportionnelle à . . . . . 9 + 10 = 19
celle des 3 serait proportionnelle à 24 + 14 = 38
celle des 4 — 25 + 27 = 52
celle des 5 — 9 + 31 = 40

Si donc le cryptogramme proposé est bien fait avec un tableau analogue à celui que nous avons choisi, avec les lettres à la même place que dans notre exemple, les fréquences des chiffres devront être proportionnelles à ces nombres.

Une autre remarque est la suivante. Si le tableau de transposition a un nombre pair de colonnes, la 1re ligne contiendra un nombre exact de bigrammes de chiffres représentant des lettres; si ce tableau a un nombre impair de colonnes, un bigramme sera coupé en deux, le 1er chiffre

à la dernière colonne de la 1re ligne, le 2e à la 1re colonne de la 2e ligne. Dans le premier cas (nombre pair de colonnes), chaque colonne du tableau contiendra uniquement soit des premiers chiffres des bigrammes, soit des seconds chiffres. Dans le second cas (nombre impair), il y aura mélange dans chaque colonne, les lignes impaires commençant par un 1er chiffre de bigramme, les lignes paires par un 2e chiffre.

Si nous supposons alors les colonnes connues, et séparées dans le cryptogramme résultant du relevé du tableau par colonnes, dans le premier cas les colonnes impaires devront donner des fréquences basées sur les premiers chiffres des bigrammes, les colonnes paires, des fréquences basées sur les deuxièmes. Or, pour certains chiffres ces fréquences diffèrent beaucoup : les 5, premiers chiffres des bigrammes, à cause de l'E (51), sont bien plus fréquents que les 5, deuxièmes chiffres (31 contre 9); les 1, deuxièmes chiffres, sont bien plus fréquents que les 1, premiers chiffres (33 contre 18). On devra retrouver ces caractéristiques dans les tranches du télégramme correspondant aux colonnes, même si elles ne sont pas assez nettes pour permettre de distinguer la fin d'une colonne et le commencement d'une autre. Dans le cas d'un tableau d'un nombre impair de colonnes, cette caractéristique disparaît, la répartition étant sensiblement uniforme, mais elle se retrouverait en considérant à part les chiffres de rang pair des tranches et les chiffres de rang impair, si les colonnes étaient assez longues pour qu'une loi puisse s'y retrouver.

On peut donc, de l'examen de plusieurs textes, déterminer, en vue d'essais tout au moins, le nombre de colonnes du tableau.

Ceci fait, on peut, par des études de fréquence, chercher les accouplements de colonnes, en admettant que le meilleur accouplement est produit par les deux colonnes qui donnent le plus grand nombre de lettres *e*.

Soit par exemple le cryptogramme :

25534 45414 51143 13441 13353 11423 13121 55
135 35341 24244 12141 45311 45525 45322 55

On y distingue au moyen des 5 et des 1, avec une approximation suffisante, 6 colonnes se suivant dans l'ordre : 1 impaire, 2 paires, 1 impaire, 1 paire, 1 impaire. Comme le nombre des lettres du cryptogramme est divisible par 6, toutes les colonnes sont égales, et nous n'aurons pas d'hésitation sur les colonnes longues et les colonnes courtes (hésitations qui devraient, soit être admises et donner lieu à des essais multiples, soit être tranchées, par exemple, par de multiples télégrammes, permettant de faire des hypothèses sur le commencement et la fin des colonnes).

Coupons alors le cryptogramme en 6 tranches égales :

I. — 255344541451	II. — 143134411335
III. — 311423131215	IV. — 513535341242
V. — 441214145311	VI. — 455254532255

et cherchons à juxtaposer les tranches en les plaçant en colonnes. Nous ne ferons le travail qu'en supposant déterminées les colonnes paires et les colonnes impaires, et n'essaierons par suite que la juxtaposition d'une colonne paire à une colonne impaire. Mais, si l'on n'était pas sûr de la parité des colonnes, on ferait l'essai sur toutes les colonnes.

Juxtaposons successivement aux tranches I, IV et VI les tranches II, III et V :

A	B	C	D	E	F	G	H	I
I II	I III	I V	IV II	IV III	IV V	VI II	VI III	VI V
2 1	2 3	2 4	5 1	5 3	5 4	4 1	4 3	4 4
5 4	5 1	5 4	1 4	1 1	1 4	5 4	5 1	5 4
5 3	5 1	5 1	3 3	3 1	3 1	5 3	5 1	5 1
3 1	3 4	3 2	5 1	5 4	5 2	2 1	2 4	2 2
4 3	4 2	4 1	3 3	3 2	3 1	5 3	5 2	5 1
4 4	4 3	4 4	5 4	5 3	5 4	4 4	4 3	4 4
5 4	5 1	5 1	3 4	3 1	3 1	5 4	5 1	5 1
4 1	4 3	4 4	4 1	4 3	4 4	3 1	3 3	3 4
1 1	1 1	1 5	1 1	1 1	1 5	2 1	2 1	2 5
4 3	4 2	4 3	2 3	2 2	2 3	2 3	2 2	2 3
5 3	5 1	5 1	4 3	4 1	4 1	5 3	5 1	5 1
1 5	1 5	1 1	2 5	2 5	2 1	5 5	5 5	5 1

Si nous considérons alors les fréquences des différents bigrammes, nous avons :

	A	B	C	D	E	F	G	H	I
11	1	1	1	1	2				
12									
13									
14				1		1			
15	1	1	1			1			
21	1					1	2	1	
22								1	1
23		1		1		1	1		1
24			1					1	
25				1	1				1
31	1				2	3	1		
32			1		1				
33					2			1	

	A	B	C	D	E	F	G	H	I
34			1		1				1
35									
41	1			1	1	1	1	1	
42			2						
43	2	2	1	1	1			2	
44	1		2			1	1		2
45									
51			4	3	2			4	5
52						1		1	
53	2				2		3		
54	2		1	1	1	2	2		1
55							1	1	

Nous remarquerons dans ce tableau, où les solutions justes sont les combinaisons B D I, que les plus fortes fréquences portent sur l'E (51) et que les solutions fausses ne présentent souvent aucune fréquence un peu forte, les bigrammes se répartissant sur l'échelle des nombres, à moins que, par un hasard qui pourrait perdre son poids à mesure que s'augmenterait la longueur des colonnes, la combinaison qui correspond à E ne se multiplie aussi, mais à un moindre degré, dans ces solutions fausses.

Retenant cette remarque, appliquons-la au cas où, sachant que les lettres sont réparties en ordre normal dans le tableau de 25 cases, nous ne connaissons pas le numérotage adopté pour les lignes et les colonnes, c'est à-dire la clef du tableau de substitution. Nous aurons là un moyen de découvrir l'E. Ce sera le groupe correspondant aux plus grandes fréquences obtenues en accouplant chaque colonne successivement avec toutes les autres, sous réserve bien entendu des erreurs qu'on doit admettre dans le calcul des probabilités.

Lorsqu'on aura ainsi accouplé les colonnes et trouvé l'E on retombera, puisque chaque bigramme de chiffres

représente une lettre, sur un compte de fréquences de substitution simple qui permettra de faire des hypothèses sur la valeur des autres lettres. Parmi celles-ci, on sait déjà, si le tableau de 25 cases est établi dans l'ordre normal, quelles sont celles qui sont sur la ligne et sur la colonne de l'E, celles d'entre celles-ci qui sont fréquentes ou qui sont rares, et la détermination de toute nouvelle lettre donne des hypothèses sur sa ligne et sa colonne. Exemple, J correspond à un groupe dont le 1er chiffre est le même que celui de E. Parmi les lettres qui ont le même 2e chiffre que J, seul I est fréquent. Donc la ligne F G H I J correspondra à une rare de la colonne de l'E, et aura 1 lettre fréquente. On remarquera aussi qu'à la ligne K L M N O, seule la lettre K est très rare. Si donc on a une ligne présentant 4 lettres fréquentes et 1 absente, ce sera probablement la 3e, et la colonne de la lettre absente sera la 1re.

Avec quelques lettres du clair, on essaiera de travailler le tableau de transposition pour replacer dans leur ordre les couples de colonnes que l'on a juxtaposées. On aura ainsi résolu le problème suivant : l'ordre des lettres du tableau de 25 cases seul étant connu, sans qu'on en connaisse les coordonnées, retrouver la clef de transposition et les coordonnées du tableau.

Si l'on a trouvé que la clef de transposition a un nombre impair de lettres, il faudrait pour chaque colonne traiter d'abord la série des chiffres de rang pair, avec la colonne de droite, puis avec celle de gauche, et la série des chiffres de rang impair, avec ces deux colonnes successivement. On aurait ainsi quatre séries d'essais à faire au lieu d'un.

Tableau de 25 à somme de fréquences constantes. — Les raisonnements, dont nous n'avons donné ci-dessus qu'une assez brève esquisse (ne désirant sortir que le moins possible des questions générales sans traiter ici des problèmes de cryptographie qui dépassent les éléments de cette science), sont basés sur le fait de l'inégalité des totaux de fréquences des lettres prises par lignes et par colonne, C'est ainsi que nous avons considéré les parti-

cularités de 5 et de 1 pour en tirer des conclusions sur la contexture du tableau de transposition.

On a alors cherché, tout en ne faisant pas du tableau de 25 un élément secret et variable, et en permettant de le garder par écrit au risque d'en laisser prendre copie à un indiscret, à composer un tableau où les totaux des fréquences des lignes et des colonnes diffèrent peu entre eux. Le tableau suivant répond à cette condition :

e	17	k	0	h	0	v	2	y	0	TOTAL 19
g	1	l	5	i	7	r	7	j	0	— 20
q	0	c	4	n	9	b	1	t	7	— 21
x	1	d	4	f	1	s	7	u	7	— 20
z	0	a	7	p	3	m	3	o	7	— 20
TOTAUX. .	19		20		20		20		21	

La difficulté des recherches est considérablement augmentée, en particulier la différence de fréquence des 5 et des 1 signalée dans le système précédent n'apparaît plus. On peut pourtant traiter encore les problèmes posés par l'emploi de ce procédé, en faisant des essais successifs, avec des hypothèses sur la longueur des lignes de tableau, à moins que la comparaison de plusieurs télégrammes ne supprime la nécessité de ces essais en donnant des éléments de précision sur cette longueur. Le travail se base sur cette remarque, que E est la seule lettre fréquente dans sa ligne et dans sa colonne. Lorsqu'on fera les accouplements de colonnes comme plus haut, le bon accouplement, celui qui donne un maximum de E, présentera la fréquence d'un bigramme composé de 2 chiffres qui, l'un et l'autre, seront très rares, en dehors de ce bigramme, l'un comme 1er chiffre, l'autre comme 2e.

On voit donc que, malgré sa complication, un système de substitution simple à représentation unique et de transposition peut être attaqué par un décrypteur avec de bonnes chances de succès. La meilleure parade sera de fournir aux études un minimum de documents chiffrés avec les mêmes éléments, en changeant la disposition des lettres du tableau de 25 et la clef de transposition.

On peut aussi avoir recours aux représentations multiples, les lignes et les colonnes du tableau de 25 portant chacune plusieurs indicatifs. Dans un pareil système, il semble actuellement à peu près impossible de retrouver les clefs, si l'on ne dispose que de cryptogrammes. D'après le général Cartier, qui s'est particulièrement attaché aux études sur les surchiffrements, lorsqu'on possède le texte clair d'un cryptogramme et le nombre de colonnes du tableau de transposition, on peut retrouver la clef de ce dernier tableau et le tableau de substitution, mais cet auteur fait lui-même remarquer qu'avec des chiffreurs habiles, ne tombant pas dans la faute commune d'adopter certaines représentations de préférence aux autres, ce n'est que grâce à la possession d'une grande abondance de textes qu'on pourrait parvenir à un résultat.

Substitution à double clé et transposition. — On a employé des systèmes comportant une substitution à double clef et une transposition. Comme système de substitution à double clef, nous avons surtout rencontré des systèmes genre Gronsfeld, où les alphabets employés étaient peu nombreux et voisins de l'alphabet clair.

Commence-t-on par la transposition ? Le texte qui en résulte est soumis à la substitution avec les alphabets successifs réglés par la clef. Si l'on a de nombreux cryptogrammes, on peut, les lettres de même rang étant traitées par le même élément de clef, rechercher l'alphabet qui y correspond. On écrit les textes l'un sous l'autre, et, dans l'hypothèse d'un procédé Vigenère ou Gronsfeld, on peut trouver l'alphabet qui correspond à la fréquence maxima, sinon d'une seule lettre, douteuse pour E du clair à cause du désordre des transcriptions, du moins d'une série type ERASINTULO (Voir page 87). Si on retrouve la clef et tous les alphabets, on retombe sur le problème de transposition.

Si, comme nous l'avons vu ordinairement, la substitution est faite d'abord, et que la transposition soit pratiquée ensuite, on remarquera que le tableau de transposition se présente de manières différentes suivant

que le nombre de lettres à la ligne est égal à la longueur de la clef de substitution (ou à un multiple de cette clef) ou qu'il en est différent. Dans le premier cas, la périodicité de la clef ramène à chaque ligne le même alphabet dans la même colonne, il n'en est pas de même dans le deuxième. On peut traiter le problème sous la forme générale. Mais nous indiquerons seulement sur un cas particulier fort simple les remarques qui conduisent à la solution.

Nous supposerons que le texte est chiffré à l'aide d'un système de Gronsfeld à clef 012, si bien que le texte clair étant représenté par AAAAAAAAA..., le texte substitué serait ABCABCABC.....

Si la clef de transposition a un nombre de lettres multiple de 3, la 1re colonne du tableau sera composée uniquement des lettres du clair AAAA..., la 2e, de lettres suivant dans l'alphabet la lettre du clair BBBB..., la 3e, de lettres à deux rangs après celles du clair CCCC..., la 4e, de lettres A du clair, etc..., et le cryptogramme sera d'un type tel que BBBBAAAACCCCBBBBCCCC etc...

Si la clef a une lettre de plus qu'un multiple de 3, le tableau sera du type :

A B C A B . . . . A B C A
B C A B C . . . . B C A B
C A B C A . . . . C A B C
A B C . . . . . .

et dans toutes les colonnes on aura des suites du type ABC. Le cryptogramme sera du type :

A B C A A B C A C A B C B C A C A B C

la rupture des séries ABC résultant du changement de colonnes.

Si la clef a deux lettres de plus qu'un multiple de 3, le tableau sera du type :

A B C A B . . . . A B C A B
C A B C A . . . . C A B C A
B C A B C . . . . B C A B C
A B C . . . .

Dans toutes les colonnes on trouvera la série ACB, et le cryptogramme sera du type :

A C B A A C B A B A C C B A

Le classement d'un cryptogramme dans un de ces trois types permettra donc d'avoir une hypothèse sur le nombre de lettres de la clef de transposition, et une grande facilité pour reconstituer la clef puisque les colonnes commençant par une lettre du clair, ou une lettre voisine de celle du clair avec un décalage de un ou de deux, doivent se succéder en ordre. En même temps le problème de la substitution sera résolu.

Mais, lorsque l'on a affaire, non à des lettres ABC, mais à un cryptogramme réel, il y a des difficultés à reconnaître les lettres du clair inchangées de celles qui ont été modifiées. Il faut avoir recours aux considérations de fréquence.

Une lettre donnée du cryptogramme, N, peut représenter soit N, soit M, soit L. Nous supposerons pour chaque lettre du cryptogramme qu'elle représente toujours la plus fréquente des trois lettres dont elle peut tenir la place, et, dans un relevé schématique du cryptogramme, nous désignerons par *a* les lettres qui sont elles-mêmes la plus fréquente du trio (ici N représentant N), par *b* celles qui seraient le résultat d'une transformation de la lettre la plus fréquente avec la clef + 1 (F, par exemple, parce qu'elle suit dans l'alphabet E qui est la plus fréquente des 3 lettres DEF que peut représenter F), par *c* celles qui résulteraient de la clef + 2 (G, par exemple, qui représentera plutôt E dont la fréquence est 17 que F dont la fréquence est 2). On peut dresser une table comprenant la liste des lettres et le type dans lequel elles rentrent, suivant qu'en considérant la lettre en question, et les deux qui la précèdent, la plus fréquente est la lettre elle-même, la précédente ou l'antéprécédente.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
a b c a a b c a a b c a b a b c c a a b c c c c b c

Or, en étudiant un certain nombre de cryptogrammes établis sur ces types en vue d'en rechercher les particularités, on reconnaît comme l'a signalé le capitaine Painvin, que dans la plupart des cas, suivant que le cryptogramme comprend une majorité de séquences type aa, type ab ou type ac, il appartient au 1er, au 2e ou au 3e type.

Soit alors le cryptogramme de 48 lettres :

VKTKU BFTEB VGQTG VUIPM CLMNA NOJJF ESSFG GPNRS TNUBW BPZ

En remplaçant chaque lettre par l'indice du type auquel elle se rattache, on a :

ccbcc bbbab cccbb ccacb cabaa abbbb aaabc ccaaa bacbc cbc.

Les séquences du type aa, bb, cc sont au nombre de 20;
Celles du type ab, bc, ca, au nombre de 14;
Celles du type ac, cb, ba, au nombre de 13;

On en conclura que le nombre de lettres de la clef de transposition est multiple de 3.

Dans la plupart des cas, un seul cryptogramme ne pourra pas donner un renseignement plus complet. Mais, si l'on en a plusieurs, on peut arriver, en comparant les débuts et les fins, à estimer la longueur des colonnes, en voyant plus ou moins nettement le point où la série ccc fait place à la série bbb ou aaa qui appartiendra à la 2e colonne relevée dans notre cryptogramme (ou, si les premières colonnes sont de même ordre, à une colonne suivante). Il est probable ici que le b 3e lettre est un accident et que la 1re colonne prend fin avec le 1er groupe, mais, du côté du 4e et du 5e groupe, les séparations de colonnes ne sont plus du tout nettes.

La clef, avons-nous dit, est multiple de 3, une clef de 9 conduirait à des colonnes de 5 et 6 lettres, une clef de 15 à des colonnes de 3 et 4 lettres, qui pourraient aussi convenir. Nous supposerons que nous avons d'autres documents et que des débuts plus nombreux nous ont con-

firmé une clef de 9 lettres, et nous donneraient la succession de colonnes suivantes :

cbcaabcab (une colonne du type c relevée la 1re, une du type b relevée la 2e). On verrait de même, par la considération des longueurs des colonnes possibles avec les différentes longueurs de cryptogrammes et la clef de 9, quelles sont les colonnes qui doivent être les colonnes longues, et on arriverait à placer le cryptogramme en tranches comme ci-dessous :

Type	c : VKTKU,	b : BFTEBV,	c : GQTGV
	a : UIPMC,	a : LMNANO	b : JJFES
	c : SFGGPN,	a : RSTNU	b : BWPBZ

On a, immédiatement les trois premières colonnes (les colonnes longues) dans l'ordre a b c :

L	B	S	ou, en traduisant,	l	a	q
M	F	F		m	e	d
N	T	G		n	s	e
A	E	G		a	d	e
N	B	P		n	a	n
O	V	N		o	u	l

les deux autres colonnes type a, essayées comme 4e colonne, donnent les bigrammes :

q	r
d	s
e	t
e	n
n	u

q	u
d	i
e	p
e	m
n	c

le bigramme *qu* fait adopter la 2e solution. En continuant de proche en proche, on retrouve le texte : « La 4e division se portera demain de Nancy sur Toul. »

Le cryptogramme :

BSTBD URQEC RFBIT EOTFP KSAUL FPNVU GTMUS RMGBU VFVJA PFHSW TGWOU KFNNJ JNGZA W

donne comme schéma :

babba cacac abbab abbbc caaca bcacc cbbca abcbc cbcba cbaac bccbc cbaab bacca c

Séquences type aa : 16, type ab : 23, type ac : 25.

Il est en effet chiffré avec une clef de 11 lettres. Le texte clair est : « La 4e division se portera demain de Nancy sur Toul. Départ à 3 heures. »

Dans cet exemple de surchiffrement, nous voyons comment la superposition du système de substitution à la transposition facilite la reconstruction du tableau de transposition. Il est donc permis de se demander si la complication du chiffrement est légitimée par l'avantage obtenu au point de vue de la solidité du système. Si on se contente de changer les clefs de transposition sans modifier celle de la substitution, et que la correspondance soit assez active pour que le décrypteur puisse établir à l'aide des schémas la longueur des colonnes et leur situation en longues et courtes sur plusieurs documents avec une bonne approximation, la résolution du problème de la clef de transposition devient presque mécanique.

Nous avons montré sur ces quelques exemples comment, lorsqu'on a identifié un système compliqué, ou qu'on en a connaissance par un moyen quelconque, on doit le disséquer pour voir par quel moyen on peut le traiter, et le ramener à des cas simples qu'on sait résoudre par les méthodes générales et qui forment les étapes successives de la solution du problème. Quant à la grosse difficulté, d'identifier les méthodes qui ont fourni des cryptogrammes reçus par le décrypteur sans explications complémentaires, on la résout, quand on peut la résoudre, par une connaissance (due à l'expérience) des résultats donnés par la transformation d'un texte clair en chiffres au moyen des méthodes qu'on a eu l'occasion de travailler antérieurement, et par des essais sur des textes que l'on chiffre par différents procédés, pour reproduire les particularités

du cryptogramme. On ne devra pas s'étonner si, ayant à combattre des chiffreurs exercés, maîtres de méthodes compliquées, et changeant fréquemment les clefs, et même les procédés, on n'arrive pas à rompre le sceau de secret qu'ils ont voulu imprimer sur leur correspondance.

