REVUE DE L'ARMÉE BELGE

24me ANNÉE

1899-1900

AVIS

La REVUE DE L'ARMÉE BELGE est éditée par la **Direction à Liége**, sans intervention d'aucune maison de librairie.

La Direction n'est pas responsable du service des abonnements fait par les libraires.

Néanmoins Messieurs les abonnés servis par les librairies, qui auraient des réclamations à faire, sont priés d'en informer la Direction de la REVUE DE L'ARMÉE BELGE, à Liége.

LIÉGE - IMP. H. DESSAIN.

REVUE

DE

L'ARMÉE BELGE

PARAISSANT TOUS LES DEUX MOIS

24me année. - Tome II. - Septembre-Octobre 1899

DIRECTEUR :
Lt-Colonel E. DAUBRESSE

DIRECTION & ADMINISTRATION, LIÉGE

1899

SOMMAIRE.

ETUDE

SUR LA

CRYPTOGRAPHIE

Son emploi à la guerre et dans la diplomatie.

La lecture de la correspondance ennemie est une des plus sûres bases des mesures à prendre par le commandement.

Cacher ses dessins à l'ennemi est aussi important que connaître les dispositions et les projets de ses adversaires.

INTRODUCTION.

L'importance d'un langage secret pour la transmission des correspondances militaires, diplomatiques et commerciales, a été reconnue de tous temps. Pas n'est besoin de discourir longuement pour démontrer l'impérieuse obligation d'user d'un chiffre, afin d'assurer le secret des opérations à la guerre. L'extension donnée aux communications télégraphiques, optiques et téléphoniques, fait ressortir tout particulièrement cette nécessité.

Les cas d'emploi sont nombreux et fréquents: relations directes et latérales entre le gouvernement, le commandant en chef et les places fortes, les détachements indépendants, les corps de partisans, les gouverneurs des provinces, les chefs de service de l'arrière et de l'intérieur; communications des ministres des chemins de fer, postes et télégraphes, de l'intérieur et des affaires étrangères avec leurs agents, dans le pays ou à l'étranger.

Les officiers envoyés en mission en avant et sur le flanc des armées (reconnaissances secrètes, reconnaissances d'état-major, pointes d'officiers), devront faire un usage constant de dépêches chiffrées. Les transmissions en langage clair, quelque anodin que soit leur contenu, ont parfois l'inconvénient, grave lorsque la presse s'en empare, ou qu'elles sont commentées par les habitants qui en sont instruits, de jeter l'inquiétude et l'alarme parmi les populations; les nouvelles sont grossies de proche en proche, dénaturées peu à peu, tronquées, faussées, sous les dehors de la vérité affirmée par cent bouches et arrivent souvent, sous forme de rumeur publique, à la connaissance des autorités, induisant quelquefois en erreur les états-majors eux-mêmes.

Dans la correspondance par pigeons, il est nécessaire, non seulement que toutes les dépêches soient cryptographiées, mais, comme pour la transmission des ordres et rapports de grande importance, il est indispensable que le système employé soit matériellement indéchiffrable.

L'histoire militaire prouve combien l'oubli ou la négligence, le dédain même du langage chiffré, ont été funestes. Nous allons citer quelques exemples à l'appui de cette assertion.

Pendant la campagne d'Italie, Louis XII éprouva, dit-on, les revers qui caractérisent la campagne de 1512, à cause de l'interception d'une lettre en clair expliquant la situation fâcheuse où se trouvait le général La Palice; les Italiens reprirent l'offensive et chassèrent les Français d'Italie.

Durant le siège de St-Dizier en 1544, qui arrêtait les Impériaux depuis un temps considérable, le cardinal de Granvelle surprit un paquet de lettres, contenant l'indication du chiffre que le duc de Guise employait pour correspondre avec le gouverneur de la place. Le cardinal en profita pour lui envoyer un message au nom du roi de France, par

lequel il lui conseillait de se faire accorder une capitulation honorable, ce qu'il fit, alors qu'il aurait encore pu tenir assez longtemps pour permettre au duc de Guise de le dégager.

Le maréchal de France Montluc, dans ses mémoires, cite aussi un exemple où la surprise du chiffre ennemi amena la capitulation de la place de Mondovi, par le seigneur de Dros. Henri IV, ayant pu faire saisir des lettres chiffrées adressées aux Espagnols par les Ligueurs, il chargea le célèbre Viète d'en trouver la clef. Le mathématicien y parvint ; Henri IV arriva ainsi à lire la correspondance de ses ennemis et à être au courant de leurs projets.

Pendant la campagne de 1806, le comte de Hatzfeld fut autorisé à conserver ses fonctions de bourgmestre de Berlin, après l'entrée des Français dans cette capitale, à condition qu'il ne tirerait aucun parti des renseignements qu'il pourrait recueillir, et de ne rien révéler des mouvements de troupe qu'il serait à même de surprendre. Il communiqua cependant avec son souverain. Ses dépêches furent interceptées, et leur lecture prouva à l'Empereur qu'il avait trahi sa parole. La preuve de sa trahison se trouva tout au long dans le texte en clair de la missive dont on s'était emparé. Il fut jugé par un conseil de guerre et condamné à la peine capitale. Il n'eut la vie sauve que grâce à de puissantes influences. On peut croire que l'acte du bourgmestre de Berlin, explicable par le grand patriotisme dont ce magistrat avait donné des gages manifestes, en conservant ses fonctions et en tentant de renseigner malgré tout le Roi de Prusse, n'eut pas eu de conséquences fâcheuses, s'il avait eu soin de cryptographier sa lettre, ou pour mieux dire, si la précaution si élémentaire de chiffrer les correspondances, n'avait pas été négligée, au même titre que tant d'autres, pendant cette malheureuse campagne.

En 1807, les Russes, se laissant tromper par une fausse

retraite de l'armée française quittant ses quartiers d'hiver de la Passarge, s'enfonçaient entre le gros de l'armée française à gauche et la mer à droite. Bernadotte leur tendait l'amorce: il devait se retirer lentement en tâchant de se lier aux mouvements du corps principal. Les Russes s'étaient avancés à ce point qu'ils allaient être tournés et jetés dans la Baltique. Malheureusement, un officier (le duc de Fezensac), envoyé au maréchal Bernadotte et porteur de dépêches, qui indiquaient la combinaison de l'Empereur et la position des différents corps, tomba entre les mains des Cosaques. Le général russe, éclairé sur le danger qu'il courait, arrêta sa marche offensive et se retira jusqu'à Eylau, où il livra la bataille de ce nom. — Si les dépêches adressées à Bernadotte avaient été chiffrées, c'en était fait de l'armée russe.

Pendant la campagne de 1813, les souverains alliés, à la tête de leur grande armée, avaient franchi, le 31 août, les montagnes qui séparent la Bohême de la Saxe, et s'avançaient sur Dresde. Un courrier portant en Angleterre les papiers de Moreau adressés à sa femme, tomba aux mains des coureurs français. Ces notes étaient un précis des journées qui précédèrent sa mort, et des débats avec l'état-major autrichien, dont il avait été témoin. Ces renseignements apprirent à Napoléon tout l'avantage qu'il avait sur ses adversaires, par l'unité dans le commandement et dans ses combinaisons.

Ils lui permirent de prendre les mesures complémentaires destinées à parer aux coups de la grande armée de Bohême, en concentrant à temps toutes ses forces autour de Dresde[1].

En 1814, l'interception par les Cosaques, d'un courrier envoyé de Strasbourg au maréchal Victor, fit connaître aux Alliés la vraie situation des Français, au moment où ils

(1) Napoléon au tribunal de César, par Jomini.

hésitaient encore à s'engager résolument dans une guerre contre la France même. Le capitaine Weil, dans sa relation de la campagne de 1814, d'après les archives impériales et royales de Vienne, rapporte que le 14 janvier, à l'instant, où la fortune favorisait les Alliés, le hasard fit tomber entre les mains des cavaliers de Pahlen, qui battaient le pays du côté de Mutzig et de Wasselonne, un courrier que de Strasbourg, Rœderer, commissaire extraordinaire de l'Empereur dans le Bas-Rhin, expédiait à Victor. Sur ce courrier on trouvait, outre la dépêche de Kellermann transmettant au duc de Bellune les reproches et les ordres de l'Empereur, et indiquant les positions des troupes entre Nancy et Charmes, une lettre de Rœderer au duc de Rovigo, dans laquelle il rendait un compte exact de l'état peu rassurant des esprits à Strasbourg, ainsi que de la terreur produite par l'apparition des premières troupes alliées aux environs de la ville.

Nous indiquons ci-après :

1° la lettre de Rœderer au duc de Rovigo;

2° l'ordre à Victor.

Leur lecture fera mieux ressortir l'importance des dépêches interceptées par les Cosaques.

1° Rœderer à M^r^ le duc de Rovigo, Ministre de la Police générale :

Strasbourg, 7 janvier 1814.

« Monsieur le duc, l'ennemi s'est approché hier de la ville en tiraillant jusqu'à une demi-lieue. Cette situation a fait un grand changement dans l'esprit du peuple. On criait dans les boutiques et dans les cafés que la ville était vendue, que le duc de Bellune en avait emmené la garnison, que la ville serait rendue sous trois jours. Ces bruits ont jeté la terreur dans la masse des habitants. Cette terreur procédait d'un bon sentiment ; mais plusieurs de ceux qui jetaient l'alarme m'ont paru suspects.

» En conséquence, j'ai pris le parti :

» 1° De faire une proclamation pour rassurer les bons;

» 2° De donner des ordres pour l'arrestation des orateurs, s'ils recommençaient aujourd'hui;

» 3° De prendre des mesures pour l'évacuation des étrangers suspects qui sont à Strasbourg.

» Je vais m'occuper de mesures de finances pour assurer tous les services . . . , le tout en cas que les communications soient coupées avec Paris, et elles sont au moins douteuses en ce moment.

» . . . . Les forces de l'ennemi, qui a passé devant le fort Vauban, ne sont guère que de 8.000 à 9.000 hommes; mais ils se sont répandus sur tout le pays, et se joignent avec les troupes du passage de Bâle . . . . .

» Enfin, il faut des secours du centre de la France, et il faut les promettre pour entretenir le zèle de cette ville-frontière. »

2° Le maréchal duc de Valmy, à S. E. le maréchal duc de Bellune, commandant le 2e corps.

« Mon cher Maréchal, j'ai fait connaître à S. M. l'Empereur le contenu de la dépêche que vous aviez adressée au commandant de Phalsbourg, et que vous l'aviez chargé de me communiquer.

» L'Empereur répond par dépêche télégraphique datée de ce jour de Paris :

» Ce n'était pas sur les hauteurs de Saverne que le duc de Bellune devait se diriger, mais sur Epinal. S'il est toujours du côté de Saverne, ordonnez-lui de filer sur Nancy. »

« Je m'empresse de vous transmettre cette dépêche, mon cher Maréchal, et de vous prévenir que la 1re division de jeune garde et les troupes réunies de la 4e division sont entre Nancy et Charmes, avec deux batteries, et prêtes à se porter sur Epinal, si la cavalerie ennemie dans les Vosges n'est pas soutenue par de l'infanterie.

» P. S. Le duc de Raguse était hier à Hombourg, près

Deux-Ponts, et le général Ricard à Ottweiler, avec les 8e et 32e divisions. »

On lit dans les *Recherches historiques sur l'art militaire* du général Bardin, à l'article *Chiffre sténographique*, que l'usage des chiffres s'était éteint au milieu de la conflagration de 1814, et que, lorsque Napoléon voulut réunir au noyau de l'armée toutes ses garnisons de l'étranger et plusieurs grandes garnisons françaises, ce fut en pur et clair français que Feltre et Berthier expédièrent ses ordres ; aussi, peu de dépêches parvinrent-elles à destination ; l'ennemi s'empara de la plupart.

« Peut-être, dit Bardin, le sort de la France et la face de l'Europe ont-ils dépendu de la désuétude où était tombée la cryptographie.

Pendant la bataille de Mont-Saint-Jean, un officier de chasseurs amena un hussard noir prussien, qui venait d'être fait prisonnier par les coureurs d'une colonne volante battant l'estrade entre Wavre et Planchenoit. Ce hussard était porteur d'une lettre annonçant l'arrivée du 4e corps prussien qui n'avait pas donné à Ligny. Le général Bulow demandait au duc de Wellington des ordres ultérieurs.

Le duc Dalmatie expédia sur le champ la lettre interceptée, et le rapport du hussard au maréchal Grouchy, auquel il réitéra l'ordre de marcher tout de suite sur Saint-Lambert, et de prendre à dos le corps du général Bulow. Il était onze heures ; l'officier n'avait au plus que quatre ou cinq lieues à faire, toujours sur de bons chemins, pour atteindre le maréchal Grouchy : il promit d'y être à une heure. (1)

Pendant la guerre d'Espagne, un Espagnol trouva le moyen de dérober le chiffre de Suchet ; il s'en servit pour faciliter à ses compatriotes la reprise de Mesquineux et Serida. (2)

(1) Mémoires de Napoléon : tome IX. — (2) d'après Kerckhoffs.