CHAPITRE XIV

SYSTÈMES A DICTIONNAIRES

Description des systèmes et surchiffrements.

Généralités. — Les systèmes à dictionnaires sont des systèmes de substitution, où les éléments des tableaux de correspondance, comprenant des lettres, des syllabes, des mots, des phrases, sont si nombreux qu'il n'est pas possible de les retenir par cœur ni de les rétablir au moment du besoin, et qu'il faut en faire l'objet de listes écrites. L'ensemble de ces listes forme ce qu'on appelle un code, ou un répertoire, ou un dictionnaire chiffré, ou des tables de chiffrement. On pourrait peut-être établir entre ces mots une différence de sens suivant l'aspect extérieur et la taille du document. Nous emploierons ici indifféremment l'une ou l'autre de ces appellations.

On trouve des dictionnaires chiffrés tout imprimés dans le commerce. Quand on veut conserver le secret des tableaux de correspondance, on doit avoir recours à des dictionnaires composés spécialement et conservés secrets : les grandes administrations, les services d'État ont ainsi leurs dictionnaires.

Dans tous les documents de cette nature, un certain nombre de mots figurent tels qu'ils existent dans la langue; quelquefois, à la même ligne, un radical est suivi de plusieurs terminaisons qui correspondent par exemple à un verbe et un substantif, à un adjectif et un adverbe (commenc-er, -ement; facile, -ment).

Le sens, ou une convention spéciale, indique si, au déchiffrement, on doit traduire par le premier ou le deuxième des mots qui figurent ainsi accolés.

Certaines phrases ou des mots composés, ou des combinaisons de mots fréquents figurent aussi dans le dictionnaire.

Mais il est des mots ou des noms propres qui n'y figurent pas. On les décompose alors en éléments alphabétiques ou syllabiques qu'on chiffre successivement. Beaucoup de dictionnaires renferment pour faciliter cette opération des groupes de convention dont l'emploi est expliqué dans l'avant-propos. On désigne fréquemment les mots chiffrés par éléments par l'expression : les syllabés.

Plus il y a de mots ou d'expressions, moins on a besoin de recourir au syllabage, plus, dit-on, le dictionnaire est riche.

Lorsque dans le tableau de correspondance, les deux listes : mots et leurs représentations, sont ordonnées toutes deux alphabétiquement ou numériquement, on dit que le dictionnaire est ordonné. Pour chiffrer, on cherche dans le tableau un mot à sa place alphabétique, et on écrit dans le cryptogramme la représentation de ce mot figurant en face de lui; pour déchiffrer, on cherche, *dans le même tableau*, à sa place alphabétique ou numérique, cette représentation, et on trouve en face d'elle le mot du texte clair.

Mais nous avons vu dans les substitutions que l'emploi d'un alphabet de substitution incohérent complique beaucoup la tâche des décrypteurs. On obtient le même résultat en adoptant l'incohérence dans l'ordre des représentations pour le dictionnaire. Dans ce cas, au lieu de pouvoir se servir du même tableau pour les recherches des mots à chiffrer ou des représentations à déchiffrer, on adopte des tableaux différents : l'un où les mots à chiffrer sont en ordre alphabétique, et les représentations sans ordre, l'autre où les représentations sont en ordre alphabétique ou numérique, et les mots du clair sans ordre. On évite ainsi les longues recherches, qui seraient nécessaires si l'on n'avait qu'un seul tableau, pour retrouver au déchiffrement par exemple une représentation noyée dans une longue liste désordonnée.

Les deux tableaux sont appelés tableau chiffrant (ou table chiffrante) et tableau déchiffrant (ou table déchiffrante). Le dictionnaire est souvent dit à bâtons rompus ou incohérent.

Exemple d'une page d'un dictionnaire ordonné :

2000 Corse	2050 couronner
2001 Cortège	2051 courrier
2002 Cortès	2052 par le courrier
2003 Corvée	2053 cours
2004 Corvette	2054 au cours
2005 Coryza	2055 cours moyen
2006 Costume	2056 dernier cours
2007 Cote	2057 course
2008 Côte	2058 court
2009 Côté	2059 courtage
2010 à côté de	2060 courtier
2011 de tous côtés	2061 cousin
2012 du côté de	2062 couteau
2013 coter	2063 coûter
. . . . .	. . . . .

Exemple de pages d'un dictionnaire à bâtons rompus :

Table chiffrante		*Table déchiffrante*
piège	4367	1020 madame
pierre	1025	1021 convoi
pierrerie	9872	1022 accord
piété	0013	1023 marne
pile	1421	1024 heure
pillard	5718	1025 pierre
piller	6884	1026 porteur
pilote	4321	1027 repos
. . . . .		. . . . .

On trouve enfin dans certains cas des dictionnaires mixtes. Tous les mots sont par ordre alphabétique, et la grande majorité des groupes sont en ordre, de sorte qu'une seule table pourrait servir. Mais, pour des raisons qui seront

exposées plus loin et qui résultent des méthodes de décryptement des codes ordonnés, il est bon que certains mots ne soient pas représentés par un groupe correspondant à leur place alphabétique; ainsi en français, il est mauvais que A soit représenté par 0001.

On fait alors figurer en face de A, à sa place alphabétique, un groupe quelconque, et on reproduit ce groupe à sa place numérique en écrivant en face le mot A, dont cette représentation n'est plus alors à sa place alphabétique. Ceci exige 2 lignes du dictionnaire pour les mots ainsi traités et rompt l'ordre des tables, mais on peut faciliter la lecture par des artifices typographiques. Un tel procédé permet de ne pas imposer aux rédacteurs du dictionnaire la tâche très pénible de collationnement qu'exigent les dictionnaires à bâtons rompus, et d'économiser sur le papier et l'impression, puisque quelques mots seulement figurent deux fois, au chiffrement et au déchiffrement, alors que dans le dictionnaire à bâtons rompus tous les mots figurent une fois à la table chiffrante et une autre fois à la table déchiffrante :

Exemple :

A	1404	dilapider	1401
ab	0002	dilater	1402
abaisser	0003	dilatoire	1403
abandon	0004	— A —	1404
abattre	0005	dilemme	1405

Mots et groupes codiques. — Nous avons parlé des représentations des mots du clair. Ces représentations sont, en général, soit des groupes de chiffres, soit des groupes de lettres, soit des mots.

Jusqu'à ces dernières années, il semble que les groupes de chiffres aient eu la préférence. Une disposition fort commune était le dictionnaire ordonné de 100 pages de 100 lignes en deux colonnes : soit 10.000 mots, avec des groupes de 4 chiffres, qu'on passait au télégraphe soit par tranches de 4 chiffres, soit par tranches de 5 en acco-

lant toutes les tranches de 4 et coupant le résultat par groupes de 5. Les essais de dictionnaires en lettres n'avaient pas eu grand succès, peut-être parce que dans les transmissions télégraphiques Morse deux lettres risquent, si elles sont mal lues, de donner à la lecture d'autres lettres ou même une seule, ce qui multipliait les fautes, tandis que les chiffres, toujours composés de 5 signaux se suivant dans un ordre spécial, pouvaient bien donner lieu à une erreur (d'ailleurs fréquemment d'une seule unité), mais étaient tous représentés sans que deux d'entre eux viennent se confondre en un seul.

Les dictionnaires qui n'employaient pas les groupes de chiffres employaient souvent les mots complets, empruntés à des langues parlées, et figurant au répertoire de la convention de Berne qui contient tous les mots provenant des langues admises dans les correspondances internationales et taxés au tarif d'un mot : les fautes de transmission sur ces mots étaient en général assez visibles.

Depuis quelques années, le relèvement des taxes télégraphiques a donné une grande importance à tout ce qui peut raccourcir les télégrammes. Or, si un groupe de 5 chiffres ou un mot de la liste de Genève est taxé pour un mot, on admet également pour un mot un ensemble de 10 lettres formant un mot quelconque, même absent de la liste de Genève, pourvu que ce mot soit prononçable. On s'est donc efforcé d'adopter comme représentation des groupes de 5 lettres seulement (soit 1/2 mot du tarif, puisqu'on les accouple par deux pour former un mot de 10 lettres) en choisissant les voyelles et les consonnes de manière à former une séquence prononçable.

On appelle souvent mots codiques, ou groupes codiques les représentations des mots du clair; les groupes codiques de 5 lettres prononçables sont donc actuellement à la mode.

Dans ce même but d'économie, les dictionnaires les plus récents vendus dans le commerce contiennent un très grand nombre de phrases de plusieurs mots, se rapportant à des opérations commerciales. Quelques-uns sont même spéciaux à certains genres de questions (commerce

des vins, mines, etc...). Dans ces dictionnaires, le but visé n'est pas principalement la cryptographie pour cacher le sens du document aux tiers, mais c'est plutôt l'économie de n'avoir à transmettre qu'un mot codique au lieu d'une phrase en clair. Toutefois, de tels documents pourront souvent être proposés au cryptologue qui se heurtera à des difficultés provenant d'abord de l'incertitude sur le dictionnaire employé (même si aucune modification n'a été faite à la signification des groupes codiques), puis des procédés cryptographiques qu'aura peut-être employés pour modifier ces groupes un correspondant désireux de cacher ses communications aux indiscrets, concurrents ou employés, qui pourraient connaître son dictionnaire. La reconnaissance des dictionnaires employés exige une longue pratique, servie par une bibliothèque spéciale fort bien montée, où figurent les dictionnaires de toutes les nations qu'on peut se procurer dans le commerce, et aidée par des répertoires de caractéristiques de dictionnaires portant sur des points que nous signalerons plus loin. Quant au travail fait sur les groupes codiques, il peut rentrer dans les études cryptographiques qui font l'objet principal du présent opuscule, et nous en dirons un mot.

Pour pouvoir adopter un ordre dans l'étude des dictionnaires, nous commencerons par distinguer (distinction purement superficielle) ceux qui ne comprennent comme groupes codiques que des groupes de chiffres. Nous passerons ensuite à ceux qui comportent des groupes codiques en lettres.

Nous nous heurterons d'ailleurs aux mêmes difficultés que les auteurs antérieurs pour exposer des théories d'ensemble au sujet de la résolution des problèmes posés par les dictionnaires, et nous aurons recours seulement à des explications et des exemples portant sur des cas particuliers sans pouvoir en déduire de méthodes générales. Nous renverrons le lecteur, désireux de se documenter plus amplement, au deuxième volume de l'ouvrage de Valério, où cet auteur donne plusieurs exemples de déchiffrement.

Code chiffré Sittler. — Le dictionnaire chiffré à groupes

codiques en chiffres le plus employé en France dans la période de 1900 à 1920 est certainement le code télégraphique chiffré de Sittler. C'est un volume de 100 pages, chacune d'elles comprenant deux colonnes de 50 lignes et les 100 lignes ainsi obtenues dans chaque page étant numérotées de 00 à 99. Les mots y sont rangés par ordre alphabétique, les expressions importantes figurant après le mot qui semble représenter l'idée énoncée (accorder, d'accord avec, être d'accord, etc..., agir, agir de manière que, agissez, dont il s'agit, etc...). Les lettres, les rares syllabes représentées dans le code sont à leur place alphabétique. Un certain nombre de lignes en blanc, à la fin de chaque liste des mots commençant par une lettre donnée de l'alphabet, permet aux correspondants quelques additions commodes pour leurs affaires.

Les pages ne sont pas numérotées.

La manière classique d'employer ce dictionnaire est d'adopter une pagination conventionnelle. Le procédé le plus simple est d'appeler 00 une page quelconque et de continuer la numération en partant de cette page. On obtient ainsi le même résultat qu'en ajoutant un nombre constant à la pagination obtenue en numérotant les pages du dictionnaire du commencement à la fin de 00 à 99; c'est une substitution numérique ordonnée, du genre des substitutions simples à alphabets normalement ordonnés.

Comment, étant donné un cryptogramme, retrouver la pagination employée par les correspondants?

De même que, pour étudier les systèmes alphabétiques, la première opération est de relever la fréquence des lettres pour tâcher d'avoir une base d'hypothèses sur le système, de même dans les télégrammes codiques, mais non pour le même emploi, il est avantageux de relever les différents groupes pour en vérifier la fréquence et parfois les séquences. Pour les études de longue haleine, ces relevés se font sur des registres où chaque ligne est numérotée et correspond à un groupe, et, après avoir réuni en liasse les documents à étudier et avoir paginé cette liasse, on inscrit sur le registre la référence des pages où figure chaque groupe, de manière à pouvoir rapidement retrou-

ver chaque répétition de ce groupe, quand on fera des hypothèses sur le sens qu'il a. Pour les premières recherches, on peut se contenter d'écrire par colonnes les groupes du télégramme commençant par un même chiffre, de manière à en faire un premier tri et à pouvoir compter facilement les fréquences.

Ces relevés révéleront donc les groupes fréquents. Parmi ces groupes se trouvent généralement les prépositions et les ponctuations. On distingue quelquefois les mots d'une langue, eu égard à leur rôle, en mots *pleins*, qui donnent le sens au discours, et mots *vides :* conjonctions, articles, prépositions, auxiliaires, pronoms, etc..., qui entrent dans les phrases, quel que soit le sujet traité. Valério donne même un relevé des fréquences des mots vides. Nous retiendrons seulement que ce sont ces mots vides qui sont les plus fréquents.

Or, dans la méthode d'emploi du Sittler que nous avons indiquée, les deux chiffres indiquant la ligne des mots ne sont pas modifiés. Sans doute, on peut écrire les deux chiffres de la page avant, ou après, les deux chiffres de la ligne. Mais quand on a pris note de la ligne d'un certain nombre de mots vides, on retrouve bientôt les deux chiffres de cette ligne dans les groupes les plus fréquents (et : 33; par : 68; pour : 63, etc...) et en identifiant le mot avec un groupe, on obtient le numéro d'une page. Dans le cas exposé d'une pagination continue, cela suffit pour permettre de lire tout le texte. L'hypothèse doit naturellement être vérifiée sur d'autres groupes.

Il est à remarquer que nous n'avons que rarement trouvé les articles ou la préposition « de » parmi les mots les plus fréquents. Sous prétexte de « style télégraphique », les correspondants les suppriment ordinairement.

Bien que le paragraphe qui va suivre ne soit pas ici à sa vraie place, et aurait dû être reporté au chapitre des surchiffrements, nous signalerons tout de suite un des procédés, souvent employés, pour augmenter le secret du Sittler, c'est la transposition portant sur les 4 chiffres d'un groupe. Si nous représentons les 2 chiffres du numéro

de la page par PA, les deux chiffres du numéro de la ligne par LI, on trouve en plus des combinaisons PALI ou LIPA toutes les combinaisons de ces 4 chiffres, telles que PLIA, PILA, etc... On aura souvent à essayer des hypothèses sur plusieurs combinaisons de cette nature avant de rencontrer la bonne, en accouplant successivement les chiffres des groupes deux à deux pour chercher à identifier un numéro hypothétique de ligne avec un mot comme il est dit plus haut, quand, ce qui arrive fréquemment, on n'a pas assez de documents pour avoir des fréquences très évidentes.

Dans le cas où la numération des pages est normale et continue, la connaissance d'un seul groupe entraîne la solution du problème. Mais, souvent, cette numération n'est pas normale et continue. On trouve parfois dans la numération un certain ordre : par exemple, pagination de 99 à 00 en ordre inverse de l'ordre naturel, emploi de tous les nombres pairs, puis de tous les nombres impairs, emploi des 10 nombres terminés par 0, puis des 10 nombres terminés par 1, etc...

Mais souvent aussi le désordre est poussé plus loin (respect de l'ordre dans chaque dizaine, mais mélange des dizaines par exemple) au point qu'il faut un tableau de concordance aux correspondants eux-mêmes pour remplacer la pagination naturelle du dictionnaire par la pagination adoptée, et on va ainsi jusqu'à l'incohérence absolue.

On commence alors les recherches par des mots probables, et l'on s'efforce de déterminer la page d'un certain nombre de mots et de trouver une loi entre les numéros de ces pages et la pagination naturelle du volume. On facilite beaucoup les recherches en préparant d'avance un registre où on réunit à une même page les 100 mots qui correspondent à une même ligne dans le dictionnaire, ce qu'on appelle un Sittler par lignes.

Certaines hypothèses en effet, sur le sens des groupes, peuvent se baser sur leur place dans le cryptogramme. Beaucoup de correspondants terminent par « point » (ligne 31) et beaucoup aussi par « amitiés » (96). Lettre

(98) suit (52), est aussi une fin fréquente, tandis que « j'ai reçu » (49), réponse (76) sont plutôt des débuts. Parmi les bonnes sources d'exploitation, il faut citer encore toute la série des mots qui expriment l'idée de télégraphier, et les mots qui expriment des valeurs et des poids (francs, tonnes) et des nombres.

A propos de ces derniers, nous ferons une remarque sur la contexture du Sittler en particulier et des codes en général. Nous avons dit que, dans le Sittler, les expressions dérivées d'un mot sont à la suite de ce mot, c'est ainsi qu'après CENT nous aurons DEUX CENTS, TROIS CENTS, etc... La présence de ces nombres parmi les mots représentés devrait diminuer la fréquence de CENT dans les textes. Dans la pratique, il n'en est à peu près rien. Ayant à chiffrer DEUX CENTS, le chiffreur qui n'est pas spécialiste va, d'abord, chiffrer le mot DEUX, et quand, ensuite, à côté de CENT, il trouve DEUX CENTS, il ne raie pas le groupe déjà écrit, il chiffre à côté CENT. Ainsi, dans les dictionnaires, la vraie place de toutes les expressions devrait être la place alphabétique de leur premier mot. D'ailleurs, quand on en met un trop grand nombre, les chiffreurs ne se donnent pas la peine de lire la liste. Dans la pratique, et quand il ne s'agit pas des codes faits pour diminuer le prix du télégramme par l'existence de phrases toutes faites correspondant à un seul mot codique, il est à notre avis inutile d'insérer dans les dictionnaires trop de phrases ou de formules.

Nous avons indiqué comme procédé de déchiffrement du Sittler la permanence du numéro de la ligne, et la connaissance de ce numéro pour les mots fréquents. La parade au décryptement sera donc la modification du numéro de la ligne, soit seulement pour les mots fréquents, qu'on permute avec d'autres mots de la page, soit par une substitution générale portant sur le numéro de la ligne comme celui qui porte sur le numéro de la page. Quand cette substitution est simple, telle que celle qui résulte de l'addition d'un même nombre à tous les numéros de lignes, la comparaison entre les groupes fréquents du cryptogramme, parmi lesquels, par la soustrac-

tion d'un même nombre, on peut faire réapparaître les numéros de ligne de mots fréquents (par et pour différent de 5 lignes; la, le, les, à la même page, différent de 53 et 30 lignes), suffit quelquefois pour donner des bases d'hypothèses sur le sens de certains groupes. On peut faire une sorte de graphique des fréquences du Sittler normalement ordonné et de celles du cryptogramme qui parfois donne des résultats. Mais si l'on soumet les lignes à une substitution à tableau incohérent employée en même temps pour les pages ou réciproque de cette dernière, ou bien encore différente, le décrypteur se trouve en face de très sérieuses difficultés et ne doit guère compter que sur l'accumulation des éléments de travail pour faire des remarques qui lui seront utiles.

Nous avons dit que le Sittler se présente en groupes de 4 chiffres. Dans la pratique, on passe fréquemment des télégrammes en Sittler par groupes de 5, en coupant la succession des groupes par tranches de 5. Certains correspondants, lorsque le dernier groupe ne comporte pas 5 chiffres, le laissent tel quel ou le complètent par des zéros, ce qui attire l'attention. Mais certains ont la précaution de terminer par des chiffres nuls autres que des zéros, ce qui peut faire régner l'incertitude sur l'emploi d'un dictionnaire à 4 ou 5 chiffres. Cette incertitude, lorsque le texte n'est pas trop court, est levée par la considération des répétitions. En coupant le texte en tranches de 4 chiffres, on voit apparaître des répétitions de groupes tandis que l'on n'en voit pas, ou pas autant, dans les groupes de 5 chiffres. Cette recherche du nombre de chiffres des groupes est à faire toujours avant d'entreprendre les relevés de télégrammes.

Pour tromper sur l'identité du dictionnaire, des correspondants emploient alors le Sittler avec 5 chiffres. On y arrive très simplement par divers procédés :

— D'abord l'emploi de nulles : l'intercalation d'un chiffre nul à une place convenue dans le groupe de 4 chiffres. Ce procédé se révèle ordinairement assez vite dans l'examen des groupes fréquents, à moins d'être employé avec une maestrïa bien rare. Il diminue en effet la fréquence, puisque

le cinquième chiffre diffère d'une répétition à l'autre, mais l'identité de 4 chiffres finit par attirer l'attention d'un décrypteur, averti de l'existence de tels procédés.

— Puis par l'emploi d'une numération des pages en groupes de 3 chiffres. Si l'on n'emploie qu'un numéro par page, l'emploi de cent numéros au maximum figurant seuls dans les relevés finit par apparaître, encore que si les chiffres de la ligne et de la page sont bien mélangés dans le groupe, le décrypteur puisse chercher longtemps avant que le classement des groupes lui fasse reconnaître le procédé. Si l'on emploie plusieurs numéros par page, à prendre indistinctement, la difficulté s'accroît encore.

— Ou bien encore par l'emploi de procédés permettant, par l'emploi de 3 chiffres et d'une opération arithmétique, de reconstituer un nombre de 2 chiffres. Exemple : remplacer le premier chiffre du numéro de la ligne par un groupe de 2 chiffres tels que le chiffre des unités de leur somme reproduise ce premier chiffre de la ligne (7 sera remplacé par 07, ou 16, ou 25, etc..., ou 89). Ajouter au numéro de la ligne un chiffre quelconque qu'on écrit ensuite (16 est remplacé par 259 = 25 — 9 reproduit 16., ou 171, 17 — 1 = 16).

On voit donc que les procédés ne manquent pas pour dérouter les décrypteurs. Ceux-ci, avons-nous dit, ne peuvent avoir recours qu'à l'abondance des documents, qui, à force de répétitions, peuvent donner des bases à certaines hypothèses.

On supprimera même cette branche de salut en modifiant la convention, ou la clef, d'un télégramme à l'autre.

On peut indiquer des procédés à changer chaque jour, ou même à chaque télégramme, soit dans un ordre donné, soit en les faisant connaître au correspondant par un mot ou un groupe de convention. Parmi ces procédés, nous avons vu employer le suivant; les correspondants conviennent d'un mot du dictionnaire pris comme mot clef et le chiffrent en tête avec le procédé employé pour le télégramme, par exemple en ajoutant à chaque groupe du télégramme un nombre donné, ou en adoptant un ordre donné pour les 4 chiffres du groupe.

Nous n'en dirons pas plus sur ce sujet. Mais on voit qu'un dictionnaire du commerce, fort simple, convenablement « truqué » par un décrypteur exercé, et employé par des idoines, peut constituer un excellent instrument de correspondance secrète. A vrai dire, nous n'avons pas souvent vu employer ainsi les Sittler ni les codes analogues. On se contente presque toujours de modifier la pagination, ou d'ajouter un même nombre, dit « clef additive » aux groupes. Remarquons que dans ce dernier cas, certains correspondants prennent le soin de ne pas écrire le 1 des dizaines de mille si l'addition le fait apparaître, tandis que d'autres ne prennent pas cette précaution ce qui attire l'attention. Dans l'emploi de ces clefs additives, il arrive fréquemment qu'au lieu d'additionner le nombre formé par PALI avec la clef, en tenant compte de toutes les retenues, on n'additionne que chaque chiffre d'un des nombres avec le chiffre correspondant de l'autre sans faire aucune retenue. 4597 plus 2068 donne 6555 et non 6665. C'est une convention à fixer entre les correspondants.

Autres codes à groupes de 4 chiffres. — Nous ne prétendons pas faire ici une liste de tous les codes, pas même de ceux que nous connaissons et qui sont loin de former la plus grande partie de ceux qui ont été mis dans le commerce. Nous en citerons seulement un certain nombre comme types.

A côté du Sittler on peut ranger les chiffres de Bazeries, deux documents à peu près analogues dits table n° 1 et table n° 2. Bazeries prévoit trois numérations différentes pour les pages : ordinaire, réservée, spéciale. Certains correspondants indiquent par un de ces mots, en clair, la pagination employée et fournissent ainsi une hypothèse sur le code. Un des points faibles des tables Bazeries est la ponctuation, groupée dans une même dizaine de la même page, la première pour la table 2, la dernière pour la table 1. Les syllabes sont groupées en tête de chaque lettre; ce qui, lorsqu'on recherche des noms propres comme mots probables, comme nous le verrons plus loin, et qu'un nom a deux syllabes commençant par une même lettre,

peut donner un point de repère. Mais la multiplicité des formules composées d'une préposition ou d'une conjonction et d'un article, la répartition des nombres qui figurent à la place alphabétique du premier nombre énoncé (deux cents est à « deux »), font, à notre avis, des chiffres Bazeries des documents d'un emploi plus sûr que le Sittler, surtout lorsqu'on se contente des procédés simples de numérotage des pages sans aller chercher les méthodes cryptographiques déjà compliquées dont nous avons parlé plus haut et qui donnent au Sittler lui-même une sécurité de premier ordre.

Le Code *Nilac* est encore à 100 pages, mais le seul chiffre qui figure dans le texte imprimé est un numéro de 0 à 9, en face de chacun des 10 mots ou expressions qui constituent les 10 séries, séparées par les dispositions de l'impression, figurant à chaque page. Les correspondants doivent donc convenir non seulement des deux chiffres de la page, mais du chiffre de la dizaine, et le décrypteur n'a pour le renseigner qu'un seul chiffre imprimé, quand encore un procédé cryptographique ne vient pas le masquer. Les expressions viennent après le mot important pour le sens, et non à la place alphabétique de leur premier mot. Les nombres composés figurent avec leur premier élément (deux cents à « deux »).

Nous trouvons dans le Nilac une disposition nouvelle. A côté de la série des mots et expressions ordinaires figure une deuxième série composée de syllables et de noms géographiques. A une même ligne, à un même groupe de quatre chiffres, correspondent donc deux traductions différentes. Le sens suffit ordinairement à distinguer celle qu'il faut adopter en déchiffrant, mais en cas de doute, le chiffreur annonce qu'il faut prendre la deuxième traduction, au moyen de groupes spéciaux traduisant : noms propres (emploi de la colonne des...) Commencement — id. fin... et syllabes (emploi de la colonne des...) Commencement — id. fin.

Remarquons en passant que les chiffreurs novices ont une tendance à faire emploi de ces groupes spéciaux même

quand le sens ne l'exige pas, et que la réapparition de groupes accouplés (commencement-fin), quand le cryptogramme contient beaucoup de noms propres ou syllabes, appelle l'attention du décrypteur et peut fournir une base à une hypothèse sur la signification de groupes et par suite donner ce qu'on appelle « une entrée » dans le code.

Emploi du cinquième chiffre. — Cette colonne de noms propres et de syllabes se trouve dans certains codes privés, mais on a parfois recours pour en indiquer l'emploi à d'autres procédés que celui d'un groupe spécial. Certains dictionnaires à quatre chiffres comportent l'emploi d'un cinquième chiffre, placé avant ou après le groupe de 4 pour indiquer soit l'emploi d'une colonne spéciale, soit l'emploi du deuxième ou du troisième mot de la ligne (chasse, chasser, chasseur), soit des flexions grammaticales (pluriel, féminin, participe passé, indicatif présent, etc). Les cryptogrammes présentent alors des groupes de 4 et des groupes de 5 chiffres, parfois même des groupes de 6, 7 et 8 avec des chiffreurs qui abusent des indications grammaticales (féminin pluriel; 2° mot de la ligne participe passé féminin pluriel). Le relevé des groupes, permettant de reconnaître des groupes de 4 chiffres et ces mêmes groupes avec leurs chiffres adventices, révèle le procédé. Ce dernier est connu sous le nom d'emploi du cinquième chiffre. Remarquons que certains codes entraînent régulièrement l'emploi de groupes de 4 et de groupes de 5 chiffres, et que par suite, à première vue, l'emploi du cinquième chiffre peut aiguiller les recherches sur d'autres codes que ceux du type à 4 chiffres.

Le *Telescand Code*, code français de 100 pages en ce qui concerne les mots courants, avec un supplément pour les noms propres, emploie ainsi un cinquième chiffre, qui est toujours O, pour indiquer l'emploi d'une colonne d'expressions doublant la colonne des mots. Celle-ci multiplie par deux, étant donnée sa richesse, le contenu du Code. Ce code n'a été édité qu'en 1914 : il ne nous paraît pas encore, en 1923, fort répandu.

Dictionnaires étrangers à groupes de chiffre. — Parmi les dictionnaires étrangers vendus dans le commerce, un certain nombre (*Chiffrier Wörterbuch*, de Friedmann à Berlin, par exemple) sont du type Sittler. Mais on rencontre des variétés de ce type que nous allons signaler.

Le *Chiffrierbuch* de Stern et Steiner (Vienne, 1892) et le *Dizionario per corrispondenze in cifra* de Baravelli (Turin, 1896) présentent une partie principale ou « dictionnaire » de 100 pages, analogues à celles du Sittler, avec 100 lignes à la page, où figurent des mots ou expressions. Mais, au début du volume, se trouvent 3 tableaux. Le 1er, appelé tableau des voyelles et ponctuations, ne comprend qu'une page avec 10 lignes numérotées de 0 à 9. Le 2e, d'une page avec 100 lignes comprend les lettres isolées, les pronoms, les terminaisons de la conjugaison, les verbes auxiliaires. Le 3e, de 10 pages avec 100 lignes numérotées à la page, comprend les syllabes. D'après les exemples donnés par les auteurs, les expressions du 1er tableau figurent dans le cryptogramme en groupes d'un chiffre, celles du 2e en groupes de 2 chiffres, celles du 3e en groupes de 3 chiffres, celles du « dictionnaire » en groupes de 4. On est maître de règler par convention le numérotage de 0 à 9 des pages du tableau III, et le numérotage de 00 à 99 du « dictionnaire ». Dans la pratique, les correspondants se figurent parfois qu'ils augmentent la sécurité des communications en modifiant le chiffre imprimé des dizaines du tableau II et les chiffres uniques du tableau I.

Les cryptogrammes faits avec ces codes, présentent donc, en général, une majorité de groupes de 4 chiffres, mais aussi des groupes de 1, 2 et 3 chiffres. Il ne peut être question de les passer en tranches de 5 chiffres, comme cela serait possible si tous les groupes étaient égaux. Les mots chiffrés par syllables se présentent sous forme de séquences de groupes de 1, 2 et 3 chiffres, tout à fait caractéristiques des dictionnaires de ce genre.

Pour éviter cet aspect caractéristique, et pour faciliter des opérations de surchiffrement dont nous parlerons plus loin, certains correspondants unifient tous les groupes à 5 chiffres en adoptant une pagination à 3 chiffres, qui

englobe les 4 parties, avec la précaution de représenter par des nombres de 2 chiffres les lignes de la table I. La réunion des syllabes dans les mêmes pages permet parfois, quand l'attention se fixe sur les suites de groupes provenant de pages très voisines, de déceler néanmoins la nature du dictionnaire employé.

Dictionnaires de plus de dix mille mots. — Il semble que, dans tous ces dictionnaires, les auteurs se soient efforcés de ne pas dépasser 10.000 mots ou expressions, et se soient astreints pour augmenter la richesse du code à des procédés secondaires plus ou moins ingénieux (plusieurs mots à la ligne, 2 colonnes, etc...). Les auteurs de toute une série de codes, parmi lesquels le *Nuovo Cifrario* Mengarini (Rome, 1898), le *Cifrario per la corrispendenza segreta* de Cicero (Rome, 1889), le *Diccionario Cryptographico* édité à Lisbonne en 1892, le *Diccionario para a correspondencia secreta* de Vaz Subtil (Lisbonne, 1871), etc..., se sont contentés d'écrire sur des pages de 100 lignes les mots qu'ils jugeaient utiles, sans s'inquiéter *a priori* du nombre de pages, qui atteint près de 300 dans certains de ces opuscules. Suivant les instructions en tête des volumes, il appartient aux correspondants d'établir la pagination de convention pour l'inscription de laquelle une place est réservée dans certains ouvrages, ou d'adapter sur la pagination existante, ou sur les numéros figurant en groupes de 4 ou 5 chiffres en face de chaque ligne, une clef pour assurer le secret de la correspondance (mélange des chiffres d'un groupe, en considérant le nombre des mille comme formant une entité à un ou deux chiffres inséparables — addition d'un nombre à chaque groupe, etc).

Ces dictionnaires donnent donc des cryptogrammes à groupes de 4 chiffres, et à groupes de 5 chiffres qui commencent sauf transposition par les premiers chiffres de la numération 1, 2 et 3. Quelquefois les correspondants unifient la forme des groupes en faisant précéder d'un 0 les groupes de 4. Quelquefois aussi, les idoines appelés à employer ces dictionnaires adoptent une pagination en 3 chiffres, s'étendant de 000 à 999, avec des manques

ou avec plusieurs numéros pour chaque page. Mais beaucoup de télégrammes présentent l'aspect que nous avons cité plus haut, et comprennent des groupes de 4 chiffres quelconques et des groupes de 5 commençant seulement par les plus bas chiffres de la numération.

Puisqu'il y a des cas où les correspondants sont amenés à placer un zéro devant les groupes de 4, les auteurs de certains dictionnaires ont fait imprimer ce 0, et ont ainsi des codes à groupes de 5 chiffres. La *Clave telegrafica* de Darhan (Madrid, 1912) présente ainsi une suite de groupes allant de 00001 à 32400, chaque ligne étant numérotée par un groupe complet. Son auteur du reste, d'après l'avant-propos, ne l'avait pas destinée à être employée à des transmissions en groupes de chiffres, mais elle devait servir à remplacer un mot du texte clair par un autre mot de la table servant de mot de convention, la correspondance entre ces 2 mots reposant sur des opérations arithmétiques convenues reliant les groupes numériques qui représentent ces deux mots. Mais nous avons vu le Darhan employé comme dictionnaire à groupes codiques en chiffres, avec des changements dans l'ordre des chiffres (transposition dans le groupe codique).

Le *Slater's Code* (Londres, 1906) avec 25.000 groupes, est conçu pour le même objet que le Darhan et donne lieu à la même remarque.

Un certain nombre de dictionnaires qui présentent des mots codiques renferment aussi des groupes codiques en chiffres, commençant à 00001 et allant jusqu'à la fin du dictionnaire (75.800 pour le Lieber's, 103.000 pour l'A B C, 379.300 pour le *Western Union*, etc... On peut ainsi trouver des groupes de 6 chiffres), et parfois, dans des télégrammes, on trouve l'emploi de ces groupes, mais plus généralement les groupes ne sont employés dans ces dictionnaires que pour permettre des opérations facilitant l'usage d'un procédé cryptographique, conduisant à la transmission des mots codiques en lettres.

Enfin, comme type de dictionnaire en groupes de 5 chiffres nous citerons le *Dictionnaire chiffré Diplomatique et Commercial* d'Airenti (Paris). Ce dictionnaire commence à vieillir parce qu'il contient beaucoup de noms propres de notabilités du monde financier, politique, commercial, etc., aujourd'hui mortes, disparues ou remplacées. Mais il est très complet, et a été très employé.

L'Airenti comprend les groupes de 5 chiffres de 25.001 à 84.200, il ne renferme donc pas de groupes commençant par 1 ou 9, ou par 20, 21, 22, 23 et 24. C'est un des moyens d'en reconnaître l'emploi. Il arrive souvent qu'on intervertisse l'ordre des chiffres dans chaque groupe; il est donc bon, quand on soupçonne l'emploi de l'Airenti, de vérifier si, en considérant individuellement la série des 1er, 2e, 3e, 4e et 5e chiffres des groupes on ne trouve pas une de ces séries réduites aux nombres de 2 à 8. Certains chiffreurs emploient une autre numération : les groupes de 5 chiffres comportent dans chaque page une partie immuable : les 3 premiers chiffres, et seuls les 2 derniers chiffres changent par ligne de 01 à 00 en passant par 99. D'autre part, en haut de la page, figure une pagination commençant à 101. On remplace alors souvent les 3 chiffres des centaines, mille et dizaines de mille de chaque groupe par les 3 chiffres du numéro de la page. Alors la numération de l'Airenti va de 10.101 à 69.200. Le procédé prôné par l'inventeur pour la cryptographie est l'addition aux groupes codiques en chiffres de nombres, soit le même pour chaque groupe, soit différents, suivant une certaine loi. Nous reviendrons plus loin sur ces procédés.

Nous arrêterons ici les indications sur les codes à groupes codiques en chiffres.

Dictionnaires à groupes codiques en lettres. — Comme dictionnaires à groupes codiques en lettres, nous citerons d'abord des documents anciens où les groupes de lettres ont été employés pour obtenir un plus grand nombre de combinaisons que n'en donnent les groupes de chiffres de même longueur (26 lettres au lieu de 10 chiffres),

sans qu'on ait cherché à se soustraire au paiement d'un mot pour 5 caractères.

Le Dictionnaire Mamert Gallian (Paris, 1874), contient ainsi près de 17.600 (26^3) « ternaires », ou groupes de 3 chiffres. Le système cryptographique prôné est une transposition dans le groupe ou une substitution simple avec alphabet normalement ordonné portant sur les lettres. Mais Valerio, dans le 2e volume de son ouvrage, remarque que toutes les opérations des substitutions à clefs périodiques avec alphabets quelconques peuvent s'effectuer sur la suite de lettres formées par un télégramme Mamert Gallian; il étudie des solutions des problèmes de cette nature, où il a recours à des considérations de fréquence extrêmement intéressantes. Nous citons cette étude pour mémoire : elle peut être utile à analyser comme exercice, à titre d'entraînement pour certaines recherches de surchiffrements compliqués, mais dans la pratique nous n'avons jamais constaté nous-même l'emploi du dictionnaire Mamert Gallien.

Le *Chiffrier-Wörterbuch* de Katscher (Leipzig, 1889) comprend des groupes codiques de 4 lettres dont la première et la 3e sont a, b, c, ou d, sans aucune des autres lettres de l'alphabet (e quelquefois comme 1re lettre), les deux autres lettres étant quelconques.

Sans insister sur ces documents anciens, nous passerons alors aux dictionnaires plus modernes à groupes codiques de 5 lettres prononçables.

Comme nous l'avons dit, le but des auteurs de ces ouvrages est d'économiser sur les taxes télégraphiques. On n'a donc pas hésité de faire des volumes très gros (le *Western Union* a 1.800 pages) et très chers, pour y placer toutes les formules et expressions dont on peut imaginer l'emploi probable et qui comprennent plus d'un mot : les dates pour les 365 jours de l'année, les prix en livres, dollars, francs, roubles, etc... de 1/2 unité en 1/2 unité, les poids, les noms des banques de tous les pays, la liste des valeurs cotées en Bourse, etc... L'économie qui résulte de la taxation de deux de ces formules pour un seul

mot (deux groupes de 5 lettres formant un mot codique de 10 lettres, prononçable) paie rapidement le prix du volume quand on correspond beaucoup. Beaucoup de ces dictionnaires possèdent en fin de volume une table des mots codiques classés alphabétiquement d'après leurs dernières lettres; si des erreurs de transmission altèrent le mot codique, on a ainsi 2 tables pour rechercher le mot intact : le dictionnaire lui-même dans l'espoir que le début du mot est inaltéré, la table finale pour le cas où, le début étant changé, la fin serait intacte. De plus, les auteurs, en choisissant les groupes codiques, s'imposent fréquemment la condition qu'un groupe employé diffère de tout autre groupe du dictionnaire d'au moins deux lettres, ce qui rend les confusions moins redoutables.

Nous ne pouvons donner beaucoup de détails sur ces dictionnaires, qui sont extrêmement nombreux déjà et se multiplient tous les jours. Ils se distinguent les uns des autres par certaines particularités des mots codiques, et par les groupes représentant les mots les plus fréquents, si bien qu'on peut arriver à reconnaître *a priori* les télégrammes où l'on a employé un de ces codes. Ainsi les groupes du Bentley (anglais), un des plus employés à l'heure actuelle (1923), commencent indifféremment par des voyelles et des consonnes. On y rencontre des séquences de deux voyelles et de deux consonnes et des redoublements (abbig, abjin, cyapt); mais si la 1re lettre est une voyelle la 2e est une consonne et, sauf rares exceptions, donnant des bigrammes très prononçables (cl, ch, fl, kl). Une 1re lettre consonne est suivie d'une 2e lettre voyelle, les lettres q et x ne sont pas employées, et on ne trouve pour y et z que des suppléments à remplir par les correspondants, donc d'un emploi rare. Le point se dit tugny.

Dans l'A B C, 6e édition (anglais) on trouve des séquences de 2 voyelles ou de 2 consonnes dans les deux premières lettres (aetma — bjaul — bruwn). La lettre q est employée, mais seulement suivie de u (quawd, quuoj) et les groupes se succèdent régulièrement jusqu'à zyzyo.

Dans le Code interprète Veslot (français) il y a des groupes codiques de 4 lettres représentant des syllabes, et

des groupes codiques de 2 et 3 lettres pour les formes grammaticales. Les mots du télégramme ont donc des longueurs variables. Tous les groupes de 5 lettres sont du type consonne-voyelle-consonne-voyelle-consonne; les seules lettres finales sont c, d, g, l, n, r, s, t, x, z (10 en tout). Les lettres h, k, q, w, x, ne sont pas employées comme initiales. Le code proprement dit s'arrête à nenel, et la suite ne comprend que des suppléments. Ce code, comme certains autres, a des éditions en diverses langues, mais tandis qu'une seule table suffit pour le code de base, en français, il faut dans les autres langues des tables chiffrantes (où les mots sont par ordre alphabétique et où les groupes codiques sont dans l'ordre imposé à la fois par leur sens en français et par le mot étranger qui traduit ce sens) et des tables déchiffrantes (où les groupes codiques sont dans l'ordre).