En 1854, la veille de la bataille de l'Alma, le maréchal de St-Arnaud avait fait rédiger sous sa dictée, le plan de la bataille de l'Alma, et donné au colonel Trochu (depuis général) l'ordre de le porter à Lord Raglan, avec mandat de répondre aux demandes d'éclaircissement que pourrait faire l'Etat-major anglais. Il était nuit noire quand le colonel Trochu se mit en route pour le quartier général anglais, accompagné d'un camarade, le colonel d'Etat-major de Lagondie, officier de grand mérite et attaché militaire français auprès de lord Raglan. « Dans l'obscurité profonde où nous cheminons, dit le colonel Trochu, nous sommes tenus à quelques précautions, car du haut de mon observatoire d'aujourd'hui, j'ai vu que beaucoup de cavaliers russes battaient la campagne. Le quartier général anglais est à une lieue de nous sur le Boulganak, qui coule en plaine sur un lit sableux avec quelques centimètres d'eau. Voilà notre voie, une voie sûre, qu'autrefois en Afrique, la nuit, dans les mêmes préoccupations de sûreté, j'ai plus d'une fois suivie. »

« A d'autres, répondit le colonel de Lagondie. Le Boulganak est plein de détours, et vous allez doubler pour le moins l'étape. Bon pour vous dont la nuit est sacrifiée ; mais moi, j'entends la passer dans mon lit de bivouac pour me préparer à la bataille. Je vous annoncerai à Lord Raglan. »

Et le voilà parti au trot en riant et raillant. Mais ce fut moi qui l'annonçai à lord Raglan. Il avait été capturé par un parti russe. Si, ajoute le colonel Trochu, j'avais suivi mon compagnon dans son voyage à travers champs, comme lui, et avec lui, j'aurais été fait prisonnier. L'ennemi aurait saisi sur moi le plan écrit et dessiné de la bataille de l'Alma. Il y aurait expressément vu que le maréchal de Saint-Arnaud, comptant sur l'agilité et l'endurance de la division d'Afrique (Bosquet), la mettait avant le jour en mouvement (trois heures avant les autres, en raison du long parcours

qu'elle avait à faire), pour marcher droit aux escarpements du bord de la mer, avec l'ordre d'en faire l'ascension, dès que notre centre et notre gauche seraient engagés. Ainsi avertis, les Russes réunissaient des troupes et des moyens de défense sur ces hauteurs, qu'en raison de leurs difficultés de franchissement, ils avaient négligées, et alors?...

Je ne veux rien affirmer, mais qui pourrait dire ce qu'aurait été la bataille de l'Alma, si la décisive entreprise de la division d'Afrique avait échoué ? (1)

L'examen de quelques faits de la guerre franco-allemande de 1870-71, d'après la relation du grand état-major prussien, fera ressortir particulièrement l'importance de la cryptographie aux armées.

Tandis que la Ire et la IIe armées allemandes livraient les batailles autour de Metz, la IIIe armée atteignait les bords de la Meurthe dans les journées du 15 et du 16 août, et poussait ses têtes de colonnes jusque sur la haute Moselle.

Au quartier général du Prince Royal de Prusse à Lunéville, on continuait encore, à cette époque, à manquer d'indications précises sur le 5e corps français ; mais on supposait que les masses françaises qui avaient repassé la Moselle devant la Ire et la IIe armées, poursuivaient leur mouvement rétrograde vers Châlons, où les renseignements recueillis annonçaient la concentration de forces sérieuses.

Le 17 août, la 4e division de cavalerie allemande gagnait Vaucouleurs, et faisait rayonner ses avant-gardes dans la région située entre la Meuse et l'Ornain. Un demi-escadron du 2e régiment des hussards du corps donnait la main, par Commercy, à la brigade des uhlans de la Garde, jetée par la IIe armée vers Saint-Mihiel, et s'emparait, dans la première de ces villes, d'un courrier français dont les lettres fournissaient maints renseignements.

(1) Général Trochu — Œuvres posthumes : La Société, l'Etat, l'Armée Tome II.

C'est ainsi qu'on apprenait, entre autres choses, la présence au camp de Châlons de la division de cavalerie du 6e corps, l'appel sous les drapeaux de tous les hommes âgés de 25 à 35 ans, la formation d'un 12e et d'un 13e corps sous le commandement des généraux Trochu et Vinoy. Des indications étaient recueillies sur la retraite du 1er et du 5e corps français (1).

Sous Metz, dans l'après-midi du 19 et dans la journée du 20 août, les communications régulières par chemin de fer et par le télégraphe, étaient interrompues par les Allemands entre Metz et Thionville. Cependant des émissaires connaissant bien le pays, cherchaient et parvenaient à se glisser au travers des lignes de troupes prussiennes, dont les emplacements étaient assez exactement connus. Les Français cherchaient en outre à entretenir avec le dehors des relations, très précaires il est vrai, d'abord en abandonnant au courant de la Moselle des bouteilles renfermant des lettres, puis plus tard au moyen de ballons-poste. Du côté prussien, on s'était immédiatement aperçu de cette ruse et des dispositions étaient prises pour recueillir les bouteilles. On s'emparait également d'un émissaire porteur de lettres du maréchal Bazaine à l'Empereur Napoléon. Le 19 août, le maréchal Mac-Mahon avait expédié à Metz un télégramme invitant le maréchal Bazaine à lui faire connaître ses dispositions. Le commandant de l'armée du Rhin lui avait répondu le 20 : « J'ai dû prendre position auprès de Metz pour donner du repos aux soldats et les ravitailler en vivres et en munitions. L'ennemi grossit toujours autour de moi. Je suivrai très probablement pour vous rejoindre, la ligne des places du nord et je vous préviendrai de ma marche, si toutefois je puis l'entreprendre sans compromettre l'armée. »

(1) Ouvrage du grand état-major prussien: Marche de la IIIe armée et de l'armée de la Meuse dans la direction de Châlons, — 1re partie, tome II.

Suivant les déclarations du maréchal de Mac-Mahon, cet avis ne parvint pas à destination. Nous pouvons donc admettre qu'il fut intercepté par les Allemands, et que le texte en clair permit à ceux-ci de connaître les intentions des chefs des deux grandes fractions de l'armée française, pendant que les deux maréchaux demeuraient dans la plus grande incertitude au sujet de leurs projets réciproques. Ce ne fut que le 29 août que le maréchal Bazaine apprit le mouvement dessiné par l'armée de Châlons; tandis que le maréchal de Mac-Mahon, persuadé par le texte de la dépêche, envoyée le 19 août de Metz, et reçue à Reims le 22, que le maréchal Bazaine était déjà en marche vers Montmédy, se décidait à reprendre le 23 sa marche vers l'Est.

La finale de la dépêche du 19, qui relatait que l'armée française avait conservé ses positions de St-Privat, et prendrait un repos de deux ou trois jours, était ainsi conçue: « Je compte toujours prendre la direction du nord et me rabattre ensuite par Montmédy sur la route de Sainte-Menehould à Châlons, si elle n'est pas trop fortement occupée. Dans le cas contraire, je continuerai sur Sedan, et même sur Mézières, pour gagner Châlons. »

Ce sont ces considérations qui amenaient le maréchal à revenir sur sa résolution première, de se rabattre sur la capitale pour tendre la main à l'armée du Rhin.

Si Mac-Mahon avait eu connaissance de la seconde dépêche de Bazaine (celle du 20), il est très probable qu'il eût continué sa retraite sur Paris, car ce n'est que contraint et forcé moralement par le ministre de la guerre et son entourage, qu'il s'était décidé à se porter au secours de Bazaine. « C'est ainsi, » dit l'ouvrage du grand état-major, « que les Français entraient définitivement dans la voie fatale qui, dix jours plus tard, devait les conduire à la catastrophe de Sedan. »

« Le 24 août, le commandant en chef de la IIe armée

avait fait parvenir une lettre interceptée dans laquelle un officier français de haut grade, appartenant à l'armée bloquée sous Metz, exprimait son ferme espoir d'être bientôt secouru par l'armée de Châlons. » Le grand quartier général du Roi à Commercy, avait été également informé que l'Empereur se trouvait à Reims avec une grande partie des forces françaises. Ces renseignements étaient communiqués au commandant de l'armée de la Meuse.

Le 24 août, un télégramme de Paris, daté du 23 au soir, et reçu par la voie de Londres, mandait : « L'armée de Mac-Mahon se concentre à Reims. L'empereur Napoléon et le prince sont avec elle. Mac-Mahon cherche à faire sa jonction avec Bazaine. »

Dans l'après-midi du même jour, le prince Albrecht de Prusse avait adressé au commandant en chef un journal de Paris qui confirmait les nouvelles reçues dans la matinée, à savoir que le maréchal de Mac-Mahon avait pris position à Reims avec 150.000 hommes environ.

L'interception de tous ces courriers, dépêches, etc., et leurs assertions concordantes, rédigés en langage clair, amènent le grand quartier général prussien, à émettre « l'avis qu'une tentative des Français pour se porter de Reims au secours de Bazaine, si elle était difficilement admissible en raison des objections qu'elle soulevait au point de vue militaire, pouvait cependant s'expliquer par des considérations politiques. Mais tous les renseignements qu'on possédait alors indiquaient que l'intention de l'ennemi était de couvrir la capitale, soit directement, soit en prenant position latéralement, à peu près vers Reims. »

Les données relatées ci-dessus permettaient de conclure sûrement à l'existence du projet de secourir Bazaine et à sa mise à exécution.

Cependant l'incertitude subsistait toujours quant à la manière dont l'ennemi comptait effectuer la jonction pro-

jetée. Nous allons voir comment la prise d'un courrier permit aux Allemands de connaître les dispositions prises par les Français, au moment décisif de la marche sur Sedan.

Le 29 août au matin, le capitaine d'état-major marquis de Grouchy fut fait prisonnier. Il était porteur des dépêches relatives aux dispositions prises par le commandant en chef des forces françaises, pour la journée du 29 août. En outre, on trouva sur lui divers renseignements sur les mouvements effectués les jours précédents, par l'armée de Châlons.

Quelle ne dut pas être l'importance de cette capture, au moment où le quartier général allemand était dans une grande perplexité au sujet de l'objectif précis de l'offensive générale projetée pour la journée du 30 août !

Qui peut dire combien la possession des documents trouvés sur l'officier d'état-major français, facilita aux Allemands le décèlement des intentions de l'ennemi, parmi toutes les incertitudes que devaient faire naître chez eux les incohérences apparentes de la marche de l'armée de Mac-Mahon ?

Qui peut affirmer combien les renseignements dus à l'interception des dépêches françaises, permirent au grand état-major prussien de diriger ses corps dans l'exécution du beau mouvement vers Reims et vers Sedan, alors que pendant cette conversion vers le nord, les Français ignoraient tout ou presque tout, non seulement de ce qui concernait l'armée adverse, mais encore et surtout, la situation et les intentions réciproques des deux tronçons des forces françaises qui avaient pour but de se réunir ou de se secourir ?

. . . . . .

Voici un nouvel exemple, où la prise d'un courrier dissipe les ténèbres qui enveloppent encore les mouvements des armées ennemies :

Pendant les marches et les opérations de la subdivision d'armée du grand-duc de Mecklembourg, pour couvrir Ver-

sailles, contre les troupes françaises qu'on croyait au Mans, la III^e^ armée allemande se dirigeait vers la Loire, et les forces françaises s'organisaient et se renforçaient dans cette partie de la France.

Le 20^e^ corps français, formé dans l'Est, avait été transporté à Gien; le 18^e^ était porté vers Ladon et Montargis.

Le manque de renseignements précis engage le quartier général allemand à ordonner des reconnaissances offensives pour la journée du 24 novembre. Elles amènent les combats de Maizières et de Ladon. Dans ce dernier, un officier d'état-major français fut tué. Les Allemands trouvèrent sur lui « un carnet contenant divers renseignements, l'ordre donné pour la journée au 18^e^ corps, et une lettre du Gouvernement de la Défense nationale donnant Gien comme clef des positions françaises sur la Loire et indiquant ses vues sur la suite des évènements militaires. »

Les exemples que nous avons tirés de l'histoire militaire contemporaine, portent en eux leurs enseignements et les conclusions à en tirer s'imposent d'elles-mêmes.

Voici ce que M. Kerckhoffs, dans son étude sur la cryptographie militaire, disait en 1883, et ses paroles n'ont pas cessé d'avoir toute leur valeur.

« Il ne suffit pas d'avoir un chiffre de correspondance secrète, il faut encore qu'il présente des garanties sérieuses d'indéchiffrabilité ; or, c'est le côté faible de la plupart des systèmes imaginés jusqu'à ce jour, et là où ce défaut capital a été écarté, on se trouve en présence d'inconvénients pratiques tout aussi graves. Même au ministère de la guerre, on ne s'est pas montré très heureux jusqu'ici dans le choix ou la combinaison du chiffre.

Ce n'est un secret pour personne, que pendant la guerre turco-russe on reçut, un dimanche, d'un des attachés militaires qui suivaient les opérations des armées en lutte, une dépêche chiffrée qui, par suite de l'absence du chef de

bureau chargé de la correspondance cryptographique, ne put être déchiffrée. Le ministre, qui ignorait la clef de la dépêche, ne crut alors pouvoir mieux faire que de prier un des officiers de l'état-major d'en essayer le déchiffrement *sans clef :* au bout de quelques heures le cryptogramme était traduit ! Heureusement pour le secret de la correspondance, l'habille déchiffreur était le fils du ministre lui-même. (Le capitaine Henri Berthaut, auquel je fais allusion, est certainement un des plus habiles déchiffreurs de l'état-major).

On a pu voir par les articles nécrologiques publiés en 1879 dans les journaux allemands, à l'occasion de la mort du capitaine Max Hering, le chef du service télégraphique, qui découvrit en 1870 le câble de la Seine, quels services a rendus aux assiégeants l'absence d'un système sûr de correspondance secrète, entre l'armée de Paris et les généraux de la province.

Je ne sais ce qu'il faut penser des affirmations des journalistes d'outre-Rhin ; mais lorsque je vois des juges autorisés déclarer que la cryptographie est un « auxiliaire puissant de la tactique militaire » (1), et que je songe que les destinées d'un pays, le sort d'une ville ou d'une armée, pourraient à l'occasion dépendre de la plus ou moins grande indéchiffrabilité d'un cryptogramme, je suis stupéfait de voir nos savants et nos professeurs enseigner et recommander, pour les usages de la guerre, des systèmes dont un déchiffreur tant soit peu expérimenté trouverait certainement la clef en moins d'une heure de temps.

On ne peut guère s'expliquer cet excès de confiance dans certains chiffres, que par l'abandon dans lequel la suppression des cabinets noirs et la sécurité des relations postales, ont fait tomber les études cryptographiques. »

Cet abandon de la cryptographie a largement contribué

(1) Voyez Dictionnaire philosophique — article *poste*.

à donner cours aux idées les plus erronées sur la valeur de nos systèmes de cryptographie.