Le *Rudolf Mosse Code* (allemand, Berlin, 1922) a des groupes codiques de 5 lettres, où le Q n'est pas employé. Les groupes sont de formes très diverses (abkru, aboow, aeboa, daool, daoud, deass, heuur, tropt) et se succèdent jusqu'au z. Le même volume renferme un code réduit avec des groupes de 3 lettres qui se transmettent par grou-groupe de 10, à savoir 3 groupes de 3 et une lettre témoin. L'emploi de la lettre témoin se rencontre d'ailleurs sous des formes diverses dans d'autres ouvrages, par exemple dans le Code international Lugagne (édité Paris), en 7 langues, qui contient plus de 6.000 groupes, tous de 3 lettres. Elle a pour but de faire apparaître les fautes de transmission. Par exemple dans le *Rudolf Mosse Code*, chaque groupe de 3 est affublé d'un chiffre pris au hasard de 1 à 9, exemple : ahm 1, aup 4, evi 6, écrit au-dessous. Quand on a chiffré 3 groupes, par exemple ahm aup evi, on fait la somme de leurs chiffres $1 + 4 + 6 = 11$. On trouve à chaque page du code une table donnant les correspondances des lettres de l'alphabet en nombres de 3 à 27 ($1 + 1 + 1$ à $9 + 9 + 9$). En face de 11 se trouve z : on écrit ahmaupeviz. Supposons que le télégraphe transmette ahnaupeviz. Le destinataire fait le total (ahn $= 4$) $4 + 4 + 6 = 14$; z donne 11, il y a donc

une erreur, et il n'accorde pas confiance au sens de la phrase. Certaines parties du Code Mosse avec des représentations numériques peuvent donner lieu à l'emploi d'un condenseur (voir plus loin) permettant de gagner 50 % sur le prix de transmission, et les mots de 10 lettres du condenseur sont formés de bigrammes voyelle-consonne ou consonne-voyelle.

Le Code Marconi (anglais avec deux autres langues par volume) a des groupes de formes diverses de 5 lettres, qui, en grande majorité, ne commencent pas par 2 voyelles ni par 2 consonnes ni par q. Les dernières lettres ne sont ni h, ni j, ni q, ni v, ni w, ni x. Certains groupes, représentant des nombres, d'après une autre table, commencent par 2 consonnes ou qu suivies de syllabes de 2 lettres.

Le *Western Union* (américain) comporte pour chaque ligne deux groupes codiques de 5 lettres à employer au choix, l'un prononçable, l'autre formé de 5 lettres quelconques, pouvant être par hasard prononçables, ou non. Les lettres q et x ne sont pas employées comme initiales, ni la lettre z dans les groupes prononçables, qui, à partir de r, correspondent à des nombres, dates, valeurs, etc... Ce code est très riche, il contient près de 380.000 groupes.

Nous n'insisterons pas sur ces exemples. On voit suffisamment ainsi que les différents dictionnaires ont leur physionomie propre, et que certains groupes codiques peuvent donner lieu, même quand on n'a pas sous la main la collection des codes, à l'affirmation qu'ils ne viennent pas d'un dictionnaire donné.

D'autres dictionnaires, publiés en général avant les augmentations des taxes télégraphiques qui ont suivi la guerre de 1914-1918, emploient des mots codiques tirés de langues parlées, d'une longueur telle qu'ils comptent pour un mot chacun, mais les erreurs y sont moins redoutables que dans les mots codiques forgés, parce que les mots des langues parlées se reconstituent en général plus facilement que ces derniers.

Le Code français AZ a employé des mots codiques tirés uniquement du hollandais, dans le but, dit l'auteur, de faire reconnaître plus facilement l'emploi de l'AZ, et aussi d'empêcher la confusion des mots laissés en clair par le chiffreur avec des mots codiques, la langue hollandaise n'étant pas très usitée.

Le Liebers emploie des mots codiques de toutes langues, commençant par A. B. C. D. E. Il est publié en plusieurs langues, et, pour éviter toute difficulté inhérente à la mise en ordre des mots du clair en ordre alphabétique, il est divisé en courts chapitres se rapportant à un sujet donné : la table alphabétique de ces sujets, dans la langue de l'exemplaire du code, est en tête, et renvoie aux pages utiles, mais à ces pages les mots ou formules ne sont pas en ordre alphabétique. Par contre, les mots codiques sont rigoureusement dans cet ordre.

Le Code ABC (5e édition, anglais) emploie également des mots codiques de toutes langues, et, dans la partie principale ou dans ses divers suppléments, il emploie comme lettres initiales tout l'alphabet de A à Z.

Nous n'en citerons pas d'autres du même type. Nous rappellerons seulement qu'un grand nombre de maisons de commerce ont des codes avec mots convenus, dont l'expédition correspond par exemple à la demande d'une pièce de rechange d'une machine. Il existe de petits codes pour donner des nouvelles à des absents, pour retenir des chambres d'hôtel, etc..., et une bibliothèque de cette littérature, nécessaire pourtant à un important bureau de décryptement, est presque toujours bien incomplète. La plupart de ces codes ont d'ailleurs des aspects caractéristiques : ainsi le *Marconi's Wireless Telegraphic Code*, qui renferme près de 12.000 formules, n'a que des mots codiques commençant par A (de Abaissaix à Alumbrado).

Parfois ces codes renferment des mots codiques, *forgés*, de plus de cinq lettres. L'*Ingénieur Code* de Galland (allemand) qui a près de mille pages, emploie des mots codiques de sept lettres, commençant par les lettres de A à M.

C'est la même disposition que l'on trouve dans le *Teles-*

cand, dont nous avons déjà parlé comme dictionnaire en groupes codiques de 4 chiffres. L'auteur de cet ouvrage a forgé des mots codiques de 9 lettres, pouvant être portés à 10 avec une lettre convenue pour indiquer l'emploi de la 2e colonne de la page ou la conjugaison; les mots sont formés de radicaux forgés de 6 lettres suivis de finales de 3 lettres au nombre de 6 seulement (aba, bec, cie, den, eru, ion). Leur origine est donc particulièrement facile à reconnaître.

Nous arrêterons ici ces indications sur quelques-uns des nombreux types de dictionnaires que l'on trouve dans le commerce. Les codes secrets, pour une bonne partie, rentrent dans des formules analogues.

Procédés cryptographiques. Surchiffrement. — Nous avons, à propos du Sittler, indiqué une série de procédés cryptographiques employés avec les dictionnaires. Nous allons reprendre et développer ce même sujet.

L'application d'un procédé cryptographique au cryptogramme obtenu en remplaçant des mots du clair par leur représentation dans le dictionnaire constitue une superposition de procédés, ce que nous avons appelé un surchiffrement.

Nous rappellerons d'abord les procédés déjà mentionnés à propos du Sittler : transposition des éléments d'un groupe, substitutions portant soit sur certains éléments du groupe, soit sur tous. Ces substitutions peuvent, comme nous l'avons vu, être du type à représentation unique, basé sur un tableau de concordance, ou à représentations multiples, un nombre étant représenté par le résultat d'une opération arithmétique dont on écrit les termes, et ces termes pouvant varier, ou bien encore une page portant plusieurs numéros.

On présente souvent la substitution sous une forme un peu différente de celle que nous avons indiquée plus haut. Nous avons surtout montré la substitution à un numéro de page ou de ligne d'un autre nombre de 2 chiffres. On la présente souvent sous forme de tableaux numériques, donnant pour chaque chiffre de 0 à 9 un nouveau

chiffre à substituer, opération qui ne se fait qu'après le chiffrement initial. Il faut remarquer que des opérations de ce genre n'altèrent pas la physionomie d'un groupe : si le 1er, le 3e et le 5e chiffre, par exemple, d'un groupe codique sont semblables, on trouvera 3 chiffres semblables dans le groupe après la substitution. Les répétitions d'un groupe donneront lieu également à des répétitions de groupes si l'on n'emploie qu'un seul tableau de substitution. On est donc amené, pour faire disparaître les répétitions, à changer fréquemment de tableau de substitution. On peut aussi, même au cours d'un cryptogramme, chercher à changer la physionomie des groupes en employant des tableaux différents pour les différents chiffres du groupe (1er, 2e, 3e, etc...), ce qui revient à une substitution à double clef, et, pour éviter avec ce système les répétitions de groupes qui se produiraient s'il y avait autant de tableaux que de chiffres dans chaque groupe, puisque chacun des chiffres d'un groupe répété serait remplacé par un *même* autre chiffre dans les répétitions, on peut employer une substitution à double clef avec une clef de longueur différente de la longueur d'un ou plusieurs groupes.

Dans le même ordre d'idées que les substitutions, nous citerons les clefs additives (ou soustractives). On ajoute parfois un certain nombre à chaque groupe. On peut, pour éviter les répétitions, modifier d'un groupe à l'autre le nombre à ajouter. On peut aussi, pour éviter autant que possible d'ajouter un même nombre à la répétition d'un même groupe, choisir le nombre de chiffres de la clef additive aussi différent que possible du nombre des chiffres d'un ou plusieurs groupes. On peut encore, en choisissant un document auxiliaire qui donne de longues listes de chiffres (table de logarithmes, code lui-même s'il est à bâtons rompus), avoir des clefs indéfinies. Enfin on peut faire des clefs autoclaves. Pour l'emploi de tous ces systèmes, et afin de pouvoir opérer de la gauche à la droite, il est commode d'additionner simplement le chiffre du groupe au chiffre de la clef, sans jamais tenir compte des retenues.

En traitant la suite des groupes tirés du dictionnaire comme un texte, on peut faire subir à ce texte toutes les transpositions imaginables. Parmi celles-ci on peut citer, comme étant d'un emploi commode, les transpositions à tableau avec relevé successif des colonnes dans l'ordre indiqué par une clef, soit toutes les colonnes de haut en bas, soit suivant une loi convenue. On rencontre souvent aussi des transpositions reposant sur le mélange des chiffres de deux lignes superposées de la suite des groupes écrite en ligne d'une longueur convenue.

Les correspondants tiennent compte, quand ils adoptent des surchiffrements, de la répercussion possible des erreurs de transmission. L'omission d'un ou plusieurs groupes par le télégraphe peut avoir dans certains cas pour résultat de rendre le télégramme absolument incompréhensible. C'est pourquoi, avec certains procédés, on cherche à limiter le mélange des chiffres au strict nécessaire pour éviter les répétitions et pour cacher les groupes du dictionnaire, tout en se réservant le moyen de traduire tout au moins une partie du texte en cas d'accident, ce que ne permettrait pas un mélange trop général des chiffres du document.

Parmi les procédés de cryptographie employés sur les dictionnaires et prônés par leurs auteurs, nous mentionnerons ceux qui figurent dans la clef Darhan et quelques autres. Au mot à chiffrer correspond un groupe. On fait subir à ce groupe une opération : addition, soustraction, interversion de certains chiffres, etc... On obtient un nouveau groupe auquel, dans le dictionnaire, correspond un mot de la langue. C'est ce mot qu'on écrit dans le cryptogramme. Parmi les opérations prévues par Darhan se trouve le sectionnement en tranches de 4 chiffres de la suite des groupes de 5 chiffres obtenus par la traduction du clair, et le remplacement de chacun de ces groupes par un mot du dictionnaire, qui se trouve alors toujours dans les premières pages, et qui par suite, ce qui donne une hypothèse sur la méthode, commence par une des premières lettres de l'alphabet. Avec les dictionnaires à mots codiques, ce système de cryptographie nous a paru

l'un des plus employés : on remplace le mot codique par un autre mot codique, choisi généralement à un intervalle donné du premier.

Emploi des livres. — Avant de passer aux indications générales sur le décryptement des dictionnaires, nous dirons encore un mot de l'emploi des ouvrages imprimés qui ne sont pas destinés à la correspondance chiffrée, et des combinaisons ou condenseurs.

De même qu'on peut chercher dans une page d'un livre la représentation d'une lettre définie par le numéro de la ligne où elle se trouve et la place qu'elle occupe dans cette ligne, de même on peut chercher dans un livre un mot, et le représenter par ses coordonnées dans ce livre. Avec des sujets très spéciaux, et en ne chiffrant que certains mots, on peut avoir recours à des ouvrages quelconques ou à des répertoires, tels que le *Tout Paris* pour chiffrer des noms et des adresses. Mais, on peut toujours faire appel à un dictionnaire qui contient tous les mots d'une langue, et, profitant du nombre énorme de dictionnaires, soit monolingues, soit bilingues, qui contiennent la liste alphabétique de ces mots, mettre le décrypteur en présence d'une très grosse difficulté s'il veut chercher le dictionnaire employé. L'emploi de ces procédés se révèle généralement par la forme des groupes du cryptogramme, où la séparation entre le numéro de la page et celui de la ligne ressort généralement, et où le numéro de la ligne ou du mot dans la page atteint rarement 99. Le décrypteur trouve à résoudre alors le problème de la reconstitution d'un dictionnaire ordonné.

On emploie aussi avec le dictionnaire ordinaire un procédé analogue à celui que nous avons signalé plus haut à propos du Darhau, le remplacement du mot du clair par un autre mot du dictionnaire repéré par rapport au premier (5 au-dessus, même numéro de la page précédente, etc.), ce qui donne des textes incohérents.

Combinaisons codiques. — Nous avons vu que la taxa-

tion télégraphique rendait moins onéreuse la transmission des mots codiques prononçables en lettres que celle des groupes de chiffres. On a donc été amené à remplacer par des groupes de lettres les groupes de chiffres des anciens dictionnaires. Depuis déjà longtemps des tableaux de substitution de groupes de 2 lettres à des groupes de 2 chiffres (facilement obtenus par la combinaison de 5 voyelles et de 20 consonnes), et de trigrammes prononçables aux groupes de 3 ou de 4 chiffres, sont dans le commerce [combinaison Pierron, éditée à Paris; combinaison du Bottin (volume Etranger), Voller's 12 Figure system édité à Hambourg, etc...]. Ces combinaisons, comme les codes, ont leurs particularités d'emploi de lettres qui permettent de reconnaître si un document a pu être chiffré ou non avec l'une d'elles. Leur emploi constitue un surchiffrement par substitution, et des combinaisons de ce genre peuvent être inventées par les correspondants et modifiées de façon à faire disparaître les répétitions de groupes.

Le code Rudolf Mosse, par exemple, bien que composé en groupes de 5 lettres, présente en fin de volume un « condenseur » pour l'emploi de certaines indications numériques en 2 et 3 chiffres. On peut, dans des questions techniques, substituer ces indications aux indications de même nature en groupes de 5 lettres, si bien que 10 chiffres remplacent 4 groupes de 5 lettres. On les « condense » ensuite en un nouveau groupe de 10 lettres. Ce condenseur a deux bigrammes différents pour figurer chacun des nombres de 00 à 99. L'emploi de l'un ou l'autre de ces bigrammes pour chaque tranche de 2 est réglé d'après le total des valeurs numériques des chiffres au moyen d'un tableau spécial, ce qui est sensé donner un contrôle sur les erreurs de transmission, mais ce qui constitue un procédé assez compliqué sans que l'avantage de cette complication soit bien évident.

Bien que ces combinaisons n'aient été, en principe,

prévues que pour réaliser des économies, elles peuvent constituer des procédés cryptographiques, et être désagréables pour les décrypteurs, en raison du grand nombre de systèmes qu'elles constituent et qui se superposent à de très nombreux dictionnaires.

CHAPITRE XV

GÉNÉRALITÉS SUR LE DÉCRYPTEMENT DES SYSTÈMES A DICTIONNAIRES

Nous ne pouvons donner que des directives très imprécises sur les procédés de décryptement des systèmes à dictionnaires. Le problème, assez simple quand on est sûr du dictionnaire employé, devient extrêmement compliqué lorsqu'on ignore non seulement le dictionnaire et son type, mais la langue des correspondants, et ce n'est pas, à notre avis, en se tenant dans le domaine de la science cryptographique pure que l'on pourra ordinairement le résoudre. La cryptographie, au point de vue militaire, naval, diplomatique ou policier, n'est qu'un élément du service des renseignements, et tous les éléments de ce service doivent collaborer à la découverte de la traduction d'un cryptogramme.

Nous indiquerons sur quelques exemples classiques comment des renseignements d'ordre général sont venus orienter des décrypteurs.

Toutefois, pour pouvoir utiliser les renseignements, ou même les faire rechercher, il faut que le service de décryptement ait préparé des matériaux et des bases d'hypothèse; c'est de cette préparation que, faisant appel à nos souvenirs et à notre expérience, nous allons parler tout d'abord. Bien entendu, les procédés que nous indiquerons, pour les avoir appliqués ou vu appliquer avec succès, ne sont donnés qu'à titre d'exemple. Ils peuvent ne pas être les meilleurs et ne sauraient être proposés comme une règle.

Examen des cryptogrammes. — Le premier examen qu'il est bon de faire subir à un cryptogramme a pour but de rechercher s'il est surchiffré ou non, et si l'on connaît le dictionnaire employé. On cherchera pour cela des répétitions de groupes ou de fragments de groupes, en faisant au besoin un relevé sommaire en colonnes d'après le 1er caractère de chaque groupe (tous les groupes commençant par 0, tous les groupes commençant par 1, etc...) ou, si l'on suppose, d'après quelques répétitions, l'existence de tranches de 4 ou de 3 caractères, d'après le premier caractère de chaque tranche. Si l'on n'a pas de répétitions, il faut craindre le surchiffrement, et nous réserverons l'étude de cette hypothèse. Si l'on a des répétitions, et que l'on ne soit pas certain que l'on a affaire à un dictionnaire secret, on cherche dans le répertoire des groupes fréquents dans les dictionnaires que l'on connaît si des éléments de ces répétitions peuvent permettre d'identifier des mots et des pages, comme nous l'avons dit à propos du Sittler.

Mots en clair mélangés au chiffre. — Remarquons que la recherche de l'identité d'un groupe et d'un mot est grandement facilitée quand on a *à priori* des hypothèses sérieuses sur le sens du mot représenté par le groupe, et qu'on n'en est pas réduit à examiner seulement des possibilités ou impossibilités basées sur la liste des mots se trouvant par exemple à une certaine ligne du Sittler (relevé par lignes; voyez plus haut). Or la présence de mots en clair facilite de beaucoup ces hypothèses. L'habitude de ne chiffrer que quelques mots d'un texte qu'on veut tenir secret est déplorable au point de vue de la sécurité du chiffre, elle est proscrite dans tous les bureaux de chiffreurs. Toutefois, un chiffreur très habile peut se permettre de garder volontairement en clair les mots que nous avons définis comme mots vides : prépositions, conjonctions, articles, etc..., dont le chiffrement donne des fréquences et des renseignements au décrypteur. Il peut ainsi priver celui-ci de ces renseignements. Nous ne conseillerons cependant pas de jouer ainsi avec la difficulté.

La présence de mots clairs garantit au décrypteur que l'on n'a pas employé de surchiffrements qui englobent la totalité du document (transposition à tableau par exemple). Elle le renseigne, sauf malice du chiffreur, sur la langue employée dans les parties chiffrées (cette malice se rencontre, peut-être même sans préméditation, pour certaines questions commerciales où les correspondants prennent les mots à chiffrer dans un dictionnaire unique, et où l'un d'eux, fixé dans un pays de langue étrangère, emploie cette langue pour le clair. Cela fait une sorte de sabir, mais cela se rencontre). Surtout, comme nous l'avons dit, le clair permet les hypothèses sur le sens des groupes d'après le contexte. Souvent, lorsque les mots en clair sont très rares, et que l'on suppose l'emploi d'un dictionnaire donné, la présence dans ce dictionnaire d'un mot laissé en clair dans le cryptogramme doit faire renoncer à l'hypothèse, car le chiffreur, consciencieux d'autre part, n'a laissé en clair que les mots qu'il n'a pas trouvés dans son dictionnaire. Ainsi « obus » se trouve dans Bazeries et non dans Sittler : un texte un peu long où le seul mot en clair sera « obus » ne sera probablement pas chiffré avec Bazeries, mais pourra l'être avec Sittler.

Relevé des groupes. — Lorsque ce premier examen a permis de conclure, grâce à des répétitions, sur l'emploi d'un code et la longueur des groupes, et qu'aucun rayon de lumière n'a permis l'identification du dictionnaire employé et du procédé cryptographique simple appliqué à ce dictionnaire, il y a lieu de procéder à un « relevé » (ou à « l'inscription ») des groupes. Si l'on dispose, ou si l'on prévoit qu'on pourra disposer, de beaucoup de documents, et qu'il y aura lieu de procéder à la reconstitution d'un dictionnaire, on fera bien de commencer immédiatement ce relevé sur un registre, en numérotant les documents et en notant, en face de la ligne du registre qui porte le numéro du groupe, le numéro de chaque document où le groupe apparaît (on peut faire de simples registres en papier quadrillé, dont on numérote les pages et dont on repère les lignes par exemple de 10 en 10). Si

l'on croit, d'après les correspondants, que l'on a affaire à un dictionnaire du commerce et qu'on le trouvera en n'étudiant que des documents peu nombreux, on fait un relevé plus simple, sur une feuille de papier divisée en colonnes, en mettant les groupes approximativement plus ou moins haut dans ces colonnes, pour les placer peu à peu, à mesure que le relèvement se poursuit, à leur place numérique.

Ces relèvements permettent de reconnaître : 1° les fréquences; 2° les séquences, si l'on a soin, chaque fois que l'on inscrit un groupe déjà rencontré, de se reporter à ses apparitions antérieures.

Les séquences correspondent ordinairement, soit à des suites de mots du dictionnaire revenant plusieurs fois dans les textes, soit à des mots syllabés. Parmi les premières, les noms de société, les quantités de marchandises, les sommes d'argent, etc..., sont des sujets fréquents; des séquences rompues, où des groupes semblablement placés sont différents tandis que d'autres sont les mêmes, suggèrent l'hypothèse de nombres (mille trois cent cinquante francs, mille trois cent cinquante-deux francs, les groupes représentant 50 et 52 différant seuls). Parmi les syllabés, la connaissance des sujets intéressant les correspondants peut donner des idées sur les mots représentés : des télégrammes d'agences venant d'une ville où se tient une conférence ont des chances de renfermer les noms d'hommes politiques, par exemple.

Si l'on considère les groupes fréquents, on peut trouver qu'en calculant la distance qui sépare deux d'entre eux dans le relevé (par une soustraction), on retombe sur la distance qui sépare deux groupes fréquents d'un dictionnaire connu, et que par suite on n'avait affaire qu'à une clef additive portant sur un seul groupe à la fois dans un dictionnaire que l'on possède. En considérant les groupes fréquents et les séquences, on peut faire des hypothèses sur certains mots. Si j'ai 5202 5383 0073 2289 4203 comme séquence fréquente dans un télégramme d'avril 1922 venant de Gênes, et que 5204 5257 5285 soient fréquents dans ce télégramme, je ne craindrai pas

d'essayer L.lo.y.d Georges et la, le, les, pour sens de ces divers groupes, et je retrouverai le Sittler PALI avec la clef + 102.

Quand on ne peut retomber sur un dictionnaire connu, on doit se lancer dans la reconstitution d'un dictionnaire.

Reconstitution d'un dictionnaire ordonné. — Cette opération, lorsque le dictionnaire est ordonné, n'offre généralement pas de difficultés insurmontables; il en offre d'autant moins que le dictionnaire est moins riche. Toutefois, pour les dictionnaires commerciaux du type récent où des pages entières sont consacrées aux expressions de sommes d'argent variant de 10 francs en 10 francs par exemple, et où, constamment, la phrase « je possède » telle chose se trouve à une ligne de distance de la phrase « je ne possède pas » cette chose, les difficultés ne pourraient être surmontées qu'avec une connaissance technique très exacte des sujets traités.

Il est presque toujours avantageux, quand on le peut, d'avoir un dictionnaire chiffré ayant à peu près le même nombre de groupes que le dictionnaire que l'on étudie, et de même langue que ce dernier : on se rend compte ainsi de la position approximative qu'occupent les mots fréquents, et, si la pagination ne commence pas par 00 à la première page, ce qui arrive souvent (de façon à ne pas commencer par exemple en français le dictionnaire par la fréquente A), cela permet de faire tout de suite des hypothèses sur le décalage par une sorte de graphique des fréquences où l'on marque sur une droite pour le dictionnaire connu et le dictionnaire inconnu, des segments successifs proportionnels au nombre de groupes qui sépare deux groupes fréquents.

Nous avons, presque toujours, dans les études de ce genre, cherché d'abord les ponctuations. Souvent les télégrammes se terminent par une ponctuation. Souvent une ponctuation précède certaines des répétitions du groupe qui figure en tête d'un télégramme, puisque celui-ci commence une phrase. Quand, d'après ces remarques,

et d'après la position dans les textes de certains groupes qui semblent se répéter à des distances convenables pour jouer le rôle du point ou de la virgule, et qui ne se juxtaposent pas, on est arrivé à des hypothèses sérieuses sur l'identification des ponctuations, on fait appel aux particularités des langues pour des hypothèses sur les mots qui commencent et qui finissent les phrases, sur les articles, les pronoms, les auxiliaires, les verbes sous forme de participes passés, etc. Des relevés groupant les séquences qui précèdent et suivent un groupe qu'on étudie et permettant de les comparer entre elles sont souvent utiles. Tous ces travaux, quand un décrypteur les fait lui-même et ne les confie pas, sous prétexte qu'il s'agit d'opérations matérielles, à des aides, font connaître parfaitement à ce décrypteur les cryptogrammes qu'il étudie, et lui permettent de faire des remarques qui se traduisent par des hypothèses nouvelles.

Il nous a été fréquemment utile de faire des relevés des 10 à 20 premiers groupes des cryptogrammes et des 10 à 20 derniers. Nous y avons vu apparaître un certain nombre de séquences ou de répétitions de groupes, qui peuvent orienter les recherches postérieures. Dans les fins, on trouve les signatures, souvent précédées d'une ponctuation et de « fermez les guillemets ». Dans les commencements, on trouve les références, des formules telles que : Pour Monsieur... J'adresse le présent télégramme à... ou : Je reçois le télégramme suivant... On peut surtout trouver un élément précieux : la numération. Beaucoup de correspondants chiffrent les numéros et quelquefois la date de leurs télégrammes. On voit alors se succéder dans la série des documents, entre certains groupes qui ne changent que toutes les dizaines pour les nombres, ou que tous les mois pour les dates, des groupes changeant à chaque fois, mais reparaissant périodiquement et qui donnent les nombres successifs. Or, la numération est une très bonne base de départ pour l'attaque d'un dictionnaire.

Quand on a ainsi des hypothèses sur un certain nombre de groupes, on cherche à s'étendre, d'une part, dans le

dictionnaire, en donnant des sens aux groupes qui sont numériquement voisins, d'autre part, dans le cryptogramme, en cherchant à construire des éléments de phrase. Il n'y a plus ici à donner d'indications sur la manière de procéder : nous ne pouvons que recommander l'audace. Notre propre expérience, et celle de nos maîtres, nous ont souvent montré que des erreurs grossières sur les premières hypothèses n'ont pas empêché d'aboutir. La grande question, c'est de prêter à des « groupes » des sens en « mots », pour leur donner, dans les recherches successives, une existence pour ainsi dire, une personnalité qui les distingue du troupeau des autres groupes, qui attire l'attention sur eux et qui permette d'apprécier la valeur des assemblages que font naître dans le cryptogramme ces premiers essais : les corrections viennent ensuite. C'est donc dans cette période de l'étude que l'on se rend ordinairement compte de la contexture du code, que l'on voit s'il a des tables à part du « dictionnaire » proprement dit : syllabes, noms géographiques, verbes auxiliaires, numération, etc... (voir description du Baravelli), tous artifices adoptés par les auteurs pour essayer d'empêcher le décrypteur d'utiliser les mots fréquents ou les séquences trop visibles, les uns et les autres plus facilement traduits que le contexte, en vue d'obtenir des points de repère dans la liste alphabétique des mots.

Dispositions dangereuses des dictionnaires. — Ces artifices, suivant que l'emploi en est fait, ou non, par un chiffreur habile, risquent d'aller contre leur but. Exemple : l'auteur de dictionnaires que nous avons étudiés plaçait une liste des représentations des mots les plus fréquents à la page finale de son ouvrage (tout en laissant une autre représentation de ces mots à leur place alphabétique). Il y avait plusieurs dictionnaires en service à la fois, et les combinaisons de clefs changeaient fort souvent. Mais la fréquence du numéro de cette page était tellement supérieure aux autres (vu que les chiffreurs n'employaient presque jamais que cette représentation plus commode à trouver et non l'autre), que toutes les transpositions et

toutes les clefs additives ne portant que sur un groupe étaient faciles à retrouver par l'hypothèse que le groupement des deux chiffres les plus fréquents dans les groupes représentait le numéro de cette page. D'autre part, la seule présence de groupes trop nombreux provenant d'une même page trahissait l'emploi dudit dictionnaire. Les tables séparées de syllabes faciles à reconnaître (Baravelli) donnent lieu à des recherches sur un dictionnaire syllabique généralement très court à côté du gros dictionnaire, et par cela même, facile à reconstituer (finales des mots syllabés, noms propres probables, etc.). Une fois ce résultat obtenu, on a la signification d'un certain nombre de groupes qui permettent d'étendre la traduction, tout comme si le chiffreur avait laissé du clair. L'emploi d'un 5e chiffre permet souvent de reconnaître les verbes, quand par exemple on emploie un 5e chiffre pour : participe passé, participe présent, impératif, ce qui donne trois flexions différentes pour les verbes avec 3 cinquièmes chiffres en plus du groupe de 4 chiffres traduisant l'infinitif, alors que les substantifs n'en ont qu'une ou deux (pluriel, 2e mot de la ligne). La certitude qu'un mot est un verbe restreint les recherches, et permet, grâce aux règles de construction des phrases, de trouver les auxiliaires et les pronoms, etc...

Pendant que nous sommes sur ce sujet des précautions dangereuses, nous signalerons aussi le procédé parfois employé par lequel on adopte pour les mots qui ne se trouvent pas dans le dictionnaire une méthode de chiffrement alphabétique, une substitution lettre par lettre par exemple. Nous avons rencontré ce procédé combiné avec l'emploi de codes en groupes de lettres, où l'on indiquait le changement de procédé, soit par des groupes spéciaux signifiant commencement et fin du chiffrement alphabétique, soit par l'emploi d'une lettre rare isolée en tête et en queue du chiffrement alphabétique, alors que cette lettre ne figurait pas dans le code. L'examen des séquences d'un des groupes annonciateurs du changement, dans le premier cas, ou bien des groupes commençant par la lettre rare, dans le deuxième, fit appa-

raître la constante présence du 2e groupe ou de la 2e lettre, qui ne figuraient nulle part ailleurs, et donna l'éveil sur le procédé. Mais nous avons aussi rencontré ces chiffrements par substitution en lettres dans des cryptogrammes en groupes de chiffres, où ils crevaient les yeux et orientaient immédiatement le décrypteur.

On voit donc que parfois des précautions prises par les auteurs de dictionnaires se retournent contre la sécurité de leur ouvrage. En ce qui concerne les études cryptographiques et la formation des décrypteurs, nous citons ces exemples pour montrer quel est le genre des remarques à faire sur les relevés d'un dictionnaire, qui peuvent servir à trouver une entrée dans le document.

Recherche et emploi des traductions en clair. — Le décrypteur ne doit naturellement pas négliger tout ce qui peut faciliter l'identification des groupes avec des mots clairs. Parmi les moyens qui s'offrent parfois à lui pour lui fournir d'excellents renseignements à ce sujet, on doit compter la traduction plus ou moins exacte du cryptogramme.

Il arrive assez souvent, surtout si l'on a à travailler sur des documents de grande information : agences, diplomatie, guerre, etc..., que des articles de journaux par exemple fassent allusion à des objets traités dans des télégrammes chiffrés, et même reproduisent des informations transmises en chiffres. Une comparaison entre les répétitions d'un nom propre et les répétitions d'une séquence de groupes; la division en paragraphes résultant de la ponctuation quand on a déterminé celle-ci ou quand elle est laissée en clair, ce qui arrive; les nombres, s'il y en a, sont, entre bien d'autres, des éléments d'identification. Un atelier de décryptement devra donc avoir dans sa bibliothèque une ou deux collections d'organes d'information, pour pouvoir tenter de retrouver des renseignements sur le contenu possible des télégrammes d'origine et de date données. L'expérience prouve d'ailleurs que l'on éprouve bien souvent des difficultés en apparence incompréhensibles à retrouver certains renseignements

dans la presse ou dans les feuilles d'agences, mais ceci sort du cadre de nos études.

Une aubaine encore meilleure pour les décrypteurs, c'est la possession d'un même texte chiffré à des adresses différentes avec des systèmes ou des dictionnaires différents dont l'un est connu. Cette question des télégrammes, dits bilingues même si le texte clair en est unique, parce qu'ils sont chiffrés en plusieurs langages secrets, est une des plus intéressantes pour les cryptologues.

Travaux sur les dictionnaires à bâtons rompus. — Partis de conseils pour la reconstitution des dictionnaires ordonnés, nous en sommes arrivés à des réflexions qui s'étendent à la reconstitution de tous les dictionnaires. Si en effet le décrypteur est fortement aidé dans ses recherches par la connaissance des premières lettres probables d'un mot en clair correspondant à un groupe, connaissance qu'il tire de la position du groupe par rapport aux points de repères alphabétiques fournis par les groupes déjà traduits, et si cette ressource lui fait défaut pour reconstituer un code à bâtons rompus, le principe de la méthode reste pourtant le même. Là encore, on fera des hypothèses sur le sens de certains groupes, et on cherchera à identifier les ponctuations et certains mots, soit fréquents, soit caractéristiques. Seulement, comme on n'aura pas le frein de l'ordre alphabétique à respecter, on pourra s'envoler fort loin dans le royaume des hypothèses. Il faudra donc n'admettre un sens définitif pour un mot que lorsque ce sens aura été plusieurs fois recoupé dans des phrases différentes, et, pour pouvoir faire état de documents ainsi traduits, il faudra, à notre avis, avoir pu vérifier quelques traductions faites par le décrypteur sur des traductions obtenues d'autre part (journaux, par exemple) ou sur des séries de faits historiques conduisant à une similitude parfaite entre les documents et la réalité. Des vérifications de cette nature ont été souvent obtenues au cours de la guerre, et l'on reconnut, grâce à des numéros de régiments et à des dates, que certains codes à bâtons rompus avaient été employés pour chiffrer des commu-

niqués militaires, ce qui permit d'en identifier la plus grande partie des mots en toute sécurité.

On doit d'ailleurs remarquer que, dans un dictionnaire, il y a énormément de mots qui ne sont presque jamais employés, et que par suite il ne faut pas s'effrayer trop vite quand on voit qu'un code peut avoir 100.000 groupes par exemple. Le relevé des groupes des cryptogrammes ramènera les études, en général, à un nombre de groupes infiniment moindre.

Avant de parler des moyens par lesquels on est arrivé à révéler certains surchiffrements, nous ferons une observation importante sur la contexture des codes à bâtons rompus.

Comme nous l'avons dit, le point de départ des études est le relevé des groupes et la considération des fréquences. Les représentations multiples des mots fréquents présentent donc un intérêt de premier ordre pour gêner le décrypteur dans les codes comme dans les substitutions alphabétiques. On s'efforce d'ailleurs de créer même dans les codes ordonnés des représentations multiples, en donnant une place à des expressions où figure le mot fréquent, mais souvent ces expressions viennent seulement se juxtaposer les unes aux autres sur des lignes qui se suivent (et, et à, et le, et que, etc...), et, si elles suppriment l'évidence du groupe fréquent, elles laissent subsister dans le relevé une région où beaucoup de groupes voisins apparaissent, ce qui donne au décrypteur un élément d'étude. Dans les codes à bâtons rompus, cet inconvénient n'existe plus et les auteurs ne craignent pas de multiplier les représentations d'un même mot, ou *homophones*. C'est par l'étude des répétitions des séquences que, lorsqu'il a assez d'éléments, le décrypteur parvient quelquefois à identifier entre elles plusieurs représentations d'un même mot. On ne doit pas, dans l'étude des codes à bâtons rompus, s'effrayer de rencontrer plusieurs groupes ayant le même sens, et, lorsqu'on possède la traduction probable d'un cryptogramme, il ne faut pas s'étonner de ne pas trouver des répétitions de groupes aux places où on les attendait d'après le texte clair.

Exemples de décryptements. — Fort souvent les télégrammes sont surchiffrés. Il y a lieu de découvrir ces surchiffrements avant de passer à la reconstitution ou à l'identification du dictionnaire.

Sans pouvoir donner de règles pratiques complètes, nous citerons quelques exemples montrant comment on a pu profiter des fautes des chiffreurs ou de fautes de transmission pour résoudre des problèmes. On y verra la nécessité de suivre très attentivement la réception et le classement des documents, et d'en faire une étude sommaire et une comparaison rapide avec le contenu des dossiers, de manière à ne pas laisser échapper les chances qu'offre au décrypteur la maladresse de ses adversaires. Ces exemples ne sont pas de pure imagination, et on trouve de nombreux éléments d'études analogues dans les répétitions causées par de mauvaises transmissions T. S. F. Nous n'avons pas à rappeler qu'à l'heure actuelle le nombre des documents chiffrés qui transitent par T. S. F., et qui peuvent être écoutés par quiconque le désire, nous permet de puiser, sans manquer à l'actualité, tous les exemples qu'il nous plaira dans ce genre de correspondances.

Premier exemple. — On a intercepté les deux télégrammes :

x à y — n° 485. 9 groupes 05690 99355 82354 49717 82103 01729 60224 24389 8592

x à z — n° 486. 14 groupes 05690 92718 99355 82356 55114 49717 82600 22103 01729 61129 02242 43893 32598 592

Ces deux télégrammes ont des parties communes séparées dans le 2e par des parties absentes du 1er. On pourrait obtenir un aspect de ce genre avec un tableau de transposition simple, relevé de haut en bas, avec lequel on aurait chiffré pour Y un certain texte, pour Z ce même texte auquel ou aurait ajouté une phrase. On retrouverait alors dans le 2e cryptogramme, les colonnes du 1er, égales entre elles à une unité près, avec des « queues » prolon-

geant chacune de ces colonnes. Mais la fin du télégramme est la même dans les deux textes (il n'y a donc pas de queue à cette colonne). La 1re séquence commune a 6 chiffres, la 2e en a 8, la 3e en a 8, etc... Il faut alors admettre que le tableau a été relevé alternativement de haut en bas et de bas en haut. Comme il y a un 9 en tête de la deuxième partie commune ou en queue de la première, nous avons mal fait la coupure. La 1re séquence commune n'a que 5 chiffres: 05960, et la 2e en a 8 : 99355823. Les colonnes ont donc 4 et 5 chiffres.

Juxtaposons-les dans l'ordre où elles se présentent :

0	5	8	7	1	1	7	2	4	2
5	5	2	9	7	0	2	4	3	9
6	3	3	4	8	3	9	2	8	5
9	9	5	4	2	0	6	2	9	8
0	9				1		0		

(Quand nous avons eu 9 chiffres à répartir entre deux colonnes, nous avons toujours écrit la solution 5 + 4, mais la solution 4 + 5 était possible.)

Cherchons à rétablir les colonnes du 2e cryptogramme en ajoutant des « queues » à celles du 1er : nous avons 68 lettres à répartir en 10 colonnes, 8 colonnes de 7 et 2 de 6.

Entre la 1re et la 2e colonne, nous avons à répartir 92718, soit 5 chiffres. C'est impossible sans former une colonne de 8, donc notre 2e colonne est trop longue, il fallait adopter la solution 4 + 5.

0	5	5
5	3	8
6	9	2
9	9	3
0		5

Entre la 3e et la 4e colonne, nous avons à répartir 65511; 2 chiffres à la 3e colonne, 3 à la 4e, nous donnent deux colonnes de 7.

Entre la 5e et la 6e : 60022, 3 chiffres à la 5e, 2 chiffres à la 6e.

Entre la 7e et la 8e : 1129, 2 à chacune.

Entre la 9e et la 10e : 33259, 3 à l'une et 2 à l'autre.

Nous avons alors réparti nos colonnes en 3 séries : les longues du 1er cryptogramme, longues aussi dans le 2e; les courtes du 1er cryptogramme, longues dans le 2e; les courtes dans les deux cryptogrammes. Rien ne nous garantit d'ailleurs que notre répartition est absolument exacte; entre les deux dernières colonnes par exemple, nous pouvions répartir la séquence de 5 chiffres par 2 + 3 au lieu d'adopter 3 + 2.

0	5	1	2	5	7	1	4	7	2
5	8	0	4	3	9	7	3	2	9
6	2	3	2	9	4	8	8	9	5
9	3	0	2	9	4	2	9	6	8
0	5	1	0	8	1	6	3	1	9
9	6	2	9	1	1	0	3	1	5
2	5	2	2	7	5	0	2		

Si l'on rencontre d'autres éléments d'étude du même genre, on arrivera à pouvoir resserrer les limites de la position de chaque colonne. Nous supposerons que nous connaissons le dictionnaire qui a servi à chiffrer, et que c'est le Sittler. Nous cherchons seulement la clef. Nous ferons l'hypothèse suivante : on a mis une ponctuation entre la première partie du télégramme et la deuxième. 8163 représenterait donc une ponctuation. Dans le Sittler à pagination naturelle, 6831 vaut : point. Le Sittler étant employé ici en groupes de 4, la tranche du milieu des lignes impaires (10 colonnes au tableau) sera un groupe du Sittler où les chiffres seront transposés comme dans 8163. Nous trouvons 1547 (1re ligne) cinquième — 8984 (3e ligne) sur — 0725 avec.

Pour remettre en ordre les colonnes de la 1re tranche, nous chercherons ce qui peut précéder cinquième. Nous

trouverons 5102 = la. Les deux derniers chiffres de la 1re ligne forment le numéro de page d'un mot dont le numéro de ligne est 80. Nous trouverons Division, et le tableau sera rétabli.

Remarquons que l'hypothèse de la possession d'un dictionnaire n'est pas une hypothèse très audacieuse, même pour les dictionnaires supposés secrets. Dans la pratique, on n'adopte quelquefois les surchiffrements qu'à la suite de doutes sur la sécurité d'un dictionnaire depuis trop longtemps en service dont des exemplaires ont disparu, et qu'on ne peut remplacer. Beaucoup de chiffreurs considèrent d'ailleurs qu'un surchiffrement sur un dictionnaire même connu des décrypteurs assure une sécurité suffisante. C'est notre avis, sauf accident ou faute comme celle que nous venons de montrer ou comme celles de l'exemple suivant, et on peut y parer avec un personnel idoine et attentif et un jeu de clefs ou de procédés un peu étendu.