C'est ainsi que le général Lewal affirme catégoriquement dans ses *Etudes de guerre* (Tactique des renseignements p. 76) « que les chiffres à base variable sont généralement *illisibles*, ou du moins qu'on n'arrive à les déchiffrer qu'*avec des difficultés inouïes!* » Et Voltaire lui-même n'a-t-il pas dit dans un article consacré aux écritures chiffrées, et cela à l'époque où l'art de déchiffrer était dans toute sa floraison, que ceux qui se vantent de déchiffrer une lettre « sans être » instruits des affaires qu'on y traite, et sans avoir de » secours préliminaires, sont de plus grands charlatans » que ceux qui se vanteraient d'entendre une langue qu'ils » n'ont point apprise » (1). Le comte Clarendon, dans une lettre écrite cent ans auparavant au docteur John Barwick, s'exprimait en termes analogues sur le compte des déchiffreurs: « I have heard of many of the pretenders of that skill, and have spoken with some of them, but have found them all to be mountebanks. » (2)

L'article 48 de notre règlement provisoire sur le service en campagne prescrit: « Si un message doit être tenu » secret, et si l'on craint qu'il ne soit intercepté par l'en- » nemi, on fait usage d'un chiffre. »

En campagne, il y a peu de messages qui ne doivent pas être tenus secrets, et tous courent des risques plus ou moins grands d'être interceptés par l'ennemi.

Quelles mesures convient-il de prendre *au point de vue militaire?*

D'abord, il faut avoir soin de chiffrer toutes les correspondances pour les communications réciproques à partir du régiment, avec les autorités supérieures, chaque fois que le danger et l'importance l'exigent.

(1) Dictionnaire philosophique.

(2) J'ai entendu parler d'un grand nombre de ceux qui prétendent avoir cette habileté ; j'ai parlé avec quelques-uns d'entre eux, mais j'ai trouvé que tous étaient des charlatans.

Il est nécessaire, d'autre part, que tout officier détaché en mission, puisse correspondre secrètement avec l'autorité qui le délègue.

Il serait donc désirable que chaque unité se servît fréquemment (tous les quinze jours par exemple) de son chiffre, pour des transmissions réelles ou fictives, afin de familiariser tout le monde avec ce mode de correspondance.

On objectera que l'usage de la cryptographie amène une perte de temps, par suite du chiffrement et de la lecture, et que si la dépêche tombe aux mains de l'ennemi, elle risque encore d'être connue par des déchiffreurs habiles.

A ces objections nous répondrons que si, dès la paix, l'officier s'est accoutumé à transcrire et à lire des dépêches chiffrées, le temps qui y sera consacré sera minime; ensuite, si l'on adopte un système simple, pratique, indéchiffrable, ou dont *le déchiffrement par l'ennemi demanderait un temps considérable*, on peut dire que l'inconvénient du temps perdu par l'emploi de l'écriture chiffrée, sera largement compensé par la sécurité plus grande qu'on en obtiendra. L'ennemi pourra bien intercepter la correspondance d'un courrier, mais il ne pourra pas toujours en tirer profit. Naturellement, il faut encore avoir soin de faire porter les ordres et rapports importants par plusieurs voies et, dans ce cas, on a de grandes chances qu'une de ces expéditions arrive à destination avec la certitude du secret.

Ainsi, pendant le siège de Paris en 1870, le courant d'un câble télégraphique fut détourné par les Allemands. Mais les dépêches étant chiffrées, ils ne purent tirer aucun avantage de leur opération, et ils durent se borner à couper le câble.

Nous avons rapporté la capture du capitaine d'état-major Grouchy, et nous en avons tiré des conséquences au point de vue de la connaissance des projets français pour les Allemands; mais le généralissime français, en envoyant

au général de Failly, un ordre qui modifiait sensiblement les dispositions arrêtées jusqu'à ce jour, avait confié le double de l'ordre à un second officier chargé de suivre une autre route, et qui parvint heureusement à sa destination.

Il résulte de ce qui précède, que nous devons faire usage d'un système de cryptographie peu compliqué pour l'opérateur, et indéchiffrable pour celui qui intercepte une dépêche : peu compliqué, pour réduire au minimum la perte de temps et épargner aux officiers d'état-major toute tension d'esprit inutile; indéchiffrable, eu égard à l'importance qu'il y a à assurer le secret des correspondances en campagne.

La première qualité est relativement plus utile aux unités inférieures ; la seconde est capitale pour les relations entre les autorités supérieures, le gouvernement et les places assiégées. Le facteur temps peut souvent alors être complètement négligé.

Il existe un grand nombre de méthodes cryptographiques. Leur étude approfondie n'est réellement indispensable que pour les officiers d'état-major, pour ceux que leurs fonctions ou leurs goûts obligent ou amènent à apprendre les procédés de chiffrement et de déchiffrement.

La connaissance de la cryptographie est cent fois plus utile que celle de la télégraphie pour la bonne raison, que partout où il y a un télégraphe, on trouvera des télégraphistes, tandis qu'on ne trouve pas partout des déchiffreurs; que le travail du télégraphiste n'a pas besoin d'être secret et confidentiel, tandis que celui du déchiffreur, l'est toujours. Il faut donc toujours pour effectuer ce dernier, un officier appartenant à l'état-major.

Au reste, les connaissances cryptographiques de la plupart des officiers peuvent se borner à savoir écrire et lire un texte chiffré, d'après un système adopté ou convenu.

La plupart des chiffres connus jusqu'à ce jour sont *tous* plus ou moins déchiffrables. Plusieurs auteurs ne considè-

rent comme réellement indéchiffrables que les systèmes à triple clef; mais ils les rejettent parce qu'ils sont trop longs, trop compliqués, c'est-à-dire peu pratiques. Cependant, si certains d'entre eux étaient réellement à l'épreuve du déchiffrement, il ne faudrait pas négliger d'y recourir pour les communications importantes dont on peut faire la lecture à tête reposée. Qu'importe alors le temps employé à écrire ou à lire la dépêche, pourvu que le secret soit assuré ! Nous verrons cependant que le secret des méthodes dites *à triple clef* n'est pas beaucoup mieux assuré que celui des systèmes à *double clef*, et que ce n'est pas la multitude de clefs qui est le facteur le plus important de la résistance au déchiffrement.

Le petit nombre d'ouvrages qui traitent de la cryptographie et la dispersion des notes qui s'y rattachent, l'absence de sérieuses méthodes de chiffrement, nous ont décidé à publier une étude sur ce sujet.

Dans l'exposé de ces matières, nous aurons recours aux idées émises par M. Kerckhoffs, pour ce qui concerne l'examen des méthodes dites *à double clef* et au capitaine Valério pour les procédés de déchiffrement; l'ouvrage de ce dernier auteur est le traité le plus complet et le plus scientifique qui ait été publié jusqu'ici sur cette question.

« Il y a des gens, dit Blaise Pascal, qui voudraient qu'un auteur ne parlât jamais des choses dont les autres ont parlé. Autrement on l'accuse de ne rien dire de nouveau... Mais si les matières qu'il traite ne sont pas nouvelles, la disposition en est nouvelle; j'aimerais autant qu'on l'accusât de se servir des mots anciens : comme si les mêmes pensées ne formaient pas un autre corps de discours par une disposition différente, aussi bien que les mêmes mots forment d'autres pensées par les différentes dispositions. »

Dans le but d'être utile à nos camarades, nous établirons d'abord quelques définitions, et nous reproduirons quel-

ques données sur la stéganographie dans le passé ; puis nous ferons l'exposition des systèmes de cryptographie les plus intéressants, en faisant ressortir leurs avantages et leurs inconvénients, ainsi que leurs procédés de déchiffrement.

Au cours de notre étude nous ferons connaître quelques procédés nouveaux de déchiffrement des méthodes connues, et une dizaine de méthodes de chiffrement matériellement ou mathématiquement irréductibles, tout en remplissant les conditions voulues pour leur usage à la correspondance militaire et diplomatique (1).

Les desiderata de la cryptographie militaire ont été indiqués dans le Journal des Sciences militaires, sous la signature de M. Kerckhoffs, et formulés ainsi qu'il suit: (2)

1° Le système doit être matériellement sinon mathématiquement indéchiffrable ;

2° Il faut qu'il n'exige pas le secret et qu'il puisse sans inconvénient tomber aux mains de l'ennemi ;

3° La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants;

4° Il faut qu'il soit applicable à la correspondance télégraphique ;

5° Il faut qu'il soit portatif et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes.

6° Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Pour que le système satisfasse à la condition première, il faut qu'il réponde au principe énoncé en manière de

(1) Nous rendrons volontiers compte de tout système de cryptographie qu'on voudra bien nous soumettre.

(2) Paris — Baudoin 1883.

devise par du Carlet: *Ars ipsi secreta magistro*, c'est-à-dire selon Kerckhoffs, « qu'un chiffre n'est bon qu'autant qu'il reste indéchiffrable pour le maître lui-même qui l'a inventé » (1).

Le capitaine d'artillerie Josse (2) a résumé ces six conditions en disant que la méthode ne doit comporter ni l'emploi d'un livre, ni celui d'un appareil, ce qui amène à la conclusion suivante: La cryptographie militaire proprement dite ne doit exiger que l'usage d'un crayon et de papier.

L'énoncé de ces principes comporte une interprétation qui consiste à dire, que l'emploi de tableaux, instruments ou livres *peu volumineux*, dont la saisie par l'ennemi n'entraîne pas la divulgation du secret de la méthode, ne doit pas faire rejeter les systèmes qui en usent; mais il est bon, si pas indispensable, que la perte de ces documents n'amène pas l'impossibilité pour les correspondants de continuer les relations secrètes. Il faut donc que les tableaux puissent être reconstitués rapidement par une loi mnémonique.

Aux conditions qui viennent d'être énoncées, nous en ajouterons une nouvelle, *idéale*, à remplir par les procédés cryptographiques en usage: il faut que la connaissance simultanée d'un fragment, ou même de toute une dépêche en clair, et de sa traduction en langage chiffré, ne livre pas le secret des correspondances ultérieures, chiffrées avec la même clef ou la même convention.

Il est assez rare que cette double notion existe pour les méthodes à clef littérale, numérique ou conventionnelle, mais elle est fréquente pour les systèmes à répertoire, parce que la perte, la divulgation, le détournement ou la copie d'un de ces documents, livre presque toujours le secret de la correspondance.

Les méthodes diplomatiques où il est fait usage de tables

(1) La Cryptographie, contenant une très subtile manière d'escrire secrètement, composée par maistre Jean Robert du Carlet, 1644.

(2) La Cryptographie, Revue maritime et coloniale, 1885.

chiffrantes et déchiffrantes, comportant plusieurs séries de chiffres dispersées au hasard, pour le même objet, n'assurent pas beaucoup mieux le secret, comme l'a démontré la publication des incidents d'un récent et célèbre procès militaire de haute trahison, même en admettant que la base du chiffrement soit à l'abri de toute indiscrétion ou de l'espionnage. Les procédés de déchiffrement que nous ferons connaître le prouveront à toute évidence.

Il est certain que les procédés à répertoire, même secret, tels qu'ils sont employés actuellement, tomberont bientôt dans le discrédit. Nous publierons en temps et lieu plusieurs méthodes qui assurent complètement le secret.

Certes, tous les auteurs qui ont fait des dictionnaires soi-disant secrets ont déclaré garantir l'inviolabilité de la correspondance, mais l'examen de leurs procédés de chiffrement démontrera qu'il n'en est rien. Leur plus grand avantage est de procurer une économie d'argent, parfois considérable, pour la transmission des longues dépêches; en ce point spécial, ils ont atteint fréquemment leur but.

Nous verrons qu'il y a moyen de réunir ces deux avantages.

Il n'est pas tout à fait indispensable que les méthodes à clefs remplissent la condition idéale; un système peut être bon sans cela; cependant il faudra presque toujours leur donner la préférence, lorsque d'autre part, ils répondent aux principes de Kerckhoffs. Nous étudierons à leur place les procédés que nous proposons pour y satisfaire.

Lorsque les correspondants sont en possession d'un procédé de cryptographie sûr, il faut encore que des déchiffreurs soient formés, pendant la paix, pour pénétrer le secret des dépêches surprises à l'ennemi et, dans notre situation spéciale de pays neutre, des télégrammes en transit, interceptés ou dérivés sur notre territoire et dépouillés avant leur retransmission. Songer à l'organisation de ce

service au moment de la guerre, serait arriver trop tard. D'ailleurs, même en temps de paix, on peut avoir besoin à chaque instant de correspondre secrètement et l'on comprendra l'importance du dépouillement des dépêches secrètes, transmises par courrier ou télégraphe, rien que par le caractère d'authenticité qui y est en quelque sorte inhérent.

A l'heure actuelle, l'usage de la cryptographie est répandu dans toutes les chancelleries ; le principe de la correspondance secrète est inscrit dans tous les règlements militaires, mais la pratique de l'écriture chiffrée n'est pas encore dans nos habitudes. Espérons que nous ne tarderons pas trop à entrer dans cette voie, pour que nous n'ayons pas un jour le regret de ne pas avoir fait dans ce domaine tout ce que nous pouvions et devions faire.

Pour remplir les desiderata exprimés par les cryptologues, et notamment par le capitaine Valério, il faut organiser une section de déchiffrement, composée de deux ou trois officiers déchiffreurs assistés d'un nombre égal d'aides qui, sans être initiés au déchiffrement, prépareraient le travail, en établissant les comptes de fréquence, de séquence, etc.

Le savant cryptologue déclare d'autre part : « Ce travail du déchiffreur ne doit pas être considéré comme une tâche accessoire, pouvant côtoyer des occupations importantes d'une autre nature. La somme de patience et d'assiduité à fournir, les connaissances philologiques à cultiver, suffisent pour remplir amplement la vie d'un homme ; c'est d'ailleurs par une pratique constante que le déchiffreur atteindra dans son art, le degré d'habileté suffisant pour dévoiler le secret en temps utile. »

Afin de faciliter la lecture et l'étude des matières examinées dans notre travail, nous ferons sommairement connaître celui-ci par la table ci-après :

TITRE I.

NOTIONS GÉNÉRALES PRÉLIMINAIRES.

CHAPITRE I. — LA CRYPTOGRAPHIE DANS LE PASSÉ.

La *cryptographie* (grec, kryptos, caché; graphô, j'écris) est l'art d'écrire en transposant les lettres de l'alphabet, ou en les représentant par des signes spéciaux ou conventionnels (chiffres, notes de musique, etc.). Elle a pour objet d'assurer le secret de la correspondance, entre des agents qui sont initiés à la *convention*, ou à la *clef du système* suivant lequel la transformation du *texte* ou *langage clair* a été faite, en *texte* ou *langage chiffré* ou *convenu*.

Le *chiffre simple*, ou *à simple clef*, est celui où l'on se sert toujours d'une même figure pour représenter la même lettre.

Le *chiffre double* ou *à double clef*, est celui où l'on change d'alphabet à chaque lettre ou mot.

Le *chiffre triple* ou *à triple clef*, est le cryptogramme obtenu par la combinaison d'une clef simple et d'une clef double.

Le *langage chiffré* est celui qui emploie plus particulièrement des signes, lettres ou chiffres, pour représenter des lettres, des mots ou des phrases du langage clair, en modifiant la valeur, l'ordre, le rang, le nom, etc., des signes usuels.

L'*alphabet* est le double du chiffre; il indique en regard des signes clairs, les signes secrets correspondants; c'est la *table chiffrante;* le tableau inverse où se trouve, vis-à-vis

de chaque caractère secret, son équivalent en langage clair, est la *table déchiffrante*.

Le *langage convenu* est celui qui se sert des mots de la langue courante, mais en leur donnant une signification différente de celle qu'ils ont dans le langage usuel.

La *cryptologie* (grec, kryptos, caché; logos, discours) est la science qui traite des écritures secrètes.

Un *cryptologue* ou un *cryptographe* (1) est celui qui s'occupe de la science cryptologique ou cryptographique, et du déchiffrement des textes secrets ou *cryptogrammes*.

Cryptographier, c'est transposer un texte clair en texte chiffré. Cette opération se nomme aussi *chiffrer*.

La *lecture* d'un cryptogramme est l'opération inverse, ou la traduction en langage clair d'un texte chiffré.

Nous réserverons le terme *déchiffrer* à la recherche de la signification en langage clair, de la dépêche qui a donné naissance à un texte secret quelconque, sans la connaissance de la clef ou convention qui lie les correspondants. En d'autres termes, c'est l'art d'expliquer un chiffre, c'est-à-dire de deviner le sens d'un discours écrit en caractères différents des caractères ordinaires.

Les dénominations chiffrer et déchiffrer proviennent sans doute de ce que ceux qui, les premiers, ont cherché à écrire secrètement, se sont servis des chiffres de l'arithmétique. Chez les Grecs, d'ailleurs, les chiffres arithmétiques n'étaient autre chose que les lettres de leur alphabet.

La *stéganographie* (grec, steganos, couvert, caché; graphô, j'écris) et la *polygraphie* (grec, polys, plusieurs; graphô, j'écris) synonymes de cryptographie, signifient plus spécialement, la première, l'art d'écrire en chiffres et d'expliquer cette écriture; la seconde, l'art qui traite des écritures secrètes multiples, avec des alphabets de convention.

Une autre étymologie de *poligraphie* (polis, ville ou état;

(1) Un cryptographe est aussi un instrument qui applique mécaniquement un système déterminé.

graphô, j'écris) donnerait à ce mot la signification d'art d'écrire les secrets d'états. Nous préférons la première comme plus logique, plus naturelle.

La *sténographie* (grec, stenos, étroit ; graphô, j'écris) est l'art de se servir de signes abrégés pour écrire ; elle est surtout employée pour écrire aussi vite que la parole.

Les signes sténographiques forment un alphabet spécial ; ils ne rentrent dans le langage chiffré que s'ils sont connus seulement de quelques initiés.

Tout système de signes conventionnels destinés à représenter et à abréger le langage clair, peut être classé dans la sténographie; tels sont le langage symbolique des astrologues et des alchimistes, l'écriture chinoise, les notes et signes de la musique, les notations et formules chimiques, algébriques, l'alphabet Morse, etc.

L'évêque Wilkins a décrit longuement son langage universel, par les notes musicales représentant des choses ; Thicknesse donne un système complet de langue musicale; le duc de Brunswick (Gustave Sélénus) dans sa *Cryptographie* liv. VI, ch. 19, attribue au comte Frédéric d'Ostingen le premier système d'application des notes musicales au langage. Enfin Trithème, en 1499, dans sa lettre à Bostius, dit qu'il avait l'habitude de discourir au moyen du chant ou d'un instrument de musique.

On a bien proposé de cryptographier en se servant des combinaisons des notes, des clefs et mesures de la musique, pour représenter les lettres de l'alphabet et permettre ainsi le chiffrement d'un texte clair, mais cette méthode n'est réellement de la cryptographie que si ces combinaisons se font en vertu de certaines lois, sinon ce système est un procédé de sténographie, si c'est pour abréger le discours, ou un alphabet quelconque qui a l'inconvénient grave de ne pas se prêter aux transmissions télégraphiques tout en exigeant le secret.

Les anciens n'ignoraient pas l'art d'écrire par notes. Sans remonter aux Egyptiens, dont les hiéroglyphes étaient plutôt des symboles qui représentaient des êtres moraux et physiques (Palmyre), nous trouvons chez les Grecs des tachigraphes, ou plutôt tachéographes (des mots grecs takos, vite, et graphô, j'écris), ou encore des brachygraphes (de brachos, court, et graphô, j'écris).

A raison des caractères singuliers dont ces écrivains étaient obligés de se servir, on les a assez généralement confondus avec les cryptographes, mais si l'on examine l'étymologie de leurs noms et la nature de leurs fonctions, on se convainc que c'est bien la sténographie qu'ils pratiquaient, dans le sens que nous attachons aujourd'hui à ce mot.

A Rome, on appellait *tachéographie*, l'art d'écrire aussi vite qu'on parle, par le moyen de certaines notes, dont chacune avait sa signification particulière et déterminée. Dès que le secret de ces notes eût été divulgué, la tachéographie devint une espèce d'écriture courante à laquelle on exerçait les jeunes gens. Ceux qui faisaient profession d'écrire en notes reçurent le nom de notarii, qui vraisemblablement, est l'origine du mot notarius, notaire. Il y avait à cette époque peu de particuliers qui n'eussent quelque esclave ou affranchi exercé à écrire d'une manière abrégée.

Les Romains adoptèrent ce genre d'écriture, principalement parce que souvent les discours des sénateurs étaient mal rapportés et mal interprétés, ce qui occasionnait de la confusion dans les débats.

Plutarque (1) attribue à Cicéron l'art d'écrire en notes abrégées et d'exprimer plusieurs mots par un seul caractère; il rapporte que ce consul enseigna cet art à son affranchi Tiron, qui prit mot à mot le fameux discours que Caton d'Utique prononçait contre César lors de la conjuration de Catilina.

(1) Vie des hommes illustres, traduite par Darcier.

C'est par ce moyen que nous est parvenu cet unique morceau d'éloquence que Saluste a inséré dans son histoire.

Caton n'écrivait aucune de ses belles harangues ; aussi Cicéron avait-il placé plusieurs tachéographes en différents endroits du Sénat pour recueillir les paroles du célèbre orateur.

Les notes abréviatives étaient des figures qui n'avaient aucun rapport avec l'écriture ordinaire, et chacun de ces signes représentait, comme nous l'avons déjà dit, une syllabe ou un mot tout entier. Les abréviations étaient souvent l'écriture ordinaire des inscriptions publiques et des médailles (sigles). Ainsi, chacun savait à Rome que les lettres S. P. Q. R. étaient mises pour Senatus populusque romanus (le Sénat et le peuple romain) et D. M. pour Dis manibus, etc. Par l'arrangement qu'elles avaient entre elles, par la place qu'elles occupaient dans les discours, les *sigles* équivalaient aux yeux du lecteur à une suite d'expressions connues. Les jurisconsultes les employaient communément dans leurs ouvrages, aussi bien que les philosophes et les rhéteurs dans leurs écoles.

Aristoxène, contemporain d'Aristote, dans son traité de la musique, fait de l'art d'écrire une partie de la musique, et l'on peut croire que les notes de musique et les caractères dont se servaient les médecins, sont encore des restes de ces anciennes notes qui n'étaient autre chose qu'une ou deux lettres pour exprimer tout un mot, et qui, par conséquent, étaient plutôt des abréviations que des signes ou des chiffres.

La notation de mots entiers ou de syllabes entières est due au vieux poète Ennius. On retrouve plus de mille signes abrégés dans Probus, Paul Dracon, Goltzius et à la fin des Inscriptions de Gurner. Les caractères tyroniens employés pour la sténographie ne sont pas alphabétiques. Ils présentent une grande ressemblance quand ils expriment les mêmes initiales ou les mêmes désinences latines. On

aurait tort de penser qu'ils fussent abandonnés au hasard, car ils constituaient réellement un système complet et suivi.

L'*art sténographique*, suivant Diogène Laërce et Xénophon, faisait usage des signes abrégés pour recueillir les entretiens de Socrate.

Chez les Romains, Ennius, d'après Isidore de Séville, avait inventé 11.000 signes abréviatifs appelés notes. Mais suivant Eusèbe, cette invention devrait être attribuée à Tyron, affranchi de Cicéron.

Les *notes tironiennes* reçurent par la suite de nombreuses modifications, et furent généralement employées dans les assemblées publiques, dans les écoles, dans les tribunaux même, pour la transcription de certains livres et la rédaction de certains actes, jusque dans la première année du XI^e^ siècle, où finit la sténographie des anciens.

La sténographie moderne est née en Angleterre au XVI^e^ siècle, mais ses progrès réels ne commencèrent qu'au siècle suivant, lorsqu'on sentit le besoin de recueillir les discours improvisés à la tribune parlementaire. On se servit d'abord d'une méthode créée, au siècle précédent, par Macaulay ; mais à partir de 1659, on donna la préférence à un nouveau système, celui de Shelton, lequel fut bientôt suivi d'une trentaine d'autres, dont un, dû à Weston (1743) obtint une grande faveur. En France, le premier traité de sténographie date de 1651 : c'est l'*art d'écrire aussi vite que l'on parle*, de l'abbé Cossard.

En 1681, le chevalier Ramsay nous fit connaître la méthode de Shelton, et en 1779, Coulon-Thévenot publia son ingénieux système, qui lui valut le titre de secrétaire-sténographe de Louis XVI.

D'autres publications analogues eurent lieu, tant en France qu'en Angleterre, mais une seule eut quelque succès : ce fut celle de l'anglais Sam Taylor, qui parut en 1786, et dont P. Bertin donne une traduction française en 1792.

Malgré les divers systèmes qui existaient alors, l'art sténographique était si peu cultivé au commencement de la révolution, qu'aucun journal ne put trouver des hommes capables de reproduire les séances de la Constituante. Sous la Législative, la même cause fit recourir à un moyen véritablement primitif. Cinq ou six rédacteurs rangés autour d'une table et se servant de l'écriture ordinaire, écrivaient des phrases ou des parties de phrases qui étaient ensuite réunies pour former un tout. Ce procédé reçut le nom de *Logographie*, et les personnes ainsi employées à recueillir les discours prenaient le titre de *logographes*.

La sténographie proprement dite fut un peu plus cultivée sous le Directoire; mais sous le Consulat et l'Empire, son rôle se trouva singulièrement réduit. Néanmoins c'est de cette période que datent les traités de Montigny (1799), de Clément (1801), d'Honoré Blanc (1802), de Piet (1805), etc., qui sont aujourd'hui complètement oubliés.

Enfin, l'inauguration du véritable gouvernement représentatif par la Restauration, donna un emploi régulier aux hommes qui cultivaient la sténographie et fit en même temps éclore une foule de systèmes.

On vit alors paraître successivement les ouvrages d'Astier, de Coran, de Prépéau, de Grosselin, d'Aimé Paris, d'Hipp Prévost, etc.

Aujourd'hui les méthodes sténographiques s'élèvent à un fort grand nombre ; cependant on peut les réduire toutes à trois systèmes principaux. Dans l'un, chaque son est exprimé d'après sa prononciation exacte et sans avoir égard à l'orthographe, par un signe très simple ; mais il est difficile de lier entre elles les différentes syllabes d'un même mot.

Dans le second, les consonnes s'écrivent sur des lettres écrites sur des lignes tracées à l'avance, comme la portée de la musique; on supprime les voyelles qui sont indiquées par la position de la consonne.

Dans le troisième, qui est, on peut dire, le seul en usage parmi ceux qui exercent la profession de sténographe, les mots sont tracés d'un seul jet, c'est-à-dire sans lever la plume, et en liant ensemble tous les caractères qui forment chaque mot. Au reste, toutes les écritures sténographiques ont cela de commun, qu'elles emploient des caractères de convention aussi simples que possible. La ligne droite, tantôt perpendiculaire, tantôt horizontale, tantôt oblique à gauche ou à droite; l'arc de cercle tourné en haut ou en bas, à droite ou à gauche; le cercle entier; la boucle ajoutée à l'une des extrémités de la ligne droite, et enfin le point: tels sont les éléments de toute sténographie.

Ajoutons que, quel que soit le système adopté par les sténographes de profession, chacun d'eux le modifie à son gré et imagine des monogrammes à son usage pour représenter certains mots qui reviennent souvent, des signes particuliers pour certaines désinences, etc., de telle sorte qu'un sténographe ne peut guère lire ce qu'a écrit un de ses confrères.