Deuxième exemple. — On a intercepté les télégrammes suivants :

1er mai. — X à Y — 485 — 9 groupes 05690 53285 79442 87110 30169 27539 90224 84389 8592

2 mai. — X à Y — 485 — 9 groupes — 05690 99355 82354 49717 82103 01729 60224 24389 8592

Un examen trop superficiel des premiers et derniers groupes peut laisser croire à une simple répétition, comme on en voit constamment passer par T. S. F. Un examen plus attentif révèle de grosses différences dans le texte. Le 2e groupe du télégramme 1,53285, se trouve retourné dans le 2e, 58235, puis 7944 donne 4497, etc... Le début du 2e groupe du télégramme se retrouve dans le 1er, renversé, 5399, et la fin des deux textes est la même.

Le chiffreur du 1er télégramme s'est trompé en transformant la clef littérale en clef numérique, pour un tableau de transposition où les colonnes sont relevées alternativement de haut en bas et de bas en haut. Le correspondant n'a pu traduire et a demandé répétition et on a

relevé le même tableau sans faire d'erreurs cette fois-ci sur l'ordre des colonnes. La colonne relevée la première fois comme 2e, de bas en haut, l'a été alors comme 3e et de haut en bas. L'erreur n'a commencé qu'à la 2e colonne et a cessé à 0224.

Nous avons alors, sans ambiguïté possible, la composition et la longueur de la 1re colonne relevée et des 6 suivantes, dont 3 de 5 chiffres et 4 de 4. Dans les 3 dernières, il en est 1 de 5 et 2 de 4; nous ne pouvons pas faire la répartition.

Ce renseignement, à lui seul, n'est pas suffisant pour permettre la traduction. Il donne du moins une information de premier ordre sur le système employé, sur la longueur de la clef, et sur la constitution des lignes du tableau.

Nous arrêterons ici ce chapitre. Nous désirons, dans cet ouvrage, nous en tenir aux notions générales. Dans les questions de codes, et surtout de codes employés avec surchiffrement, la limite est difficile à établir entre les notions générales et les applications, étant donné l'étendue du domaine dans lequel le chiffreur peut choisir le code et le surchiffrement, la part de l'arbitraire, le nombre des représentations des éléments de départ (100.000 groupes de 5 chiffres par exemple, parmi lesquels N groupes peuvent représenter un même mot, et qui, pour un code à bâtons rompus, peuvent être tirés au sort), et la possibilité pour lui, avec des clefs indéfinies, de n'admettre de loi ni pour le dictionnaire, ni pour le surchiffrement. Les notions générales en cryptographie ont pour but d'apprendre à retrouver des lois : quand il n'y en a pas, c'est à l'exploitation des autres auxiliaires du décrypteur : connaissance des codes du commerce, obtention des autres codes par des procédés extérieurs à la cryptographie, fautes du chiffreur, traductions en clair des cryptogrammes, etc... qu'il est nécessaire de recourir.

CHAPITRE XVI

MACHINES A CHIFFRER

Règlettes, cadrans, etc.

Nous avons déjà eu l'occasion de parler des machines à chiffrer, ou cryptographes, à propos de la règlette de Saint-Cyr, des cadrans, de l'appareil Bazeries, etc... Les appareils de ce genre sont légion; on en a encore breveté en 1919 à Paris, qui ne diffèrent de la règle de Saint-Cyr fabriquée avec deux bandes de papier, sur lesquelles on écrit l'alphabet, que par des détails de matière, de vis de pression, de signes de ponctuation, etc... Il faut, du reste, considérer que souvent les appareils à cadrans, surtout à cadrans multiples donnant des représentations multiples, ne sont que la mise en rond, pour ainsi dire, d'un tableau qu'on écrirait sur une substance malléable et dont on ferait joindre les deux côtés latéraux en maintenant le tableau à plat, et qu'il y a toute une série d'appareils à bagues ou à cylindres qui ne sont que ces mêmes tableaux enroulés sur un mandrin, ou ces cadrans emboutis sur un cône ayant son sommet en leur centre, et dont on emmène ce sommet à l'infini. Le fait de mettre des alphabets sur des bagues, au lieu de les mettre sur les lignes d'un tableau, donne un appareil brevetable, mais n'intéresse pas le décrypteur dans la plupart des cas.

Appareil Wheatstone.

Parmi les appareils à cadran classiques, nous citerons celui de Wheatstone. Il a deux cadrans concentriques fixes : l'un avec alphabet ordonné et un repère, de 27 cases,

l'autre avec alphabet incohérent, de 26 cases. Sur ces cadrans se meuvent deux aiguilles reliées par un système tel que lorsqu'on déplace la grande, la petite se déplace plus lentement et prend du retard. Quand la grande a fait 27 tours, la petite en a fait 26. Les alphabets de ce système à cadran prennent donc un retard l'un par rapport à l'autre. (C'est comme si, dans le tableau de Vigenère, la 1re ligne repère se déplaçait par rapport au tableau, ou qu'après avoir chiffré avec la colonne correspondant à la lettre de la clef, on chiffrait avec la colonne voisine de celle qui correspond à cette lettre de la clef, puis encore avec la voisine, etc..., ce qui revient à changer constamment la clef en remplaçant les lettres de celle-ci par des lettres plus éloignées du début de l'alphabet.) Mais le nombre de lettres du texte qui correspondent à ces 27 tours et par suite à un décolage de *n* lettres de la clef peut être très variable. Il faut presque un tour de B à A, sans chiffrer aucune lettre intermédiaire, tout autant que pour passer de B à A, en chiffrant C D E F... Z. Il n'y a pas de relation entre la modification de la clef et le nombre de lettres du texte. Le système a paru longtemps indéchiffrable; Kerckhoffs a fait observer que le nombre des alphabets différents donnés par l'appareil est limité, et qu'on pouvait traiter les cryptogrammes comme des substitutions à double clef faites sur une clef longue. De plus, en chiffrant par ce procédé des textes connus, on a remarqué qu'en moyenne les 27 tours correspondent à une cinquantaine de lettres. On a reconnu d'autres particularités, par exemple un redoublement dans le cryptogramme correspond à deux lettres du clair qui se suivent, en ordre inverse (BA clair donne après un tour d'aiguille MM), si bien qu'on arrive à retrouver des répétitions de mots (par exemple dans un exemple donné par Wheatstone lui-même, POUND donne lieu aux chiffrements MMCMS et IIXIA : répétitions des I symétriques aux répétitions des M). Finalement on a maintenant des méthodes qui permettent de déchiffrer les messages en Wheatstone, en particulier quand on en a plusieurs de même clef, avec un même point de départ des aiguilles.

Un appareil du même genre, mais sans aiguilles, où la réalisation du retard d'un des alphabets par rapport à l'autre est obtenue par l'inégalité des longueurs des circonférences des deux cadrans, a été proposé par M. Lock. Le cadran intérieur, qui n'a que 26 lettres portant chacune une dent, engrène avec un des 27 crans correspondant aux caractères du cadran extérieur, quand, grâce à une excentration du pivot sur lequel est monté le petit cadran, on fait tourner le point de tangence intérieure des deux circonférences inégales portant les alphabets. L'appareil est robuste et peu encombrant.

Certains appareils à cadran modernes, par exemple celui auquel est relatif le brevet Burg (1908), possèdent des systèmes d'encliquetage mus par des poussoirs, qui règlent les déplacements suivant des clefs et peuvent donner des rotations de 2, 4, 1, 5, 2, 4, 1, 5... lettres (ou toute autre combinaison), etc... Ces appareils sont disposés pour pouvoir donner le déchiffrement comme le chiffrement.

Pour les transpositions, l'examen des brevets déposés à Paris ne nous a pas donné une récolte fructueuse. En dehors de quelques appareils à réglettes, permettant, comme le cryptographe employé dans l'armée française en 1886, de numéroter toutes les cases d'un tableau en plaçant les réglettes « à la clef » et de relever dans cet ordre les lettres du texte à chiffrer écrites sur un tableau analogue, il ne semble pas que cette classe de systèmes ait beaucoup intéressé les inventeurs.

Machines à chiffrer du type machine à écrire.

Nous passerons rapidement sur les appareils des types indiqués plus haut; les cryptologues, avant de se prononcer sur leur valeur, devront les étudier avec soin, car (nous l'avons montré pour le Bazeries, et nous venons de l'indiquer pour le Wheatstone) le nombre théorique des combinaisons possibles pour représenter une lettre ou un mot, est souvent fort éloigné du nombre réel, étant donnée la

construction de l'appareil, et certaines de ces combinaisons présentent des ressemblances qui les font reconnaître et facilitent le décryptement.

Par analogie peut-être avec la désignation de machine à écrire ou à calculer, on appelle plutôt actuellement machines à chiffrer celles qui, possédant un clavier, impriment un cryptogramme quand on frappe les touches suivant le texte clair.

Machines donnant la substitution simple.

Quand on examine les brevets déposés à Paris depuis quelques années à ce sujet, on constate que plusieurs de ces brevets ne se rapportent qu'à des dispositions de détail, destinées à cacher les lettres écrites sur les touches d'une machine à écrire ordinaire, de manière par exemple à écrire une F sur la touche qui s'appelait A et qui donne toujours la lettre A. On a une substitution simple : F du clair donne A du cryptogramme. Un appareil analogue, donnant F sur la feuille de papier quand on frappe A, permet le déchiffrement. Avec des bandes de papier, on peut équiper une machine à écrire quelconque pour obtenir un pareil résultat.

Machines donnant des substitutions doubles.

Certaines machines, par contre, permettent des substitutions doubles.

Un type assez simple (auquel appartient la machine de M. de Medeiros) comprend un dispositif analogue à celui qui dans les machines ordinaires remplace les minuscules par des majuscules. Les touches donnent plusieurs lettres différentes, suivant la hauteur à laquelle on élève, devant le papier, les caractères portés par un même levier. L'appareil semble devoir être combiné de préférence avec une machine où les caractères qui impriment ne sont pas sur des leviers indépendants, mais sur un cylindre imprimeur; son mouvement d'ascension ou de descente suffit alors

pour que l'un ou l'autre des alphabets qui sont gravés autour de ce cylindre, les uns au-dessus des autres, vienne toucher le papier pour imprimer une lettre. En réglant ce mouvement au moyen de cames on a une substitution à double clef, dépendant de la came et de la composition de chaque alphabet. On conçoit qu'on puisse changer la came et le cylindre imprimeur. Le déchiffrement peut être obtenu par un cylindre déchiffrant avec des alphabets convenables.

Dans d'autres machines (auxquelles se rattache l'appareil de Bamberg et Weinhold), le clavier donne le courant électrique dans une touche disposée à la circonférence d'un disque et correspondant à la lettre du clair. En face de ce disque s'en trouve un autre, portant des touches reliées chacune à l'appareil qui fait imprimer une lettre. Les disques sont concentriques et mobiles. Dans une position origine le courant de la touche A ira faire imprimer A; mais si on fait tourner un des disques, le courant de la touche A du clavier ne trouvera plus la touche A de l'impression, mais une autre touche, M par exemple, et c'est M qui sera imprimé quand on frappera A. Si l'on fait constamment tourner les disques d'angles égaux après l'impression d'une lettre, le même appareil sans modification permettra de chiffrer et de déchiffrer.

Une machine brevetée par M. Burg en 1904 donne des substitutions doubles, grâce au procédé suivant. Les caractères destinés au cryptogramme sont placés sur un cylindre ou barillet disposé parallèlement à un autre barillet qui imprime sur une autre feuille de papier le caractère du clair frappé sur la touche. Mais le cylindre cryptographiant peut recevoir une rotation par raport au cylindre écrivant le clair, si bien que c'est une autre lettre que la lettre du clair qui est imprimée par lui. Cette rotation provient d'une crémaillère agissant sur le cylindre, et mise en mouvement soit par un levier mû à la main, avant de frapper une touche, soit, dans un autre modèle, par le mouvement des touches qui s'enfoncent. Les organes intermédiaires comprennent une pièce qui, se déplaçant

plus ou moins, fait plus ou moins monter la crémaillère, et dont le mouvement est limité par des chevilles plantées dans les trous d'un disque qui, pour chaque touche frappée, avance d'un angle constant. Suivant la position de chaque cheville, dont une nouvelle vient se présenter chaque fois que le disque avance, la crémaillère fait alors tourner le barillet d'une, deux, etc. lettres. Le barillet, après l'impression, n'a pas de mouvement rétrograde.

Le décalage de la lettre du cryptogramme par rapport à la lettre du clair dépend donc du total des mouvements de rotation du barillet dus à la crémaillère : le système est alors un système à cadran où la clef réglant les mouvements inégaux du cadran peut avoir une vingtaine de termes (autant que de chevilles sur le disque). On peut changer la position des chevilles sur le disque, et changer ainsi la clef. L'appareil est réversible et donne le déchiffrement grâce à une sorte de marche arrière faisant tourner le barillet en sens inverse de celui qui sert au chiffrement.

M. Burg a compliqué fortement le mécanisme de sa machine à chiffrer dans un brevet de 1908. Si nous avons bien compris la description de ce brevet, la roue des types qui joue le rôle du barillet est d'abord soumise à une rotation analogue à celle de la machine précédente, indépendante de la touche abaissée, réglée par un jeu de chevilles sur un disque, et ne donnant pas lieu après l'impression à un mouvement en arrière, si bien que le cryptogramme qui correspondrait à cette rotation serait celui que donne un système à cadran avec une clef (pouvant être assez longue) pour en régler les déplacements inégaux. Mais ce n'est pas ce cryptogramme que la machine imprime. Lorsque la roue des types a fait le premier mouvement dont nous venons de parler, elle reçoit une 2e rotation dépendant cette fois de la touche frappée, mais qui, après l'impression, est annulée par une rotation égale en sens contraire. Le procédé pour obtenir ce deuxième mouvement est assez compliqué; nous ne le dépeindrons pas. Nous dirons seulement que l'amplitude de la rotation dépend d'abord de l'enfoncement de la touche. On peut arrêter celle-ci en dessous à une hauteur qu'on règle au moyen d'un

double jeu de barres à encoches donnant des combinaisons variables, si bien que chaque touche peut descendre plus ou moins suivant la position de ces barreaux à encoche. Les touches sont rangées sur 7 rangs de 8 : dans chaque rang on peut avoir au moyen des barres des combinaisons différentes (au nombre de 16), pour choisir entre les 8 touches celle qui s'enfoncera le plus, celle qui s'enfoncera le moins, et les intermédiaires. De plus, grâce à des leviers dont on peut faire varier la longueur, les enfoncements des touches d'une même rangée sont plus ou moins amplifiés avant de se transmettre à la roue des types. On a donc de très nombreuses combinaisons (touches s'enfonçant peu ou beaucoup avec grande ou avec petite amplification) à désigner par des numéros portés sur les index des 14 barres à encoche (8 positions pour chacune) et des 7 leviers qui peuvent agir chacune de huit manières différentes, et elles ont pour résultat de faire varier suivant le réglage de la machine le décalage supplémentaire qu'on imprime à la roue des types quand on frappe une lettre donnée.

Il semble donc que le secret soit beaucoup mieux assuré que dans la première machine de Burg. Toutefois il serait nécessaire d'examiner le travail de la machine, et de comparer des textes avec leur traduction pour être absolument fixé à cet égard.

Un brevet déposé par M. Fuller dépeint une machine fort ingénieuse au point de vue mécanique, fort compliquée comme description et comme dessins, et dont l'auteur, à la huitième page de sa longue description, fait connaître « qu'on peut employer un très grand nombre de combinaisons ou codes avec une machine du genre de celle qui fait l'objet de la présente invention, et qu'il est pratiquement impossible de déchiffrer les messages les plus simples, étant donné qu'au cours d'un message, une lettre chiffrée quelconque représentative d'une lettre en clair peut ne jamais servir à nouveau pour représenter la même lettre dans le même message ». Faisant toute réserve sur la façon dont nous avons compris la description, car nous

n'avons pas vu l'appareil lui-même, nous exposerons le fonctionnement d'une machine que nous concevons analogue à l'appareil en question, pour montrer encore comment on peut, avec nos notions de cryptographie, chercher à classer le travail d'une machine dans un des procédés connus.

La machine a, dans ses lignes générales, l'aspect d'une machine à écrire. Quand on frappe une lettre du clavier, on détermine, par une série de transmissions, le mouvement d'un organe ou sélecteur, qui déclenche la lettre à imprimer, différente de celle que l'on a frappée. Pour comprendre le mouvement du sélecteur, imaginons un écrou fictif se déplaçant le long d'une vis, et décrivant, parallèlement à l'axe de la vis, des espaces proportionnels à la rotation de cette vis. Cet écrou se déplacerait en face des leviers des lettres à imprimer, et sa position déterminerait la lettre qui s'imprime. Or, quand on frappe une lettre du clavier, on fait tourner la vis d'une quantité donnée, différente d'une lettre à l'autre, et on fait par suite avancer l'écrou d'une quantité donnée caractéristique de chaque lettre, le déplacement conduisant cet écrou 1, 2, 3, 4 lettres plus loin qu'il n'était. Ce déplacement a lieu dans le sens de Z vers A. Nous avons supposé un écrou matériel dans cette exposition. Dans la réalité, le pas de vis existe seul, sous forme d'une sorte de rampe hélicoïdale et l'écrou fictif rentre en action à un bout de la vis dès qu'il a dépassé le dernier levier de lettre à l'autre bout.

Les mouvements de la vis peuvent être suivis par l'opérateur sur un cadran qu'elle entraîne et qui tourne en face d'un repère, et on peut agir directement sur elle à l'aide d'un volant pour la placer dans une position quelconque, sans préjudice de son mouvement automatique d'entraînement lorsqu'on appuie sur une touche du clavier, et qu'on embraye ainsi toute la machine avec un petit moteur. Supposons que la touche A donne au sélecteur un déplacement nul, que B le déplace d'une lettre, C de 2, D de 3, etc... et qu'à l'aide du volant nous mettions, au début de l'opération, le sélecteur à A. Frappons une touche, B par exemple. Le sélecteur recule de 1, et dé-

clenche le levier de la lettre qui correspond à A — 1, soit Z. Frappons maintenant E; le sélecteur recule de 4 et donne Z — 4 = V. Frappons encore E; le sélecteur recule de 4 et frappe V — 4 = R, etc... Le cractère imprimé dépend donc de la position du sélecteur après le chiffrement de la lettre précédente et de la lettre du clair frappée. Nous obtenons un cryptogramme autoclave où le cryptogramme lui-même sert de clef, après que la clef de convention d'une seule lettre qui indique la position initiale du sélecteur a permis de chiffrer la première lettre du texte.

Les correspondants ayant une machine de même construction, où les lettres du clavier ont la même influence sur le sélecteur, c'est-à-dire dont l'alphabet de substitution est le même, disposent comme clef de la position initiale du sélecteur, indiquée par la coïncidence de cette même lettre sur le cadran avec un repère fixe. Un 2e cadran peut, dans le but annoncé d'augmenter le nombre des combinaisons, être intercalé entre le cadran relié au sélecteur et le repère, et, au lieu d'indiquer directement la position du sélecteur en face d'une lettre par la coïncidence de cette lettre et du repère, on peut indiquer la coïncidence de lettres des deux cadrans entre elles et la position du 2e cadran par rapport au repère.

Si l'on se reporte à ce que nous avons dit au sujet des autoclaves du genre de ceux que fournit la machine, on verra que, si l'on connaît l'alphabet, la clef n'a aucune importance sur le déchiffrement.

Le cryptogramme Z V R... a été obtenu au moyen de la clef ? Z V R.

On écrit : Clef. . . . . ? Z V R
Cryptogramme. . . . . Z V R ...

Quelle est la lettre qui correspond à V dans l'alphabet Z? c'est E; celle qui correspond à R dans l'alphabet V? c'est E. Quant à la première lettre, on la devi..e d'après le contexte.

Le déchiffrement avec la machine est un peu plus compliqué que le chiffrement. Au chiffrement, on n'a qu'à frapper successivement les touches du clavier. Au déchif-

frement, il faut ramener chaque lettre au repère du cadran avant de frapper celle qui la suit. Partant de la clef disposée comme au chiffrement, on frappe Z. Le sélecteur qui était à A recule de 25 et donne B. On ramène le sélecteur à Z et on frappe V; le sélecteur recule de 21 et donne E; on ramène le sélecteur à V, en mettant V au repère du cadran; on frappe R. Le sélecteur recule de 17 et donne E, etc...

Comme nous venons de le dire, si le décrypteur connaît l'alphabet, il n'a pas besoin de savoir comment le sélecteur était placé au début, c'est-à-dire quelle est la lettre clef employée pour le cryptogramme. Or, il peut connaître cet alphabet, par exemple au moyen d'un texte clair qui permettra de le reconstituer, texte qui peut se réduire à l'impression de l'alphabet des touches de la machine. Les erreurs de dactylographie, peut-être insuffisamment appréciées par le personnel non idoine à qui l'on peut confier la machine en raison de la simplicité d'emploi, et pouvant donner lieu à des répétitions de télégrammes, serviront les efforts du décrypteur. Mais, sans même recourir à ces secours, celui-ci remarquera que toute lettre du cryptogramme est chiffrée avec un alphabet dont l'indicatif est connu (la lettre précédente). Il réunira toutes les lettres chiffrées avec un même alphabet, c'est-à-dire toutes celles qui suivent une lettre donnée A, B, M, etc... du cryptogramme; elles proviennent d'un même alphabet, et on emploiera alors les considérations de fréquences, de séquences et de symétrie de position pour reconstituer l'alphabet de base.