En dehors de la cryptographie et de la sténographie, mais dans le cadre des écritures secrètes, nous pouvons classer le procédé des *encres sympathiques* dont les signes, invisibles dans les conditions ordinaires, apparaissent dès qu'on les a soumis à l'action de la chaleur, de l'humidité, ou à celle d'un réactif chimique convenable. Ainsi des caractères tracés avec un sel de plomb, apparaissent en noir dès qu'on les soumet aux vapeurs sulfhydriques; ceux écrits avec une solution faible de chlorure de cobalt se montrent d'un beau bleu dès qu'on chauffe le papier, et, dans les mêmes conditions, les signes tracés au moyen du lait ou du jus de cerise, de pomme, d'orange, de citron ou d'oignon, prennent une teinte foncée, rouge, jaune ou brune, etc. caractéristique. Des dissolutions nombreuses de sels ou de sucs organiques, donnent une écriture incolore qui se

révèle dans des conditions données. Les propriétés de certaines encres sympathiques sont connues depuis l'antiquité, et nous avons déjà dit qu'elles étaient mises à profit par les rendeurs d'oracles.

Philon le mécanicien, de Byzance, dans sa « Polyorcétique » au deuxième siècle avant Jésus-Christ, disait: « Les lettres secrètes s'écrivent avec une infusion de noix de galle concassées. Quand les caractères sèchent, ils deviennent invisibles. Il suffit pour les voir réapparaître de les mouiller avec une éponge imbibée d'une dissolution de sulfate de cuivre, comme lorsqu'on prépare l'encre. »

Au sujet des encres sympathiques, M. Dallet, dans la Revue scientifique de 1887, nous rapporte les intéressants détails ci-après:

« On connaît les amusements qui sont basés sur certaines encres qui ont la propriété d'apparaître à la chaleur: telle est celle qui s'obtient en ajoutant au chlorure de cobalt, une petite quantité de chlorhydrate de tritoxyde de fer qui verdit à la chaleur. Si l'on dessine à l'encre de Chine un paysage d'hiver, et qu'on indique avec de l'encre préparée, des feuilles aux arbres et du gazon, dès qu'on élève la température, le paysage change, et l'on voit apparaître un paysage d'été. »

L'acide sulfurique, étendu de 10 fois son poids d'eau, produit sous l'action de la chaleur une couleur bleue ineffaçable.

Enfin, on obtient une belle coloration pourpre, lorsqu'on passe une solution de chlorure d'étain sur l'écriture invisible tracée avec du chlorure d'or.

Rabelais nous a conservé le souvenir des encres sympathiques, dans une lettre qui renfermait un anneau d'or; cette lettre, adressée à Pantagruel, ne portait rien d'écrit. Panurge cherche à découvrir le contenu « de la feuille de papier qui estoyt escripte, mais l'estoyt par telle subtilité que l'on n'y voyait point d'escripture. Il la mit, dit Rabe-

lais, auprès du feu pour veoir si l'escripture estoyt faicte avec du sel ammoniac détrempé en eau. Puys la mist dedans l'eaue pour sçavoir si la lettre estoyt escripte du suc de tithymale. Puys, la montra à la chandelle, elle estoyt point escripte du jus d'oignons blancz.... »

Pour faire usage de ce mode de correspondance secrète, on écrivait ordinairement entre les lignes d'une dépêche insignifiante ou trompeuse, rédigée ostensiblement, la dépêche vraie avec l'encre sympathique.

Actuellement, l'emploi de ce procédé serait fort aléatoire, car quelques notions de chimie suffisent pour trouver le réactif révélateur.

La *cryptographie*, qui est un art fort innocent, n'a pas laissé de passer autrefois pour une invention démoniaque. Trithème, abbé de Spanheim, ayant entrepris de le faire revivre, et ayant composé dans ce but plusieurs ouvrages, un mathématicien, qui ne parvenait pas à comprendre les noms extraordinaires que Trithème avait employés pour marquer sa méthode, écrivit que l'ouvrage était rempli de mystères diaboliques. D'autres savants de cette époque, et l'on n'est pas peu étonné de trouver parmi eux l'illustre Jérôme Cardan, jetèrent l'anathème sur l'abbé.

Les savants du moyen-âge furent d'ailleurs souvent obligés de cacher sous un langage mystérieux les découvertes dont ils avaient doté la science, les uns par prudence, pour éviter le bûcher des sorciers, les autres pour augmenter leur influence sur leurs crédules contemporains.

Sous Henri IV encore, le célèbre géomètre Viète, ayant réussi à découvrir, pour le compte de son souverain, le secret de la correspondance des Ligueurs avec les Espagnols, ceux-ci trouvèrent ce phénomène si extraordinaire, qu'ils citèrent le savant chercheur devant l'Inquisition, sous l'accusation de sorcellerie.

Il n'y a pas longtemps, le fait d'écrire en langage secret

ou convenu, était encore considéré comme un maléfice, exposant l'auteur aux pires condamnations. Cependant, lorsqu'on fut revenu de ces préjugés, divers auteurs publièrent des traités de stéganographie: Caramuel, le jésuite allemand, Gaspard Scott, Ernest Heidel, autre savant allemand, et même un duc de Lunébourg (Sélénus), en 1624, fit imprimer un traité intitulé « Cryptographia. »

On trouve plusieurs exemples de cryptographie dans les « Récréations mathématiques » du célèbre mathématicien français J. Ozanam (1640-1717). A cette époque un grand nombre d'ouvrages traitèrent ou parlèrent de cette science, qui bientôt prit droit de cité, et acquit une importance considérable.

Il est impossible de fixer une date précise à l'invention ou au premier emploi de la cryptographie. On estime qu'elle remonte à la plus haute antiquité, c'est-à-dire aux débuts de la plus ancienne des sciences humaines : la guerre, et de sa sœur, la diplomatie. Elle serait donc antérieure même à l'écriture. A l'origine de celle-ci, les caractères, les signes de la langue, symboliques ou sacrés, étaient eux-mêmes incompréhensibles pour les profanes, et constituaient une forme d'écriture secrète.

Vigenère, un des fondateurs de la cryptographie moderne, s'exprime ainsi au sujet de son art :

« Les hommes de tout temps ont esté curieux de se tracer, chacun pour soy, quelques notes secrètes pour se récéler de la cognoissance des autres, comme les marchands en leurs marques et papiers de compte; les médecins, en leurs pieds de mouche ; les jurisconsultes en leurs paragraphes. »

L'histoire des coutumes de chaque peuple nous montre des modes de correspondance secrète par les fleurs, les couleurs, les bijoux, les rubans, les nœuds et les sons, etc., etc.

La *Belgique coloniale* du 5 février 1899 donne des détails

très intéressants sur le mode de transmission des nouvelles à distance, usité parmi les peuplades noires : « De tous les instruments de musique, c'est le *tam-tam* qui est le plus répandu en Afrique. Par différentes batteries, les noirs fêtent une guerre, une victoire, un mariage, une naissance, une mort, une nouvelle lune, un festin de... cannibales. Le tam-tam sert encore à correspondre à longue distance, au moyen d'un langage frappé, composé d'un certain nombre de phrases usuelles et de mots qui peuvent s'assembler de diverses façons. Les Européens et même la plupart des indigènes ignorent ce langage frappé qui est fort souvent réservé aux hommes libres et aux chefs. »

Ceci est confirmé par le pasteur Reindorf pour les peuplades de la Côte d'Or, où la langue frappée sur les tam-tam, donne lieu à des demandes et des réponses énigmatiques pour les non initiés.

Chez les indigènes du Kameroun, le tam-tam et le tambour font office de téléphone et de télégraphe à des distances parfois très grandes. Là, pour que le « jeu » soit complet, il y a un grand tam-tam d'au moins 1^{m}50 de hauteur sur 50 à 70 centimètres de diamètre, qu'on bat avec des mailloches, et deux plus petits tams-tams frappés avec les mains.

Lorsqu'on entend cette musique pour la première fois, on croit que les joueurs ne cherchent qu'à faire autant de tapage que possible ; mais après quelque temps, on distingue dans cette cacophonie infernale un certain rythme et une certaine mesure. Maintes fois les joueurs de tam-tam chantent en jouant. Leur répertoire est tellement riche, que deux groupes de joueurs, ayant fait la gageure de jouer et de chanter le plus grand nombre de morceaux différents, ne purent finir en une journée leur pari.

Les peuplades indiennes de l'Amérique du Sud, et notamment du Pérou, se servaient de combinaisons de nœuds

(quipos) pour remplacer l'arithmétique des nombres, à la façon des Grecs et des Romains. Les *quipos* servaient encore à établir des relations de toute nature par la variété, la forme et la couleur des nœuds.

Tout nous porte à croire que dans l'enfance des peuples les idées se transmettaient par des signaux, par des gestes, comme le font encore les enfants avant de parler. Des faits nombreux démontrent que cette pratique était admise chez les anciens. Ovide écrit quelque part : « Je dirai des mots sans ouvrir la bouche... tu liras les mots sur ses doigts... la bouche est muette, mais d'autres moyens permettent que nous puissions échanger nos pensées. » Les Latins exprimaient les nombres au-dessous de cent à l'aide de la main gauche, et ceux au-dessus de mille par les doigts de la main droite. Juvénal et d'autres poètes font souvent allusion à cet usage. Pierins nous a conservé leur méthode de compter de 1 à 9.000. Gaspard Schott, dans sa *Sténographie*, donne leur alphabet arthrologique ou par gestes, en latin et en allemand. Falconer, dans sa *Cryptomenisis patefacta*, et Wilkins, dans son *Mercure*, le donnent aussi en latin et en anglais.

Pour faire servir à la correspondance secrète cet art de discourir par gestes, Schott a formé un alphabet, différent de l'alphabet généralement usité ; sous Charles II, roi d'Angleterre, Georges d'Algarme, dans son *Didascophalus*, préconise un caractère universel et une langue philosophique à l'usage de toutes les nations.

Polybe raconte qu'Enée le Tacticien fit, il y a environ deux mille ans, une collection de vingt manières différentes qu'il avait inventées, ou dont on s'était servi jusqu'alors, pour écrire de telle sorte qu'il n'y avait que celui qui en savait le secret qui pût y comprendre quelque chose. Il rapporte que les anciens correspondaient secrètement au moyen de signaux ignés, de dés percés de 24 trous correspondant

aux lettres de l'alphabet, dans lesquels on faisait passer un fil, pour indiquer la suite des lettres nécessaires à la confection de la phrase. Ce dernier moyen a quelque analogie avec le procédé des grilles, encore en usage, et dont nous parlerons plus tard.

Ils se transmettaient encore leurs dépêches en les introduisant dans les semelles du messager, dans des pendants d'oreilles de femmes, ou dans des ulcères produits artificiellement sur le porteur.

Ce qui nous reste d'Enée, fournit de précieux matériaux au cryptologue, et il est regrettable que l'usage traditionnel ne nous ait pas transmis celles de ses utiles découvertes dont nous ne retrouvons plus que la désignation dans Polybe.

On trouve dans l'histoire grecque un stratagème, imaginé par Histiée.

Celui-ci, établi chez les Perses à la cour de Darius, voulait faire passer secrètement, à un certain Aristagoras, des nouvelles importantes. Un de ses esclaves souffrait depuis longtemps des yeux; sous prétexte de le guérir, il lui rase toute la tête, et trace des caractères par des piqûres sur la peau mise à nu. Il écrivit ainsi ce qu'il voulait. Il garda l'homme chez lui jusqu'à ce que sa chevelure eût repoussé; alors il l'envoie à Aristagoras: « Quand tu seras arrivé, lui dit-il, recommande-lui bien, en mon nom de te raser la tête, comme je l'ai fait moi-même. » L'esclave obéit, se rend chez Aristagoras, et lui transmet la recommandation de son maître. Celui-ci, s'y soumet: c'est ainsi que la lettre parvint à son adresse. »

Une idée ingénieuse nous est encore rapportée par Hérodote. Un Grec, du nom de Démocrate, voulut faire tenir à ses compatriotes un avis du plus haut intérêt; ayant pris des tablettes, il en enleva la cire, écrivit sur le bois, l'avis qu'il voulait transmettre, puis recouvrit ses lettres de cire.

L'esclave de Démocrate, porteur de ce singulier message, ayant remis ces tablettes aux Lacédémoniens, ceux-ci ne surent que conjecturer d'un pareil envoi; mais Gorgo, femme de Léonidas, imagina de faire fondre la cire et fit connaître la dépêche.

Une ruse semblable se trouve dans une vieille histoire de Carthage.

L'usage de marques ou de caractères particuliers était adopté chez les Juifs, dans cette sorte de cabalistique appelée *combinaison*.

Voici d'ailleurs, d'après Polybe (1), les renseignements les plus anciens qu'on possède sur les méthodes de correspondance secrète : Philippe de Macédoine appelé au secours des Achéens et des Béotiens, pendant l'expédition contre les Etoliens et Attalus, s'arrêta à Démétriade ; l'ennemi s'était retiré devant lui. Pour être instruit de tout ce qui se passerait, Philippe envoya ordre à Péparèthe de l'avertir, de la Phocide et de l'Eubée, de tout ce qui se passerait par des fanaux allumés sur le Tisée, d'où les habitants peuvent très commodément informer de ce qui se fait chez eux.

Comme cette manière de donner des signaux, quoique d'un grand usage dans la guerre, n'a pas été jusqu'à présent traitée avec exactitude, il est bon que nous nous y arrêtions un peu pour en donner une connaissance plus parfaite.

C'est une chose reconnue de tout le monde, que l'occasion qui a une grande part dans toutes les entreprises, en a une très grande dans celles qui regardent la guerre. Or, de tout ce qui s'est inventé pour la conduire, rien n'est plus utile que les signaux par le feu. Que les choses viennent de se passer, ou qu'elles se passent actuellement, on peut par ce moyen les apprendre à trois ou quatre journées de

(1) Traduit du grec par dom Vincent Thuillier au 18e siècle.

là, et quelquefois même à une plus grande distance, de sorte qu'on est surpris de recevoir le secours dont on avait besoin. Autrefois cette manière d'avertir était trop simple, et perdait par là beaucoup de son utilité car, pour en faire usage, il fallait être convenu qu'il était arrivé une armée à Orée, à Péparèthe ou à Chalcis ; mais des événements qui arrivent sans qu'on s'y attende, qui demandent qu'on tienne conseil sur le champ pour y porter du remède, comme une révolte, une trahison, un meurtre ou autre chose semblable, ces sortes d'événements ne pouvaient s'annoncer par le moyen des fanaux. Il n'est, en effet, pas possible de convenir d'un signal pour des événements qu'on ne peut pas prévoir.