La machine, semblable ou non à celle du brevet Fuller, dont nous avons exposé le fonctionnement, ne semble pas devoir donner de cryptogrammes « pratiquement indéchiffrables ». Peut-être pourrait-on augmenter le secret en changeant fréquemment l'alphabet. Il ne semble pas qu'il soit facilement possible de changer la combinaison qui relie le levier d'une touche de clavier au sélecteur, mais peut-être pourrait-on faire des substitutions entre les lettres figurant sur les touches du clavier. Avec des textes longs, cette précaution ne serait pas encore bien efficiente.

Un brevet obtenu en 1920 par M. Hugo Koch correspondrait, si nos renseignements sont exacts, à une machine vendue sous le nom d'« Enigma », de fabrication allemande.

L'application du principe du brevet, que nous exposerons ci-après, conduit à une machine donnant la substitution, à une autre donnant la transposition, à une troisième donnant la superposition des deux systèmes.

Qu'on imagine, sur un plateau fixe, 10 plots électriques correspondant à une machine à écrire à 10 touches (les nombres de 0 à 9 par exemple) — (la description serait analogue pour N signes alphabétiques au lieu de 10). Supposons que ces plots soit disposés sur un cercle et à égale distance l'un de l'autre. A un certain intervalle, en face de ce plateau, mettons un autre plateau analogue, où les plots sont reliés à l'appareil imprimeur. Dans l'intervalle des deux plateaux un disque creux porte sur chaque face 10 contacts, pouvant respectivement s'appliquer sur les 10 plots du plateau « touches » et les 10 du plateau « caractères ». Chaque contact d'une face est relié, de façon absolument arbitraire, à un contact de l'autre face et à un seul.

Si en abaissant la touche 1 nous envoyons le courant, il ira par exemple du plot 1 à un contact relié au contact qui touche le plot 7 du plateau « caractères » et on imprimera 7. Jusqu'ici nous n'avons qu'une substitution simple.

Mais si nous faisons tourner le disque creux, le contact du disque côté plateau « touches » qui viendra en face du plot de la touche 1 ne communiquera peut-être plus avec un contact qui se trouvera en face du plot 7 du plateau « caractères ». Si les fils sont convenablement entre-croisés dans le disque creux, au lieu d'avoir 7 on aura par exemple 5, et, si le disque avançait d'un cran chaque fois que l'on abaisse une touche, on aurait une substitution à double clef avec période de 10.

On conçoit qu'on peut déplacer le disque de façon irrégulière : on a alors une substitution double à type cadran avec alphabet incohérent (on peut dans cet ordre d'idées le laisser immobile pour plusieurs lettres). On sait que la

longueur de la période de la clef est alors de 10 (ou 26 pour 26 lettres) déplacements égaux, dont chacun peut-être formé de plusieurs déplacements inégaux correspondant chacun à la frappe d'une touche (si le disque se déplace pour chaque frappe), ce qui peut faire une période très longue.

A la place du plateau « caractères », supposons un plateau fixe tel que ses plots traversent de part en part la matière isolante, et que le plateau présente 10 plots sur chaque face, se correspondant exactement. Intercalons entre ce plateau et le plateau « caractères », éloigné à cet effet, un 2e disque creux et tournant où les contacts d'un côté sont reliés arbitrairement à ceux de l'autre.

Si les deux disques restaient immobiles, nous superposerions deux substitutions simples, une du plateau « touches » au plateau intermédiaire, une du plateau intermédiaire au plateau « caractères », et nous n'aurions qu'une substitution simple.

Si les deux disques tournaient avec la même vitesse et la même loi et dans le même sens, le deuxième ne ferait qu'ajouter au résultat du premier une substitution simple. On aurait les résultats de substitution type cadran dont nous avons parlé plus haut.

Mais si les deux disques tournent suivant des lois différentes, on a la superposition de deux substitutions à cadran, ce qui donne une période égale au plus petit commun multiple des périodes de clef de chaque cadran. Comme on peut multiplier le nombre des disques, on voit qu'en superposant le nombre des substitutions type cadran, on peut arriver à une période pratiquement plus longue qu'aucun cryptogramme.

Nous n'insisterons pas sur les dispositions mécaniques permettant de faire tourner les divers disques suivant des lois différentes, des cames ou des roues à engrenages produisant des avancements par sauts, égaux à un ou plusieurs intervalles de contacts, de manière qu'un contact soit toujours en connexion avec les plots des plateaux, et que le courant puisse toujours passer d'une touche à l'appareil moteur de l'impression. L'inventeur d'ailleurs

décrit son appareil non pas avec fonctionnement électrique, mais avec fonctionnement pneumatique, mais le principe est le même. Les plateaux intermédiaires fixes entre les disques mobiles sont du reste supprimés dans la machine et les disques se touchent contact à contact, donnant les combinaisons multiples.

Des repères indiquant les positions origines des disques mobiles permettent, avec des appareils semblables, de mettre à la clef pour commencer le chiffrement. On peut changer facilement les disques et les cames si l'on craint qu'un indiscret n'ait un appareil qui permette de déchiffrer.

Un renversement de sens du courant permet de revenir du cryptogramme au clair; on prend toutes les transformations « à rebours » en partant de la lettre du cryptogramme.

Telle est la disposition pour la substitution. Elle semble *a priori*, et sous réserve d'examen de l'appareil, constituer un système très sûr.

Pour la transposition, imaginons d'abord un appareil placé au bord d'une feuille de papier fixe, et comprenant une série de styles parallèles, également écartés (ou par groupes de 5), s'avançant alternativement sur le papier dans un ordre quelconque, dans l'unique but de montrer à quel point du papier nous écrivons une lettre du texte. Si, par exemple, nous supposons ces styles numérotés de 1 à 10 et de gauche à droite, et que le style 7 s'avance le premier sur la feuille de papier, nous écrirons en face du point ainsi marqué la première lettre du clair; 7 se retire et 3 s'avance; nous écrivons en face de 3 la deuxième lettre du clair, etc... L'ordre des mouvements des 10 styles nous donnera donc une clef de 10 chiffres pour écrire les 10 premières lettres du texte. Or, avec une seule touche, envoyant le courant dans un seul plot d'un plateau « touche », relié par les connexions d'un disque mobile à un quelconque des 10 plots d'un plateau « styles », nous ferons manœuvrer les 10 styles dans un ordre dépendant de ces connexions. S'il n'y a qu'un disque, on reprendra

la même série pour les 10 lettres suivantes, mais s'il y en a plusieurs comme dans l'appareil précédent, on aura une série nouvelle, et la période pourra être fort longue. On met à la clef de départ au moyen des indications portées sur les disques et des repères. Mais l'auteur, dans son brevet, ne dit pas ce qui se passe quand, dans la même série, le même style est mis en mouvement plusieurs fois, ce qui ne semble pas impossible.

La même objection se présente quand on passe à la machine qui superpose la substitution et la transposition. Elle comprend deux mécanismes juxtaposés; chaque fois que l'on appuie sur une touche on actionne d'une part le mécanisme de substitution de la touche, de l'autre le mécanisme à un seul plot de la transposition. Les lettres sont portées par un barillet, et le mécanisme imprimant fait tourner le barillet d'un angle à partir du zéro, correspondant au caractère à imprimer (celui du cryptogramme), le barillet retombe au zéro après chaque impression, si bien que le caractère précédent n'influe pas sur le chiffrement d'un nouveau caractère. Ce barillet se déplace le long de son axe, et, lorsque le caractère va être imprimé, part d'une extrémité de cet axe et court devant le papier jusqu'au moment où il est arrêté par un des styles dont nous avons parlé, ce qui place la lettre pour la transposition. Le papier vient alors s'appliquer sur le caractère, puis s'en écarte et le barillet retourne au bout de l'axe. Quand une ligne, correspondant au nombre des styles, est imprimée, le papier se déplace pour présenter une autre ligne au barillet.

Tel est ce cryptographe qui, *a priori*, nous semble extrêmement sûr au point de vue cryptographique. Nous ne croyons pas que la machine soit actuellement réalisée avec une transposition. Elle donnera déjà suffisamment de travail, d'ailleurs, aux cryptologues, avec ses substitutions, surtout si, ne possédant pas l'appareil tel que le chiffreur l'emploie, ils n'ont pas seulement à retrouver la clef et les positions origines, mais les différents alphabets de substitution.

La machine brevetée par la Patent Developping Company fonctionne, avec un mécanisme différent, d'après le même principe que la machine de substitution de M. Hugo Koch, dont le brevet est antérieur. Là encore, un disque creux contient des connexions électriques réunissant de manière variable le plot où aboutit le courant venant de la touche au plot relié à l'appareil moteur du levier de la lettre. D'après la description du brevet, assez confuse, il nous semble que la roue ne se déplace que d'un mouvement régulier, et le croquis ne présente qu'une roue. Dans ce cas, nous n'aurions qu'un système avec cadrans à alphabets intervertis, ce qui donne des problèmes difficiles à résoudre, mais moins complexes que ne paraissent ceux de M. Koch. Le brevet prévoit d'ailleurs l'emploi de plusieurs disques.

Pour faciliter le déchiffrement, les connexions et les alphabets sont établis de telle sorte qu'on a des alphabets réciproques; si H se transforme en C pour une position du disque, C se transforme en H pour la même position. Pour déchiffrer, on n'a donc qu'à traiter le cryptogramme comme on a traité le clair, et chaque lettre du cryptogramme se transforme en lettre du clair.

Le disque creux est facile à enlever, pour le changer, ou, au besoin, pour partir d'une position initiale.

Le brevet pris par M. Henkels en 1922 (allemand) concerne un appareil de chiffrement qui n'imprime pas, mais fait seulement apparaître les lettres du cryptogramme qu'on doit copier d'autre part.

Cet appareil comprend un certain nombre de dispositifs analogues juxtaposés. Nous en décrirons d'abord un seul : une série d'axes portant dans un même plan perpendiculaire à ces axes des disques où sont figurées les lettres de l'alphabet, de préférence dans l'ordre normal pour faciliter les mises à la clef et les mises au clair dont nous parlerons plus loin. Ces disques sont fous sur les axes; ils portent à leur circonférence deux dentures juxtaposées; l'une, menée par un pignon intermédiaire entre le disque considéré et le disque précédent, a des dents

sur toute sa circonférence; — l'autre, menant par l'intermédiaire d'un pignon le disque suivant, a des interruptions de manière qu'en raison de ces interruptions on obtienne pour 3 disques successifs, qui s'entraînent réciproquement, des rotations fort différentes, se composant de successions de mouvement et d'immobilité. Si le premier disque fait tourner le second d'une dent par lettre pour les 15 premières lettres, puis le laisse immobile pour les 11 dernières, le passage de ces 15 premières lettres devant un repère correspondra pour le deuxième disque à des décalages successifs de 1 à 15 lettres, à partir d'une position origine, et à partir de ce moment le décalage ne se modifiera pas jusqu'à ce que la première roue, ayant fait un tour complet, se remette en prise et que sa première dent amène un décalage de 16, etc... La troisième roue subira les déplacements de la deuxième modifiés par les vides de la denture menante de celle-ci, etc...

Nous avons dit que les disques étaient mobiles sur les axes, mais que tout le système était entraîné à la fois par les pignons qui transmettent le mouvement d'un disque au suivant. Poussons tous ces pignons de côté de façon à ce qu'ils ne soient plus en face des disques; nous rompons la solidarité, et chaque disque pourra tourner librement. Plaçons alors le disque 1 de manière qu'une certaine lettre choisie (une lettre de la clef) soit en face d'un repère; puis, plaçons le disque 2 de manière qu'une autre lettre, par exemple la première du clair, soit en face du repère de disque; puis, plaçons le disque 3 en mettant une autre lettre du clair (la 11e par exemple) au repère, etc... Ramenons les pignons en prise, puis, au moyen d'une roue à engrenage menant le disque 1, et dont la manivelle se déplace devant un repère circulaire, faisons tourner la série des disques solidaires. Convenons de faire faire à la manivelle, par exemple, un tour et 2/26e. Le premier disque, par hypothèse, exécutera une rotation égale, et 28 lettres passeront devant le repère. Le deuxième tournera d'abord, puis restera immobile pour un arc du disque 1 correspondant à 11 lettres, puis repartira (en supposant qu'on n'ait pas commencé par une période de

vide, on aura un déplacement de 17 lettres au plus), etc... Chaque lettre sera remplacée par une autre lettre de l'alphabet devant le repère du disque correspondant, et ce seront ces lettres qu'on écrira dans le cryptogramme.

L'appareil complet est composé d'un certain nombre (10 par exemple) de systèmes analogues juxtaposés côte à côte, les déplacements des 10 disques d'un même arbre pouvant être tout à fait différents, puisque ce ne sont pas les arbres qui tournent, mais seulement les disques menés par leurs camarades de la même série perpendiculaire aux axes. Les repères sont constitués par des fenêtres pratiquées dans la boite qui contient le mécanisme, et l'on voit les lettres à travers ces fenêtres.

Les mouvements des disques pour les mises à la clef ou au texte clair, se font au moyen d'un poussoir à cliquet pour chaque disque, poussoirs qui hérissent le couvercle de la boîte.

De quoi dépend chaque lettre du crpytogramme? De la lettre initiale au repère du disque et de la rotation du disque. Or, le disque est mené par le disque précédent, mais avec des intervalles de prise et de lâchage. La position initiale respective des 2 disques intervient donc : si on ne déplace le disque précédent que de 3 lettres par exemple et que la lettre au repère de ce disque soit telle qu'à ce moment le pignon intermédiaire n'est pas mené pour un déplacement de 3 lettres, la lettre du disque considéré n'est pas modifiée. Au contraire, si le pignon est en prise, elle sera remplacée par celle qui la suit à trois intervalles; les cas intermédiaires sont possibles si le pignon est à la limite d'une partie dentée et d'une partie lisse. Puisque la transformation d'une lettre dépend de celles qui la précèdent, on fixe le point de départ en convenant d'un mot clef qu'on met au repère sur les premiers disques. La connaissance de ce mot clef et celle de la valeur de la rotation donnent le moyen de traduire le cryptogramme; on met les premiers disques à la clef et la manivelle à l'origine, on tourne la manivelle comme convenu, les autres disques étant débrayés; on forme le cryptogramme en en mettant les lettres au repère, on tourne

la manivelle en sens inverse — les engrenages fonctionnent en sens inverse de celui du chiffrement et déplacent les disques de quantités égales, et le clair réapparaît.

On coupe le clair par tranches égales au nombre des disques chiffrants, soit 40 disques, montés par 10 sur chaque axe, et un axe de plus pour la clef de 10 lettres.

Les 10 premières lettres, en admettant qu'on revienne à la clef pour chaque tranche, sans se servir d'une clef de plus de lettres qu'il n'y a de disques juxtaposés, et qu'on tourne toujours la manivelle de la même manière, ne dépendront que du mot clef. La rotation de chaque disque du premier axe des disques chiffrants sera toujours la même, et la substitution sera alors une substitution double du système Vigenère.

Pour les disques du deuxième axe chiffrants, l'amplitude de la rotation dépendra de la position initiale du disque précédent, et de la rotation que ce dernier disque reçoit lui-même du disque de la clef. Il y aura toute une partie de la rotation de la manivelle qui ne donnera aucune rotation à ce deuxième disque, soit parce que le disque de la clef n'engrènera pas avec le premier disque, soit parce que ce premier n'engrènera pas avec le deuxième. Cette particularité va en s'accroissant de disque en disque, et exige, pour que les lettres du dernier disque soient sûrement modifiées, que la rotation de la manivelle soit assez considérable. Mais la répercussion de l'influence des positions initiales des disques précédents paraît de nature à compliquer singulièrement la loi de représentation des lettres des derniers disques. En l'absence de textes établis avec la machine, et de la possession de la machine elle-même pour l'étudier, nous ne voyons comme procédé de déchiffrement qu'une recherche portant sur les commencements de télégrammes de même clef (ou les commencements des tranches quand on en connaît la longueur), chiffrés par le procédé Vigenère.

Une fois la première tranche trouvée, si l'on a assez de textes, on pourra faire un tri pour réunir les lettres des deuxièmes tranches chiffrées avec un même disque et une même lettre de la première tranche, et qui par consé-

quent proviennent d'une rotation égale; on pourra faire en même temps des essais sur les lettres du même disque chiffrées avec les lettres alphabétiquement voisines dans la première tranche, car, sauf au cas où l'on se trouvera sur la limite d'un secteur denté et d'un secteur lisse de l'engrenage, le décalage sera le même. Ces procédés, toutefois, ne semblent pas très pratiques, et, sur la simple description du brevet, nous estimons que les chiffrements obtenus par l'appareil seront de nature à donner du fil à retordre aux indiscrets.

Nous mentionnerons maintenant les machines construites par Aktiebolaget-Cryptograph de Stockholm, qui se rattachent, d'après leurs différents types, à plusieurs principes brevetés.

M. Damm a appliqué l'un de ces principes à plusieurs machines de formes différentes, décrites dans un brevet de 1915.

Figurons-nous un alphabet où nous lisons la lettre du clair, et, en face de lui, un tableau de n alphabets décalés d'une lettre l'un par rapport à l'autre (une tranche verticale de n colonnes d'un tableau carré « Vigenère » ou analogue). Chaque lettre du clair peut être représentée par une quelconque des n lettres qui se trouvent sur la même ligne. Pour chiffrer, nous amènerons en face d'un repère la lettre du clair et, par suite, la ligne du tableau correspondante. Devant ce tableau, supposons un écran quadrillé de manière que chaque carreau couvre une lettre du tableau, un *seul* carreau étant ouvert *à chaque ligne* de manière à former une fenêtre qui laisse lire une lettre de la ligne; c'est cette lettre qu'on substituera à la lettre du clair. (Le quadrillage n'existe pas; nous l'avons introduit pour faire comprendre la disposition des fenêtres.) Suivant les mouvements d'élévation ou d'abaissement qu'on communiquera à cet écran, devant le repère où nous avons amené la lettre du clair, la place de l'ouverture correspondant à la ligne de cette lettre variera, et la lettre à substituer sera modifiée en conséquence. Si l'écran était indéfini et si les trous s'y plaçaient dans le même

ordre, après une période de n déplacements dans le même sens, on aurait une substitution à double clef, la 1re, la n + 1, la 2n + 1, etc... lettres étant lues par la même fenêtre, et par conséquent dans le même alphabet, etc...

Tel est le principe. Les réalisations sont faites avec des cylindres ou avec des disques. Pour le type cylindrique par exemple, considérons le tableau ci-dessus enroulé autour d'un mandrin et passant devant une barre, fixée au bâti, où est pratiquée une fente qui sert de repère. L'écran a une longueur totale plus grande que la longueur de la circonférence du cylindre tableau; à plat, tandis que le tableau aurait 26 lettres, l'écran aurait par exemple la hauteur d'une trentaine de carreaux. Une fois ses extrémités agrafées ensemble fictivement, il enveloppe donc le cylindre tableau, mais sans garder le contact avec lui. Si le cylindre entraînait directement l'écran avec la même vitesse, on aurait un appareil du genre des cadrans de Wheatstone (où l'un des alphabets prend du retard par rapport à l'autre à chaque passage au repère), la succession des alphabets étant réglée par une loi où entrerait le nombre de lettres séparant deux lettres successives du clair, et la période totale serait, sauf erreur, le produit de la longueur de la circonférence du cylindre par la longueur du cadran, mesurées en nombre de lettres. Mais l'écran est entraîné par un système de roues à cliquets, qui le font mouvoir dans un sens ou dans l'autre suivant les indications d'une chaîne-clef caractéristique du système. Cette chaîne présente des maillons d'une longueur égale, mais de deux épaisseurs différentes, glissant sur un guide sous l'extrémité d'une tige. Les maillons minces laissent cette tige descendre, ce qui embraye l'écran avec une roue tournant dans le sens direct; les maillons épais font lever la tige, et l'embrayage de l'écran se produit alors avec une roue tournant en sens inverse. On peut facilement composer la chaîne-clef en agrafant l'un à l'autre les maillons épais ou minces et la mettre sur la machine; la convention pour les correspondants est donnée par un nombre ou un mot indiquant la succession des maillons. Remarquons d'ailleurs que l'écran formant

une surface continue, on peut obtenir, par une rotation directe égale à sa longueur moins n lettres, le même résultat que par une rotation inverse de n lettres. Par suite, il semble que l'écran reprendra sa position primitive au bout d'une période égale au produit du nombre de maillons de la chaîne par le nombre de fenêtres, et comme cette période peut ne pas coïncider avec une fin de période du cylindre, il faudra encore multiplier le résultat par 26 pour avoir la longueur de la clef du cryptogramme (sous réserve de facteurs réduisant ce résultat).

Dans un autre dispositif, les alphabets du tableau sont tracés sur les rayons d'un disque. L'alphabet du clair est à la périphérie de ce dernier, et les fenêtres sont placées dans un autre disque écran plus petit, qui se superpose à une partie du disque tableau, et qui jouit de mouvements dans les deux sens suivant les indications d'une chaîne-clef. La fente repère se place sur le rayon commun des deux disques.

En ce qui concerne ces deux modèles, les mouvements de l'alphabet du clair et du tableau sont bien liés entre eux, mais c'est une manivelle spéciale qui fait avancer la chaîne-clef et commande par des transmissions les mouvements de l'écran. On pourrait donc à la rigueur, semble-t-il, régler comme clef superposée au système, les mouvements de cette manivelle; on n'en parle d'ailleurs pas dans le brevet.

Dans un troisième type, nous arrivons à l'aspect extérieur d'une machine à écrire, avec des touches. Chacune de ces touches est placée en face d'un alphabet écrit sur la circonférence d'un cylindre; l'ensemble des alphabets, dont chacun est décalé d'une lettre par rapport à son voisin, formant un tableau carré enroulé. Le cylindre lui-même est soumis à des mouvements de rotation en avant ou en arrière suivant la forme des maillons de la chaîne-clef. Chaque enfoncement d'une touche quelconque fait avancer la chaîne d'un cran. On lit la lettre du cryptogramme sur la fente repère, en face de la touche qui manœuvre, en s'enfonçant, un petit volet découvrant la partie intéressante de la fente. Par conséquent, main-

tenant, le mouvement de la chaîne est solidaire du nombre des lettres; on a, nous semble-t-il en considérant un des alphabets du cylindre, le même mouvement qu'avec un appareil à cadrans qui avance par saccades irrégulières chaque fois qu'on a chiffré une lettre. Les alphabets des cadrans fictifs seraient respectivement celui du tableau et celui de la suite des touches dans l'ordre des fenêtres. Nous avons, grâce à la chaîne-clef, une période plus longue que celle qu'il serait pratique d'employer avec un cadran à main, mais nous n'avons plus la sécurité que donnaient la différence de période entre la rotation d'un cadran extérieur de plus de 26 cases et d'un cadran intérieur de 26 cases (écran et disque ou cylindre), et l'irrégularité de la position des fenêtres.

C'est ce même appareil qui devient imprimeur grâce à l'introduction de l'électricité. Suivant les diagonales de notre tableau, où figure la même lettre dans chaque ligne et dans chaque colonne, plaçons sur chaque représentation de cette lettre un plot et réunissons tous ces plots par un même fil conduisant le courant à l'appareil qui fera fonctionner le levier imprimant cette lettre. Organisons de même nos 26 lettres. Quand nous appuyons sur la touche de la lettre du clair, au lieu d'ouvrir la fenêtre par où nous lisions la lettre du cryptogramme sur le cylindre dans le modèle précédent, nous abaissons un contact qui amène le courant à un des plots dont nous venons de parler; la frappe de la touche donnera lieu à l'impression de la lettre que nous lisions tout à l'heure. Le cylindre à plots aura toujours son mouvement en avant ou en arrière réglé par la chaîne-clef.

Signalons en passant que la chaîne-clef a encore été utilisée dans un cryptographe de poche, où les déplacements d'une règle portant les 26 lettres et la fenêtre de lecture sont transmis par une cordelette au pignon d'entraînement de la chaîne-clef et du cylindre portant le tableau qui tourne dans un sens ou dans l'autre; on tire la réglette à fond avant chaque lecture pour faire avancer la chaîne-clef d'un maillon. Les mouvements du cylindre tableau sont donc, comme dans les derniers types, direc-

tement liés au nombre de lettres du texte, et on a au fond, nous semble-t-il, un système à cadran.

Les prospectus d'Aktiebolaget-Cryptograph donnent à penser que, si le principe de la chaîne à maillons est resté le même, des modifications de détail ont été apportées au dispositif. L'appareil mis en vente en 1922 est à touches et imprime sur trois bandes le clair et deux exemplaires du chiffre. Les dessins font apparaître une série de 25 disques, portant chacun en relief à sa périphérie un secteur d'un 25e de la circonférence où figure une lettre, ce qui permet, en enfilant ces disques sur un axe dans un ordre choisi, d'avoir l'équivalent du tableau, mais facile à modifier grâce à la modification de l'alphabet de ce tableau par un nouveau mélange arbitraire des lettres. On arrive alors à des nombres de combinaisons possibles pour qu'une machine diffère d'une autre, avec ces alphabets et ces maillons de chaîne (dont on peut faire varier le nombre total et la disposition) de l'ordre des décillons. Enfin, le mouvement périodique automatique semble, d'après le prospectus, pouvoir être brisé à la volonté du chiffreur, ce qui, lorsqu'on commence des textes avec la même chaîne-clef et la même position initiale des éléments, permettrait de modifier la période dès le début.

L'appareil porte des repères, correspondant sans doute aux indications de position des éléments de départ. Il sert à chiffrer et à déchiffrer, sans que des indications précises soient données dans la description au sujet du déchiffrement.

La même firme suédoise a fait breveter en 1920 une machine où les organes sont mus par l'électricité au moyen d'électro-aimants, mettant en action des cliquets qui font avancer des roues chaque fois que le courant passe et dans ce cas seulement.

Deux disques tournant en sens contraire et entre lesquels sont montés des contacts, établissent la connexion entre les fils reliés au clavier des lettres et les fils reliés aux touches. Chacun d'eux est mû par mécanisme actionné par un courant qui traverse un interrupteur

composé d'une roue établissant ou rompant le contact suivant des dents portées sur sa circonférence (ou des aiguilles plantées dans le disque formant la roue). Cette dernière roue avance d'un angle constant chaque fois que l'on appuie sur une touche. Si donc les dents sont telles que le courant passe, quand on appuie sur une certaine lettre, dans l'un des interrupteurs et non dans l'autre, un seul des disques se déplace. Si le courant passe dans les deux interrupteurs, les deux disques tournent en sens contraire, et leurs déplacements s'ajoutent. Chaque interrupteur donne un mouvement périodique au disque, la période valant au plus un tour de la roue interruptrice. En combinant les périodes des interrupteurs de façon qu'elles ne se terminent point ensemble sauf à de très grands intervalles, en faisant de plus agir l'un d'eux sur un des disques de manière qu'au lieu d'avancer d'une seule lettre à un passage de courant, ce disque avance de plusieurs, on arrivera à imposer aux déplacements relatifs des disques une période fort longue. Si par exemple les roues interruptrices ont 17 et 19 dents, leur période totale sera de $17 \times 19 = 293$ touches frappées, et il faudra encore multiplier ce produit par le nombre commun des lettres des disques pour retrouver le début de la période, si les déplacements ont été bien choisis, et si on ne retombe pas après un nombre de fois 293 déplacements inférieur à 26 sur la position de début des disques.

Les disques correspondent à un même alphabet (qui ne semble pas être l'alphabet normal) en ordre direct sur un des disques, en ordre inverse sur l'autre, la rotation étant réglée de manière qu'un mouvement simultané de 1 de chacun des disques donne à l'impression une lettre distante de 2 de la lettre frappée sur la touche, en la considérant bien entendu dans l'alphabet des disques. On aurait donc ainsi un système à cadran, avec mouvements inégaux, mais périodiques. Le problème posé par la machine est compliqué par l'artifice suivant : quand on frappe une lettre donnée, dite lettre influente, le courant électrique est coupé entre les roues interruptrices et les disques, si bien que, même au cas où les roues, dans leur période

normale, auraient dû donner un déplacement aux disques, ce déplacement ne se produit pas, et les disques restent immobiles. A la frappe suivante, comme les roues interruptrices ont continué à tourner, le déplacement est le même que celui qui se serait produit sans le dispositif dont il s'agit, mais en comparant l'appareil à un système à cadran le cadran chiffrant a pris un retard par rapport au cadran du clair, et des retards de cette nature se produisent d'après la seule présence d'une lettre donnée dans le clair, c'est-à-dire sans loi.

Pour fixer les idées, supposons qu'un des disques soit mené par son interrupteur suivant la période 1 1 0 1 0, — l'autre suivant 2 2 0 0 (nous choisissons pour cet exemple des périodes extrêmement courtes). Il en résultera pour le déplacement de la lettre du chiffre par rapport à celle du clair une période dont chaque terme est obtenu en additionnant le déplacement du premier disque avec celle du second, et qui aura 20 termes (4×5).

1 1 0 1 0 1 1 0 1 0 1 1 0 1 0 1 1 0 1 0
2 2 0 0 2 2 0 0 2 2 0 0 2 2 0 0 2 2 0 0
3 3 0 1 2 3 1 0 3 2 1 1 2 3 0 1 3 2 1 0

Si, au cours d'un texte dont le chiffrement correspond à une telle période, la lettre influente apparaît la 6e et la 9e, on aura (avec des déplacements 0 pour la 6e et la 9e) :

3 3 0 1 2 0 1 0 0 2 1 1 2 3 0 1 3 2 2 0

et tandis que la période pure donnait comme décalages entre la lettre du clair et celle du chiffre (supposées non décalées au début de la période) :

3 6 6 7 9 12 13 13 16 18 19 20 .....

la lettre influente donne

3 6 6 7 9 9 10 10 10 12 13 13 .....

Le chiffrement est donc absolument différent.

Au déchiffrement, qui se fait comme le chiffrement, le frappage du cryptogramme aux touches donnant le clair à l'impression, c'est sur le levier de l'impression de la lettre influente que se produit l'interruption du courant. Cette influence d'une lettre (ou même de plusieurs) vient accroître dans une large mesure la sécurité de l'appareil déjà grande, sauf erreur ou particularités de construction.

On prévoit, pour différencier les machines, des changements de roues interruptrices, permettant de modifier et les périodes et les déplacements élémentaires des disques qui jouent le rôle des cadrans dans les systèmes connus sous cette dernière dénomination.

Il semble que dans la réalisation commerciale actuelle de ce brevet, des modifications ont été apportées. La lettre influente a disparu. Par contre, il y a maintenant quatre signaux repères extérieurs correspondant à des disques interrupteurs à crans (ou aiguilles) touchant ou abandonnant un contact, et un cinquième disque (ou plutôt un ensemble de quatre disques, un pour chacun des précédents) qui coupe le courant ou le rétablit d'après sa période propre, ce qui ôte ou donne de l'influence sur le chiffrement à chacun des quatre premiers disques. On indique, au moyen de 5 lettres des signaux repères, les positions initiales de ces cinq disques.

Quelques autres appareils se donnent comme but la transformation de groupes de chiffres (qui paient au télégraphe une taxe de un mot pour 5 chiffres) en groupes de lettres consonne voyelle ou voyelle consonne, qui ne paient qu'un mot pour 10 lettres. Les uns donnent toujours la même syllabe pour un même groupe, par exemple par un procédé qui fait apparaître ces deux éléments l'un à côté de l'autre dans la fenêtre d'un couvercle. Parmi les autres, il en est un très portatif, qui, au moyen de couronnes concentriques que l'on peut mettre à la clef, remplace un nombre de 5 chiffres par un groupe de 4 lettres grâce à une convention permettant, d'après l'ordre des voyelles et des consonnes, de fixer l'ordre de lecture des nombres

de 2 et de 1 chiffre figurant sur ces couronnes et de former les nombres de 0 à 99999; l'application paraît du reste ne pas briller par la simplicité. Une autre encore comprend, pour les 100 premiers nombres, un tableau de 20 colonnes et 5 lignes, en face desquelles on déplace autour de leur axe des règles portant sur leurs faces des listes différentes des 20 consonnes et des 5 voyelles; la syllabe formée par la voyelle de la ligne et la consonne de la colonne remplace le nombre. La clef se donne au moyen de numéros indiquant les faces des deux règles à employer.

Aktiebolaget-Cryptograph a aussi construit un appareil de cette classe; des combinaisons de 5 voyelles avec les 10 premières consonnes représentent les 50 premiers nombres, celle des 5 mêmes voyelles avec les 10 dernières consonnes représentent les 50 derniers, la voyelle dans la syllabe représentant par exemple toujours le chiffre des dizaines, ce qui donne aux groupes un aspect caractéristique. Des leviers pareils à ceux de certaines caisses enregistreuses, se déplaçant devant des secteurs où figurent chiffres ou lettres, permettent de former les nombres au chiffrement, les groupes de deux lettres au déchiffrement. Lettres et chiffres sont en relief sur la tranche des roues imprimeuses, conjuguées deux à deux, et se déplaçant en même temps, mais décalées l'une par rapport à l'autre, au cours du chiffrement, au moyen d'une chaîne clef analogue à celle que nous avons décrite au sujet de la machine à chiffrer d'Aktiebologet-Cryptograph. Un même groupe de deux chiffres est donc représenté par des lettres différentes; la lettre représentant un même chiffre de dizaine ou d'unité change constamment au cours de l'opération.

L'emploi de ces appareils exige une deuxième opération après le chiffrement qui a donné des groupes de chiffres. Ils ne nous semblent pas fort intéressants tant qu'on ne pourra les établir à un prix fort bas, car les correspondants ayant un personnel destiné au chiffrement avec des codes, et disposés à engager, en plus, des fonds pour des machines à surchiffrer, nous semblent rares dans les circonstances

actuelles. Nous avons toutefois mentionné ces machines pour rappeler que la transformation des groupes de chiffres en groupes de 10 lettres prononçables est à l'ordre du jour et n'est pas perdue de vue par les inventeurs.

Nous arrêterons ici les descriptions de machines tirées des brevets antérieurs à 1923. Nos lecteurs ont déjà vu par des exemples qu'il n'y a pas toujours lieu de s'en rapporter aux chiffres impressionnants représentant des combinaisons différentes, présentés par les inventeurs à l'appui de l'excellence de leurs machines, mais qu'il faut analyser le travail, avec l'instrument en main, pour découvrir si une remarque du genre de celle que nous avons faite pour l'appareil Bazeries ne vient pas modifier les données du problème. Il y a lieu de tenir compte des conséquences d'une erreur de touche, et de voir ce que donnera la deuxième version si la première est intraduisible pour le destinataire. Il faudra escompter, d'après la facilité de modifier les organes clefs, la probabilité d'avoir, ou non, de nombreux cryptogrammes chiffrés avec des éléments qui en permettront l'étude conjointe. Toutefois, l'automatisme d'une machine permettant d'aborder des complications de systèmes qu'on n'oserait imposer à un chiffreur humain, il faut s'attendre à ce que l'emploi des machines à cryptographier pose aux cryptologues des problèmes nouveaux et intéressants.

CHAPITRE XVII

CONSIDÉRATIONS FINALES

Nous bornerons ici ces études élémentaires de cryptographie. Nous avons reproduit la plupart des méthodes simples, nous avons exposé les systèmes classiques qui en permettent le déchiffrement, nous avons même fait des incursions dans des domaines où la complication des méthodes rendait plus ardu le travail matériel et les efforts d'imagination du cryptologue. Nous n'avons pas craint de multiplier les exemples et d'allonger parfois certaines expositions peu attrayantes, pour que le lecteur puisse se rendre compte du détail des procédés, et qu'il sente, au milieu du labyrinthe où nous l'engagions, si sa vocation cryptographique est de taille à résister à l'ennui de lectures et de calculs méticuleux et embrouillés. Nous nous excusons des fautes qui pourront se découvrir dans le livre, soit par suite d'erreurs d'impression non corrigées, soit même comme conséquences d'erreurs de chiffrement dans les exercices.

Comme on l'a vu, nous n'avons exposé dans les pages qui précèdent qu'un nombre assez restreint de procédés et de méthodes, et, dans des brochures, des revues, des ouvrages de cryptographie, on en pourra trouver beaucoup qui ne sont point mentionnées ici. Cela provient le plus souvent de ce que nous n'avons jamais, parmi les milliers de cryptogrammes qui nous sont passés par les mains, reconnu l'emploi de ces systèmes, et que les études faites, parfois avec succès, sur leur décryptement, ne nous semblaient pas devoir prendre place dans un ouvrage destiné aux débutants en cryptographie. D'ailleurs un certain nombre d'entre eux se ramènent à

des variantes ou à des combinaisons de ceux que nous avons mentionnés, et, pour quelques-uns, les auteurs ont accumulé des complications dans des formations ou des désignations de clefs, d'alphabets, d'ordre des lettres, sans modifier au fond les procédés classiques. De telles méthodes peuvent être excellentes, et former une précieuse réserve d'armes pour les correspondants jaloux du secret de leurs télégrammes : elles peuvent parfois valoir beaucoup moins du jour où on voudrait les mettre en service dans une armée en campagne. En tout cas, nous ne les avons pas exposées ici en détail, laissant à nos lecteurs, s'il s'en trouve, le soin de disséquer ces méthodes quand ils en rencontreront la description publiée par leur auteur. Nous n'avons pas insisté non plus, dans un livre d'étudiants, sur des méthodes employées dans ces dernières années, généralement combinaisons de plusieurs procédés classiques, qui ont donné lieu à des travaux d'une grande ingéniosité et d'un vif intérêt; il eût fallu pour les explications et les exemples, faire appel à la proche histoire, et sans doute n'est-il point temps encore de traiter les sujets de cette nature.

A ce propos, nous pouvons toutefois faire les remarques suivantes :

Les études cryptographiques, immédiatement après la guerre de 1914-1919, semblent avoir pris un nouvel essor. D'un côté les systèmes se compliquent : les codes à bâtons rompus avec emploi de surchiffrement semblent couramment employés. Les superpositions de systèmes alphabétiques donnent lieu à la même constatation. On n'hésite pas à imposer aux chiffreurs, pour obtenir l'inviolabilité des cryptogrammes, des travaux bien plus considérables qu'autrefois. De plus on cherche à dérouter les décrypteurs par la fréquence des changements de clefs ou de systèmes.

D'autre part, dans la même période, des organisations puissantes, privées ou publiques, se sont occupées de cryptographie, et ont échangé des notes où se retrouve le désir de disséquer les procédés compliqués pour pouvoir confier une partie matérielle d'un travail de décryptement, puis

de déchiffrement, à des aides, ceux-ci pouvant être des débutants en cryptographie ou même des profanes. Et ces études ont donné lieu à des propositions de procédés nouveaux, évitant les points faibles des anciens.

Il résulte de tout ceci qu'en dehors même des difficultés dues aux perfectionnements des systèmes, on a beaucoup plus de mal que naguère même pour reconnaître tout simplement les systèmes employés, pour distinguer les codes des systèmes de substitution par lettres, pour différencier les codes entre eux, par suite de la disparition des « marquants » qui indiquaient les dictionnaires employés, de la multiplication des groupes pour représenter un même mot (ou homophones), etc.

Le décrypteur a donc plus de peine qu'autrefois à obtenir des résultats.

Dans ces conditions, nous ne saurions trop recommander de ne laisser échapper aucun renseignement et de donner une grande part à la statistique. Nous n'insistons pas sur l'aide que l'on doit chercher à obtenir de l'extérieur, en particulier des journaux poussés par la fièvre de l'information. Mais, dans l'étude des cryptogrammes, il faudra de plus en plus fréquemment chercher dans la comparaison des textes des renseignements, en particulier sur le procédé employé, que les relevés de fréquence et les particularités de la langue ne seront plus capables de fournir seuls. Nous conseillerons pour ces comparaisons minutieuses la transcription sur les mêmes grandes feuilles des cryptogrammes, ou au moins de parties de textes, surtout des débuts et parfois des fins ou des séquences communes : on devra chercher dans la physionomie des groupes, dans les répétitions, des renseignements que des changements de clef fréquents sur un même système chercheront à masquer, et il faudra oser des hypothèses et entreprendre des travaux parfois sans base solide.

La devise du décrypteur doit être celle de Guillaume le Taciturne : Ne pas avoir besoin d'espérer pour entreprendre ni de réussir pour persévérer. Certaines études durent des années avant d'aboutir. Pour d'autres, le cryptologue qui les a entreprises n'obtient jamais de résultats.

Mais, pour un décrypteur passionné, la joie des découvertes efface le souvenir des heures de doute et d'impatience.

En plus de la persévérance et de cette aptitude de l'esprit que certains auteurs considèrent comme un don spécial et qu'ils appellent l'intuition, ou même, à son plus haut degré, la clairvoyance, les études cryptographiques demanderont de plus en plus des qualités d'ordre et de mémoire. Les relevés devront avoir des références pour retrouver sans peine chaque lettre ou chaque groupe dans les textes de plus en plus compliqués qu'on aura à étudier, et dont l'étude, par suite, exigera des éléments plus nombreux. On devra également s'efforcer de prendre des précautions contre le relevé, dans une seule liste, d'éléments de codes ou de systèmes différents, et la plus efficiente, à notre avis, est un système de références détaillé, permettant d'éliminer d'un seul coup tout ce qui se rapporte à des documents devenus douteux au cours de l'étude. Des fiches pourront aider la mémoire pour retrouver soit les particularités de certains cryptogrammes, soit les événements ou les noms qui peuvent donner lieu à des hypothèses sur le contenu des documents.

L'auteur termine ici cette étude. Il espère que le lecteur pourra, malgré l'aridité du sujet et les fautes du livre, suivre les développements du texte. Il s'estimera heureux, si, par cette compilation d'éléments provenant de diverses sources, il a pu éviter, aux personnes désireuses d'étudier les écritures secrètes, les recherches dans des ouvrages parfois difficiles à trouver, et leur donner l'amour de travaux qui ont occupé une bonne partie de sa propre existence.

TABLE DES MATIÈRES

IMPRIMERIE BERGER-LEVRAULT, NANCY-PARIS-STRASBOURG