Enée, cet auteur dont nous avons un ouvrage sur l'art de conduire les armées, s'est efforcé de remédier à cet inconvénient, mais il s'en faut beaucoup qu'il l'ait fait avec tout le succès qu'on aurait souhaité. On en va juger. « Ceux, dit-il, qui veulent s'informer mutuellement par des fanaux de ce qui se passe, n'ont qu'à prendre des vases de terre également larges, profonds et percés en quelques endroits: ce sera assez qu'ils aient trois coudées de hauteur et une de profondeur (diamètre); qu'ils prennent ensuite des morceaux de liège (flotteurs) un peu plus petits que l'ouverture des vases, qu'ils fichent au milieu de ce liège un bâton, distingué de trois doigts en trois doigts, par quelque enveloppe fort apparente, et qu'ils écrivent sur chacune de ces enveloppes les choses qui arrivent le plus ordinairement pendant une guerre. Sur l'une, par exemple, *Il est entré de la cavalerie dans le pays;* sur l'autre, *Il est arrivé de l'infanterie pesamment armée;* sur une troisième, *De l'infanterie légère;* sur la suivante, *De l'infanterie et de la cavalerie;* sur une autre encore, *Des vaisseaux*, ensuite, *Des vivres*, et de même sur toutes les autres enveloppes, tous les autres événements qu'ils prévoiront par bonnes raisons devoir arriver, eu égard à la guerre qu'on aura à soutenir:

que de part et d'autre on attache à ces vaisseaux de petits tuyaux d'une exacte égalité, en sorte qu'il ne s'écoule ni plus ni moins d'eau des uns que des autres ; qu'on remplisse les vases d'eau, qu'on pose dessus les morceaux de liège avec leurs bâtons, et qu'ensuite on ouvre les tuyaux. Cela fait, il est clair que les vases étant égaux, le liège descendra et les bâtons s'enfonceront dans les vases, à mesure que ceux-ci se videront : qu'après avoir fait cet essai avec une égale promptitude et de concert, on porte les vases aux endroits où l'on doit donner et observer les signaux et qu'on y mette le liège. Lorsqu'il arrivera une des choses qui auront été écrites sur les bâtons, on lèvera un fanal, et on le tiendra élevé jusqu'à ce que de l'autre côté on en lève un autre ; qu'alors on baisse le fanal et qu'on ouvre les tuyaux : quand la chose dont on veut avertir sera descendue au niveau des vases, on lèvera le flambeau et de l'autre côté, sur le champ, on bouchera les tuyaux, on regardera ce qui est écrit sur la partie du bâton qui touche à l'ouverture du vase; alors si tout a été exécuté de part et d'autre avec la même promptitude, de part et d'autre on lira la même chose.

Mais cette méthode, quoiqu'un peu différente de celle qui employait, avec des fanaux, des signes dont on était convenu, ne paraît pas encore suffisante ; on ne peut pas prévoir toutes les choses qui peuvent arriver, et quand on pourrait les prévoir, il serait impossible de les marquer toutes sur un bâton. D'ailleurs quand il arrivera quelque chose à laquelle on ne s'attendait pas, comment en avertir par ce moyen ?

Ajoutons que ce qui est écrit sur le bâton, n'est point du tout précis et déterminé. On n'y voit pas combien il est entré de cavalerie et d'infanterie, ni en quel endroit du pays sont ces troupes, ni combien de vaisseaux ou combien de vivres sont arrivés. Pour marquer ces particularités sur

le bâton, il aurait fallu les prévoir avant qu'elles arrivassent, et cela n'est pas possible. Cependant, ces particularités, c'est ce qu'il importe le plus de savoir ; car le moyen d'envoyer du secours, si l'on ne sait ni combien on aura d'ennemis à combattre, ni où ils sont ? Comment avoir confiance en ses forces ou s'en défier ; en un mot comment prendre son parti, sans savoir combien de vaisseaux ou combien de vivres il est venu de la part des alliés ? »

Une autre méthode de cette époque, a pour auteur *Cléoxène ;* certains l'attribuent à *Démoclite.* D'après son inventeur, elle fixe tout, et par ce moyen on peut avertir de tout ce qui se passe. Elle demande seulement beaucoup de vigilance et d'attention. La voici :

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

« Que l'on prenne toutes les lettres de l'alphabet et qu'on en fasse cinq parties, cinq lettres dans chacune. Il y en aura une qui n'aura que 4 lettres, mais cela est sans conséquence. Que ceux qui seront désignés pour donner et recevoir les signaux, écrivent sur cinq tablettes ces cinq séries de lettres, et conviennent ensuite entre eux que celui qui devra donner le signal, lèvera d'abord deux fanaux à la fois et qu'il les tiendra levés jusqu'à ce que de l'autre côté on en ait aussi levé deux, afin que de part et d'autre on soit averti que l'on est prêt. Que les fanaux baissés, celui qui donnera le signal élèvera des fanaux par sa gauche pour faire connaître quelle tablette il doit regarder ; en sorte que si c'est la première il n'en élève qu'un, si c'est la seconde

il en élève deux, et ainsi du reste ; il en fera de même par sa droite, pour marquer à celui qui reçoit le signal, quelle lettre d'une tablette il faudra qu'il observe et qu'il écrive. Après les conventions, chacun s'étant mis à son poste, il faudra que celui qui donne le signal ait une alidade garnie de deux tuyaux, afin que celui qui le donne connaisse par l'un la droite, et par l'autre la gauche de celui qui doit lui répondre. Qu'on plante droites les tablettes proches de l'alidade, et qu'à droite et à gauche on élève un solide de dix pieds de largeur et de la hauteur d'un homme, afin que les fanaux élevés auprès fassent une lumière sûre, et qu'en les baissant on les puisse cacher. Tout cela étant disposé de part et d'autre, supposons, par exemple, qu'on veuille annoncer qu'*environ cent hommes se sont retirés chez les ennemis*, on choisira d'abord les mots qui marqueront cela en le moins de lettres qu'il sera possible, comme *Krétois cent nous ont quittés*, ce qui exprime la même chose avec moitié moins de lettres. On écrira donc cela sur une petite tablette, et ensuite on l'annoncera de cette manière : la première lettre est un k qui est dans la seconde partie et sur la seconde tablette : on élèvera donc à gauche deux fanaux pour marquer à celui qui reçoit le signal que c'est la seconde tablette qu'il doit examiner, et à droite cinq qui lui feront connaître que c'est un K, la cinquième lettre de la seconde partie qu'il doit écrire sur une petite tablette. Ensuite quatre à gauche pour marquer le R qui est dans la quatrième partie, puis deux à droite pour l'avertir que cette lettre est la seconde de la quatrième partie et ainsi de la même façon pour les lettres suivantes. Par cette méthode, il n'arrive rien qu'on ne puisse annoncer d'une manière fixe et déterminée. Si l'on y emploie plusieurs fanaux, c'est parce que chaque lettre demande d'être indiquée deux fois ; mais d'un autre côté, si l'on y apporte les précautions nécessaires, on en sera satis-

fait. L'une et l'autre méthode ont cela de commun, qu'il faut s'y être exercé avant de s'en servir, afin que, l'occasion se présentant, on soit en état, sans faire de faute, de se donner réciproquement des nouvelles de ce qu'il importe de savoir. »

Le système décrit par Polybe est très ingénieux et pourrait encore servir aujourd'hui, s'il n'était pas entré dans les habitudes d'employer l'alphabet Morse pour les communications optiques. Il a cependant l'inconvénient d'exiger deux chiffres pour la représentation d'une lettre. L'existence en français de la lettre J permet de la placer dans la case vide (la vingt-cinquième).

Le système des signaux lumineux était employé depuis un temps immémorial; les Chinois et les Persans se servaient, pour cet objet, de feux allumés de distance en distance sur des lieux élevés.

Diodore de Sicile dit que Médée et Jason usèrent de cet artifice, ce qui fait remonter cet usage à plus de 3000 ans. Pline en attribue la découverte à Sinon pendant la guerre de Troie. Eschyle dit qu'Agamemnon employa des signaux de feu pour informer Clytemnestre de la prise de Troie.

Quinte-Curce, Tite-Live, César, Hérodote, Végèce, Homère, Thucydide, Frontin, Polybe et Enée le tacticien, contemporain d'Aristote, mentionnent les signaux de feu employés de leur temps ou par les peuples qu'ils connaissaient. Nous venons de voir que Polybe les perfectionna. La flotte carthaginoise avait ses signaux marins durant la guerre punique. Ammien-Marcellin mentionne les *vexillarii* et les *speculatores* de son temps ; et quelques vieilles médailles représentent encore les pavillons et les banderolles de correspondance. Virgile a dit : « Quand il voit le ciel serein, il se tient debout vers la poupe et donne un signal lumineux », et plus loin, il rapporte qu'Agamemnon et Sinon correspondaient, l'un de son vaisseau et l'autre de la flotte.

Un emploi de feux pour la correspondance militaire se trouve longuement décrit, dans des instructions données à M. le lieutenant général, marquis de Mirepoix, commandant le corps des troupes françaises, espagnoles et génoises, dans la guerre contre l'armée sardo-autrichienne, en 1746, sous le nom de « *Table des signaux* ». La méthode consiste à placer des feux sur les hauteurs ou dans les clochers, pendant un temps déterminé à partir d'une heure fixée, à y répondre par des feux analogues, et à donner à la présence ou à l'absence de ces fanaux, des significations convenues. Le procédé est très aléatoire ; il faut des nuits suffisamment claires pour apercevoir les signaux; les évènements à prévoir ne peuvent être qu'en petit nombre, et malgré cela le plus grand doute règnera entre les correspondants au sujet des signaux négatifs, l'absence de ceux-ci pouvant être due à une cause autre que leur volonté. Néanmoins l'idée des signaux lumineux est excellente; elle a été perfectionnée par l'introduction de l'alphabet Morse, au point de pouvoir servir à toute espèce de communications, et l'application de certains systèmes cryptographiques leur assurera le secret.

Pendant le jour, la lumière artificielle est remplacée par celle du soleil ou encore par des combinaisons de signaux optiques. La marine en fait un usage constant et indispensable; tous les ordres s'y transmettent le jour par des combinaisons de signaux, de pavillons ou flammes de diverses formes et couleurs; pendant la nuit, au moyen du canon, de fusées, de fanaux, etc.; en temps de brume, on transmet les ordres par le canon, le fusil, les pétards, la cloche, le tambour, etc. Ces signaux peuvent signifier quelquefois des communications déterminées, fréquemment employées, mais aussi des lettres, ou des nombres figurant des lettres.

Nous renvoyons pour de plus amples détails aux ouvrages spéciaux. Ce que nous en avons dit suffit pour comprendre la possibilité d'envoyer des messages secrets par

cette voie, aussi bien que par la poste ou le télégraphe électrique. Ces communications rendront les plus grands services aux corps de troupes qui en feront usage, en l'absence de poste télégraphique ou téléphonique et épargneront aux estafettes une grande fatigue.

A Sparte, les *Ephores* employaient un mode fort ingénieux pour transmettre leurs ordres aux chefs militaires. Ils faisaient usage de deux baguettes ou bâtons de même longueur et de même diamètre, dont l'un était emporté par le général en chef et l'autre conservé par les *Ephores*. Plutarque, dans la Vie de Lysandre, rapporte ce procédé de correspondance de la manière suivante : « Je dois dire ce que c'est que la *scytale* à Sparte. Quand les éphores envoient un amiral ou un général commander leur armée ou leur flotte, ils prennent deux bâtons ronds d'une longueur et d'une grosseur si parfaitement égales, qu'ils pourraient s'abouter sans qu'il parût la moindre inégalité dans la superficie; ils gardent l'un de ces bâtons et donnent l'autre au général qu'ils envoient ; et ils appellent ces bâtons *scytales*. Lorsqu'ils veulent écrire quelque chose d'important et de fort secret à leurs généraux, ils prennent pour écrire une longue bande de parchemin fort étroite, qu'ils roulent autour de la scytale, ou du bâton qu'ils ont par devers eux, sans laisser le moindre petit espace entre les tours de cette bande, mais les joignant de telle sorte, que la superficie du bâton soit entièrement couverte et cachée. Ensuite, ils écrivent tout ce qu'ils veulent sur cette bande ainsi roulée; et quand ils ont écrit, ils la déroulent et l'envoient à leur général.

Le général qui la reçoit, n'y entend rien d'abord, et n'en saurait lire un seul mot, les lettres n'ayant aucune suite ni aucune liaison, et étant toutes dérangées et séparées ; mais il prend la scytale ou bâton qu'il a emporté avec lui, et roule sa lettre ou bande de parchemin sur ce bâton ; de

manière que les tours bien serrés et bien unis, remettent les lettres dans leur ordre, en les faisant cadrer ; puis la scytale rend parfaitement et présente dans son contour toute la suite de la lettre telle qu'elle a été écrite ; on appelle cette lettre *scytale*, du nom du bâton, comme ce qui est mesuré prend le nom de ce qui lui a servi de mesure. »

Malgré son ingéniosité, ce procédé ne résisterait pas longtemps à la patience du moins patient des déchiffreurs ; il ne serait pas bien difficile de faire concorder les fragments de lettres, même sans le secours d'une baguette et, défaut plus grave à notre époque, il ne se prête pas à la correspondance télégraphique. Le savant philologue italien *Scaliger* (XVI^e^ siècle) se faisait une gloire d'avoir pu déchiffrer la scytale des Grecs, mais il est aisé de comprendre que cette espèce de chiffre ne devait pas être fort difficile à deviner ; en effet, en tâtonnant un peu, on découvrait quelle était la ligne qui devait se joindre par le sens à la ligne inférieure du papier ; cette ligne, comme tout le reste, était facilement trouvée ; car si cette seconde ligne, suite immédiate du sens de la première, était, par exemple, la cinquième, il n'y avait qu'à aller de là à la neuvième, à la treizième, à la dix-septième, et ainsi de suite, jusqu'au haut du papier, et on trouvait toute la première ligne du rouleau. Ensuite, on n'avait qu'à reprendre la seconde ligne à partir du bas, puis la sixième, la dixième, la quatorzième, etc. Tout cela se saisit sans peine, en considérant qu'une ligne écrite sur le rouleau, devait être formée par des lignes partielles également distantes les unes des autres.

Nous trouvons encore dans Plutarque des renseignements très intéressants au sujet de la manière d'écrire de l'Empereur Auguste et de Jules César. Le premier ne se conformait pas exactement à l'orthographe établie par les grammairiens de son époque ; il passait des lettres et des syllabes et écrivait comme on parle, précurseur de nos

réformateurs actuels. Toutes les fois qu'il écrivait en chiffres, il mettait *b* pour *a*, *c* pour *b*, et ainsi des lettres suivantes; la lettre *z* était figurée par deux *aa*.

Jules César, pendant l'expédition des Gaules, s'accoutuma à dicter des lettres étant à cheval, et à occuper en même temps deux ou plusieurs secrétaires, méthode de travail que Napoléon renouvela pendant ses campagnes.

D'après Plutarque, César aurait inventé une sorte de chiffres fort nouveau, en mettant toujours la lettre de l'alphabet qui était la quatrième, c'est-à-dire la troisième après celle que le mot demandait. Par exemple, au lieu d'un *a*, il mettait un *d*, et au lieu d'un *d* un *g*, et ainsi de suite.

Suétone rapporte aussi que l'Empereur Auguste et Jules César employaient une correspondance secrète dans laquelle les lettres de l'alphabet étaient transposées, mais cette méthode était commune aux Grecs, aux Syracusains et aux Carthaginois. Cette invention ne peut pas être attribuée à ces potentats.

Nous avons un recueil des lettres de C. César à C. Oppius et Balbus Cornelius, chargés du soin de ses affaires en son absence. Dans ces lettres, on trouve, en certains endroits, des fragments de syllabes sans liaison, caractères isolés, qu'on croirait jetés au hasard : il est impossible d'en former aucun mot. C'était un stratagème dont ils étaient convenus entre eux: sur le papier une lettre prenait la place et le nom d'une autre; mais le lecteur restituait à chacune son nom et sa signification; ils s'étaient entendus, sur les substitutions à faire subir aux lettres, avant d'employer cette manière mystérieuse de correspondre.

Le grammairien Probus a publié un commentaire assez curieux pour donner la clef de l'alphabet employé dans les lettres de C. César.

Les procédés d'Auguste, de Jules César, et tous ceux qui reposent sur une transposition ou une inversion des

lettres ordinaires de l'alphabet, ont reçu le nom de *méthode de Jules César*. C'est le système le plus répandu, celui qui se présente le premier à l'esprit de ceux qui désirent correspondre en chiffres. Le roi Mathias de Hongrie et tutti quanti s'en servirent. Il est encore en usage aujourd'hui, avec des variantes, mais il n'offre pas la moindre résistance aux déchiffreurs.

Les Gaulois, les Saxons et les Normands inventèrent des caractères conventionnels bizarres qui ont été recueillis par les ouvrages de l'abbé Trithème, du duc Sélénus et des autres polygraphes du XV^e^ et du XVI^e^ siècles. Ils nous ont aussi conservé ceux d'Alfred le Grand, roi d'Angleterre (849-901), et ceux qu'avaient adoptés Charlemagne et ses agents. Les Irlandais usaient de chiffres particuliers nommés *oghanis* qui étaient une espèce de sténographie.

Le moyen-âge inventa un grand nombre d'alphabets de convention pour correspondre secrètement et surtout pour la confection des écrits ou manuscrits que le profane ne devait pas lire. On traduisait chaque lettre de l'alphabet ordinaire par un signe conventionnel de nature quelconque, lettre, chiffre, nombre, signe algébrique, astronomique, etc.: c'est un simple changement de nom des lettres.

Raban Maur, archevêque de Mayence (au VI^e^ siècle) cite deux exemples d'un système dont on se servait de son temps.

Dans le premier, les voyelles sont représentées par des points et on laisse subsister les consonnes.

i = . a = : e = :. o = :: u = :.:

Ainsi : « La place est fortifiée » se traduisait par le cryptogramme suivant: L: pl:c:. :.st f:: rt.f. :. :.

Dans le second, les voyelles sont figurées par les consonnes qui les suivent immédiatement :

a par b — e par f — i par k — o par p — u par v.

Ainsi la phrase précédente serait chiffrée:

Lb plbcf fst fprtkfkff.

Ces deux alphabets, signalés par les Bénédictins, étaient employés dès le IV^e^ siècle de notre ère. On comprend combien le déchiffrement devait en être facile pour le déchiffreur le moins habile.

L'*écriture tétragrammique* consistait dans la disposition des lettres de l'alphabet en croix, dans un ordre convenu qui constitue la clef.

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

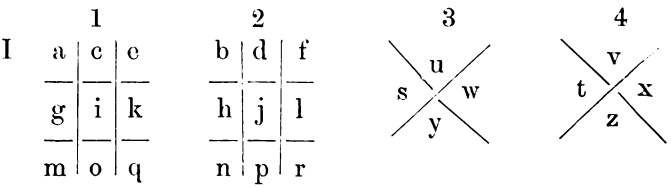
On représentait chaque lettre par un des signes __|, |__ ¯|, |¯, dans lequel on indiquait le rang de la lettre par un chiffre, ou par le nombre de points indiqués par le rang du chiffre.

On disposait aussi les lettres de l'alphabet sur deux lignes, en supprimant le j et le w, de la manière suivante:

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

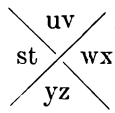
et l'on remplaçait chaque lettre du texte clair par celle qui se trouvait en regard d'elle, dans l'autre ligne.

L'écriture dite *franc-maçonnique* est une variante du système tétragrammique. Voici trois systèmes de cette espèce :



II

aj	bk	cl
dm	en	fo
gp	hq	ir



III

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

Les caractères sont représentés par un des signes _|, |_|, |_, ¯|, |¯|, |¯, ¯|, |¯|, |¯, >, ∨, <, ∧, dans lesquels on inscrit éventuellement le nombre de points, ou le chiffre qui correspond au rang de la lettre.

Dans le graphique I, les lettres inscrites dans les figures paires seules sont distinguées par un point.

A partir du XV^e siècle on fit beaucoup usage des systèmes dus à l'abbé Thrithème et à ses commentateurs et élèves.

Voici deux méthodes qui appartiennent toujours aux modes moyennâgeux.

Jean Caramuel (1635), dans son ouvrage sur la cryptographie, expose un alphabet de 24 lettres representées par des voyelles de la manière suivante:

a b c d e	f g h i l	m n o p q	r s t u x	y z & *c*
à è ì ò ù	â ê î ô û	ä ë ï ö ü	á é í ó ú	ỳ ŷ ÿ ý

Il indique encore un modèle de cryptographe, où chaque série de deux lettres ou signes du texte est représenté par un mot. C'est en quelque sorte l'instrument dû à Porta sous le nom de « *Scripti et Clavis* ».

Voici un fragment de l'*Ave Maria* de l'abbé Trithème, employé fréquemment, mais trop compliqué pour que sa vogue se maintînt longtemps: (1)

(1) Les notes historiques concernant les travaux cryptologiques de l'abbé Trithème et de ses commenteurs, seront repris plus tard, lorsque nous aborderons les systèmes par substitution.

Il consistait en colonnes verticales comprenant chacune, dans l'ordre naturel, les lettres de l'alphabet; en face de chaque lettre se trouvaient un ou plusieurs mots empruntés à l'Ave Maria, d'où le nom du système.

Pour chiffrer un texte clair, on représentait successivement chacune de ses lettres par le ou les mots qui, dans chacune des colonnes de même rang que la lettre, étaient en regard de celle-ci.

Voici d'après le capitaine Josse(1) la traduction française d'une série de l'alphabet.

I	II	III
A Je te salue	A Marie	A pleine
B Belle	B Pallas	B ornée
C Vole	G Isis	C dotée
D Accoins	D Astarté	D trône
E Salut	E Vénus	E merveille
F Parais	F Thétis	F parée
G Descends	G Flore	G douée
H Ecoute	H Eleusine	H astre
I ô.....	I Uranie	I source
J Auguste	J Vesta	J remplie
K Hélas	K Pomone	K couronnée
L Chaste	L Cypris	L embellie
M Céleste	M Cybèle	M sanctuaire
N Divine	N Hèbé	N assemblage
O Oh !	O Egérie	O miracle
P Sublime	P Cythérée	P décorée
Q Puissante	Q Aphrodite	Q parfum
R Tendre	R Diane	R éclatante
S Viens	S Astrée	S vase
T Sensible	T Thémis	T étoile
U ô toi	U Junon	U couronne
V montre-toi	V Iris	V brillante
X Ecoute-nous	X Cérès	X autel
Y Entends-nous	Y Minerve	Y étincelant
Z Exauce-nous	Z Rehéa	Z Olympe

(1) Revue maritime et coloniale, février 1891.

IV	V	VI
A de grâces	A le Seigneur	A est
B d'attraits	B un Dieu	B existe
C de sagesse	C le désir	C domine
D d'appas	D la félicité	D sourit
E de vertus	E la paix	E respire
F d'amour	F l'amour	F se plaît
G de chasteté	G l'avenir	G réside
H de science	H le bien-aimé	H erre
I d'intelligence	I le génie	I veille
J de beauté	J le bonheur	J intéresse
K de savoir	K Zéphire	K vit
L de piété	L le plaisir	L habite
M de pudeur	M Jupiter	M renaît
N de candeur	N la vertu	N brille
N de charmes	O la volupté	O règne
P de lumières	P Osiris	P soupire
Q de louanges	Q la raison	Q parle
R de perfections	R l'amitié	R folâtre
S de plaisirs	S l'allégresse	S étincelle
T de justice	T Phébus	T se délecte
U de volupté	U la sagesse	U brûle
V de sainteté	V la bienfaisance	V s'embellit
X de prudence	X la joie	X reste
Y de gloire	Y Apollon	Y badine
Z de constance	Z un ange	Z se joue

Ainsi par exemple la phrase: *Rendez la place* serait chiffrée.

R = tendre, E = venus, N = assemblage, D = d'appas, E = la paix, Z = se joue, L = chaste, A = Marie, P = décorée, L = de piété, A = le Seigneur, C = domine, E = le salut. D'où le cryptogramme:

« Tendre Vénus, assemblage d'appas, la paix se joue chaste; Marie décorée de pieté, le Seigneur domine le salut. »

Les colonnes peuvent être disposées dans un ordre convenu.

Ce procédé fournissait des textes indéchiffrables pour ceux qui ne possédaient pas la table de l'abbé; mais actuellement un tel secret ne servirait pas à grand'chose! L'inconvénient le plus grave était l'étendue hors de toute proportion du texte chiffré comparativement au texte clair.

Sa transmission par télégramme serait très onéreuse.

Le défaut de sécurité des méthodes analogues à celle de Jules César ne tarda pas à être reconnu, et l'on chercha à y remédier dès le XVI[e] siècle; M. Ch. Fr. Vesin Romanini, dans *La Cryptographie dévoilée*, qu'il publia en 1840, reproduit une dépêche chiffrée, écrite le 13 avril 1519 par P. de Nassau à Marguerite d'Autriche, gouvernante des Pays-Bas, et conservée dans les archives lilloises, et dont il put découvrir le sens.

Les caractères de ce cryptogramme sont empruntés à l'alphabet grec, à la série des chiffres arabes, et à celle des signes employés dans les mathématiques (+, —, =, ×, etc.); mais ce n'est pas ce qui en fait l'originalité; ce qui est surtout digne d'être noté, c'est que les lettres les plus fréquemment employées sont représentées par plusieurs signes différents, l'*e* par quatre signes, l'*n* et l'*i* par trois, l'*a*, le *c*, l'*m*, etc, par deux, et les lettres redoublées, *rr*, *ss*, par des caractères particuliers.

François II (1559-1560) employait un alphabet cryptographique, où non seulement les lettres étaient représentées par plusieurs caractères différents, mais où, de plus, certains caractères particuliers représentaient les mots usuels, tels que: vous, que, qu'il, tout, faire, pour, bien, dont, est, je, etc. Outre ces complications, des caractères nuls déguisaient principalement le commencement et la fin du texte.

Cette manière de procéder a été celle des rois de France jusqu'à Louis XIV.

Lord Bacon (1560-1616) faisait usage d'un alphabet de convention, composé de 25 signes empruntés aux 32 combinaisons cinq à cinq avec répétition des deux lettres *a* et *b*. A son époque, le célèbre philosophe considérait son système comme indéchiffrable. Il ne l'était pas sous la forme qui lui était donnée, mais avec certains perfectionnements, le procédé a donné naissance à un principe *que*

nous avons développé et transformé en méthode complètement indéchiffrable. Nous l'exposerons plus loin.

Au XVII^e^ siècle, *Galilée*, ayant aperçu en 1610 les phases de Vénus, et voulant annoncer sa découverte, tout en la gardant encore secrète, le fit sous cet anagramme composé en dehors de toute règle:

Hæc immatura a me jam frustra leguntur o. y.

(Ces choses non mûries, cachées aux autres, je les ai lues); dont les lettres placées dans un autre ordre donnent:

Cynthiæ figuras emulatur mater amorum.

(La mère des amours imite les phases de Diane.)

Huyghens (1629-1699), après la découverte des anneaux de Saturne, en fit part au monde savant sous le cryptogramme suivant: aaaaaaa, ccccc, d, eeeee, g, h, iiiiiii, llll, mm, nnnnnnnnn, oooo, pp, q, rr, s, ttttt, uuuu.

Trois ans plus tard, il en donnait la traduction ci-après:

Annulo ungitur tenui, plano, nusquam cohærente, ad eclipticam inclinato (Il est entouré d'un anneau plan, mince, n'adhérant à l'astre en aucun de ses points et incliné vers l'écliptique.)

A dater de la Renaissance, la cryptographie devint un art, et elle acquit une grande importance dans les relations diplomatiques et militaires de cette époque, où le besoin de moyens occultes de communication se faisait de plus en plus sentir, au milieu des intrigues diplomatiques qui se croisaient en tous sens. On imagina une multitude d'écritures secrètes, qu'on désigna sous la dénomination générique *d'écritures en chiffres*, ou simplement *chiffres*, bien qu'elles ne se composassent pas toujours des signes de l'arithmétique. Quelques-unes d'entre elles sont restées fort longtemps dans la pratique des chancelleries. Toutefois les principaux personnages ne se contentèrent pas toujours des méthodes généralement employées; ils se créèrent souvent des chiffres particuliers

dont la lecture n'était possible qu'à leurs confidents. Ainsi, dans certaines circonstances, le cardinal de Richelieu faisait usage d'une écriture composée de traits, de lettres et de chiffres arabes. Un trait signifiait un mot tout entier ou une ligne de Saint Augustin; la page, la ligne et le mot étaient indiqués par des chiffres placés au-dessous. Nous citerons encore les cartes mystérieuses dont se servait, sous Louis XVI, le comte de Vergennes. Elles offraient, en caractères ordinaires, les instructions qu'il semblait vouloir donner; mais le sens réel de ces instructions était indiqué par la couleur et la forme du papier, ainsi que par des figures qui semblaient être de simples ornements.

François Ier et ses successeurs se servaient d'un chiffre pour leurs correspondances.

Le célèbre mathématicien *Viète* (1540-1603) employé par François Ier et ses successeurs (1560-1616), lord Bacon et l'évêque Wilkins, rapportaient l'art d'écrire en chiffres à la grammaire qui, disaient-ils, « comprend dans sa latitude, l'art d'exprimer la pensée, non seulement par la parole et par l'écriture, mais encore par les signaux, par les gestes, par tous les moyens qui ont été imaginés. Pourtant les personnes qui s'en servent le plus souvent, sont bien loin de l'étudier comme une science qui a sa certitude et ses théories, d'où l'on pourrait déduire un grand nombre de conséquences utiles; pour elles, ce n'est qu'un art qu'il leur est indispensable de pratiquer ; aussi emploient-elles des combinaisons qu'un déchiffreur exercé parvient toujours à traduire.

Trithème et Porta étaient bien fiers de la découverte de leurs systèmes que tous les souverains adoptèrent avec empressement ; mais Viète montra la fragilité de ces procédés. *Wallis* (1616-1703) vint bientôt prouver aussi combien était peu fondée l'opinion qui regardait comme indéchiffrables les chiffres employés à cette époque.

Scaliger avait une grande sagacité pour interpréter les textes secrets; ce talent avait commencé sa fortune en lui assurant de nombreux avantages de la part de la Maison de Hanovre, au service de laquelle il avait mis sa science. Cependant dès lors, d'après l'opinion de Bacon et de Wilkins, qui avaient consciencieusement étudié cette branche des connaissances humaines, il paraissait possible d'imaginer un système entièrement indéchiffrable. Ils pensaient aussi qu'il n'appartient pas à tous de pouvoir se faire déchiffreur, et que, malgré les données qu'on avait sur le déchiffrement, cet art demande une étude particulière et suivie. Ces idées n'ont pas cessé d'être vraies.

Nous avons déjà exposé le principe du système de Bacon; celui de *Porta*, à son époque (1563) fut aussi regardé par son auteur comme indéchiffrable. L'événement montra qu'il s'était trompé sur ce point.

Néanmoins son procédé peut être considéré comme le fondement de la cryptographie moderne, en ce sens que ce n'est qu'à partir de sa méthode qu'on chercha à édifier la cryptographie sur des bases réellement rationnelles.

Le diplomate français *Blaise de Vigenère* (1589) étendit le principe de Porta en augmentant le nombre d'alphabets employés, afin d'accroître la résistance du système à clef littérale variable.

Les soi-disant perfectionnements ultérieurs apportés à la méthode du chiffre carré de Vigenère, sous les noms de « allemand », « anglais » (de Beaufort), et « français » (St Cyr), belge et ses succédanés (comte de Gronsfeld), rentrent dans cette méthode. Même les systèmes à alphabets intervertis, régulièrement, ou irrégulièrement, à clef, simple ou multiple, variable ou continue par parties, procèdent de leurs devanciers congénères, et n'offrent en général, pas beaucoup plus de résistance au déchiffrement qu'eux, tout en étant cependant un progrès. Jusque dans

ces derniers temps même, ils étaient considérés comme indéchiffrables, en principe, ou du moins, on croyait qu'ils opposaient aux chercheurs des difficultés matérielles telles qu'on pouvait admettre qu'ils étaient presque toujours illisibles. (1)

Monsieur Kerckhoffs, dans l'étude parue dans le « Journal des Sciences militaires » en 1883, a démontré la profonde erreur de ceux qui professaient cette croyance, et il a formulé des règles générales pour le déchiffrement des systèmes dits « *à clef variable* ».

Le capitaine d'artillerie Valério, dans son remarquable travail sur les « Procédés de déchiffrement » publié par le Journal des Sciences militaires (1893-95) a achevé d'établir les méthodes de déchiffrement sur des bases vraiment mathématiques, qui ont engagé définitivement la cryptographie dans la voie scientifique, en réduisant à un minimum l'*art* proprement dit du déchiffreur, c'est-à-dire la sagacité.

C'est précisément l'étude des modes de déchiffrement qui nous a permis d'éviter les écueils qui donnent prise au chercheur.

A partir de François Ier, avons-nous indiqué, la cryptographie commença à prendre une place importante dans les affaires diplomatiques, et dans les correspondances relatives aux menées et aux intrigues qui marquèrent cette époque.

Nous citerons ici en passant la célèbre et intéressante lettre de Madame de St André au Prince de Condé, emprisonné à Orléans après la conjuration d'Ambroise. (1560)

C'est un système d'écriture à disposition convenue, dont le sens se trouve par l'ordre dans lequel on doit lire les mots ou les lignes.

Cette lettre était disposée ainsi:

Croyez-moi, prince, préparez-vous à

(1) Lewal-Tactique des renseignements — page 76.

la mort. Aussi bien vous sied-il mal de
vous défendre. Qui veut vous perdre est
aussi de l'Etat. On ne peut rien voir de
plus coupable que vous. Ceux qui
par un véritable zèle pour le roi,
vous ont rendu si criminel, étaient
honnêtes gens et incapables d'être
subornés. Je prends trop d'intérêt à
tous les maux que vous avez faits en
votre vie, pour vouloir vous taire
que l'arrêt de votre mort n'est plus
un si grand secret. Les scélérats,
car c'est ainsi que vous nommez ceux
qui ont osé vous accuser, méritaient
aussi justement récompense, que vous
la mort qu'on vous prépare: votre seul
. . . . . .
mérite vous a fait des ennemis,
et que ce ne sont pas vos crimes
qui causent votre disgrâce. Niez
avec votre effronterie accoutumée,
que vous ayez eu aucune part à
tous les criminels projets de
la conjuration d'Ambroise. Il n'est pas
comme vous vous l'êtes imaginé, im-
possible de vous en convaincre. A
tout hasard, recommandez-vous à
Dieu. »

Mais le sens réel s'obtenait en ne lisant que les lignes impaires 1, 3, 5, etc, ce qui donnait alors:

Croyez-moi, prince, préparez-vous à
vous défendre. Qui veut vous perdre est
plus coupable que vous. Ceux qui
etc. etc.

Nous reconnaissons ici en somme le procédé des dés percés de trous, ou des grilles.

Dans l'exemple ci-dessus, c'est encore un jeu d'esprit assez difficile, qu'il n'est pas donné à tout le monde d'employer avec succès.

La correspondance de Henri IV avec Maurice le Savant, Landgrave de Hesse, éditée en 1840 par Monsieur de Rommel, directeur des archives de l'Etat à Cassel, et ayant trait aux projets d'abaissement des Maisons d'Autriche et d'Espagne, témoigne de ce que, sous ce monarque, l'usage de la cryptographie avait pris une grande extension.

Les faits politiques et militaires qui marquent les règnes de Louis XIII et de Louis XIV, les procédés de gouvernement de Richelieu et de Mazarin, la correspondance de Louvois, les mémoires de Catinat qui contiennent de nombreuses lettres chiffrées, les récompenses décernées aux déchiffreurs habiles, nous montrent que nous ne sommes plus au temps où Viète était dénoncé comme sorcier, mais que l'art de déchiffrer les écritures secrètes a acquis une importance considérable au point d'être élevé à la hauteur d'une science d'Etat. Cette grande faveur lui fut continué jusqu'à la Révolution de Juillet, aussi longtemps que l'absence de préjugés et de probité politique des gouvernants, amena ceux-ci à se servir de la violation du secret des lettres, d'espions, comme moyens de gouvernement.

Aux armées, c'est aussi à partir du XVI^{e} siècle qu'on commence à trouver trace de dépêches chiffrées, pour la transmission régulière des ordres aux chefs d'armée et aux généraux. Cependant l'emploi de la cryptographie y fut moins étendu, moins constant qu'en diplomatie.

Sous l'Empire, les communications et les relations entre les différentes parties de l'armée se faisaient généralement par dépêches chiffrées. Il y avait un *grand chiffre* et un *petit chiffre*.

Voici quelques exemples empruntés à l'histoire des dernières campagnes de Napoléon, par le Baron Fain, secrétaire de l'Empereur. (1)

Lettre de l'Empereur au Major général

Le . . . . 1812.

. . . . . .

Si la route cesse un moment d'être sûre, le Duc de Bassano est autorisé à alléger les courriers, même ceux de Paris, de tout ce qui ne doit pas être compromis et à suppléer au plus pressé par quelques lignes de chiffres.

Du même au même

Wilna, 7 Juillet 1812.

Mon Cousin, faites connaître par une lettre en chiffres au Roi de Westphalie la position du Prince d'Eckmühl, hier 6 juillet.

Du même au même

Moscou, le 18 octobre 1812.

Ayez soin de donner au duc de Trévise un chiffre, afin que la correspondance avec lui puisse être libre et sûre.

Borowsk, le 24 octobre 1812.

Mon Cousin, écrivez au duc de Bellune *en chiffres*, puisqu'il ne recevra pas de lettre avant le 26, et qu'alors il aura vu le général Nansouty.

. . . . . .

Ajoutez au duc de Bellune, *en clair*, que l'armée est réunie à Borowsk; que Moscou a été évacué après avoir fait sauter le Kremlin, et que l'armée se dirige sur Kalouga;

(1) Manuscrits de 1812-1813.

que la province de Kalouga est une des plus abondantes de la Russie, et qu'en effet nous sommes ici dans une grande abondance de tout.

Borowsk, le 26 octobre 1812.

Ecrivez au duc de Bellune à peu près la même chose sur le combat et en chiffres.

Pendant la retraite, l'arrivée d'un paysan expédié secrètement de Wilna, est annoncée. Il est porteur de dépêches chiffrées du duc de Bassano. Ce paysan se fait reconnaître pour M. A....., gentilhomme polonais. Tandis qu'on l'accueille et qu'on l'interroge, la dépêche est déchiffrée, et l'Empereur va savoir à quoi s'en tenir sur ce qu'est devenu Schwarzenberg.

Campagne de 1813. A Stuttgard, c'est le roi de Wurtemberg lui-même qui est le correspondant de Napoléon. Un chiffre particulier couvre, entre ces deux souverains, le secret de leur communications directes.

Les renseignements les plus importants arrivent par cette voie. L'empereur Napoléon y trouve de nouveaux avis sur les intrigues de l'Autriche, sur les séductions dont l'armée bavaroise est l'objet, et sur les intelligences que le Tügenbund procure à la coalition dans les états-majors, et jusque dans les cabinets de la confédération du Rhin.

Lettre de l'Empereur au Major général

Löwenberg, le 23 Août 1813.

Ecrivez au duc de Tarente que je donne ordre à mon grand-écuyer d'établir une estafette de mes postillons, depuis Löwenberg jusqu'au lieu où je serai, laquelle étant servie par mes chevaux, rendra les communications extrêmement rapides par Gœrlitz et la position où je me trouverai.

Donnez au duc de Tarente le petit chiffre, pour remplacer celui qui, probablement a été pris. Comme ce chiffre est

facile à copier, le duc de Tarente l'enverra aux généraux sous ses ordres. (1)

Le chiffrement de la correspondance n'était pas délaissé non plus pendant les guerres de l'Empire, à preuve le message par lequel Napoléon prescrit de lui faire parvenir les lettres de l'archevêque de Sélencie, envoyées de Rome à Dresde; il ajoute: « On a trouvé ici le chiffre, de manière qu'on les lit ici comme une écriture courante, mais il faudrait les laisser continuer leur route en les copiant textuellement. »

Cependant vers la fin de l'Empire, l'emploi de la correspondance chiffrée tomba peu à peu en désuétude. Pendant la campagne de 1814, toutes les dépêches étaient expédiées en langage clair, ce qui ne contribua pas peu à l'invasion, et au succès des alliés.

Il en fut à peu près de même en 1815. Ainsi, nous voyons Davoust, ministre de la guerre, demander à son collègue des Affaires étrangères, sous la date du 2 mai 1815, deux chiffres pour la correspondance militaire: « Le grand chiffre servira aux commandants des corps d'armée et je désirerais en avoir une vingtaine d'exemplaires. Quant au petit chiffre, destiné aux commandants des places fortes, une centaine d'exemplaires serait nécessaire. »

Voici quelques extraits des Maximes Napoléonniennes du général Grisot (2) qui prouvent l'importance que Napoléon attachait au langage chiffré.

« Rendez-vous près du prince de Neuchâtel pour prendre des renseignements sur les chiffres qui existaient à la dernière campagne, et savoir si le vice-roi en a un. Comme je crains que l'ennemi n'ait ces chiffres, je désire les changer. Je désirerais avoir deux espèces de chiffres, un chiffre de l'état-major de l'armée avec les différents commandants

(1) Napoléon au tribunal de César, par Jomini.
(2) Journal des sciences militaires. février 1899.

des corps, un chiffre de moi avec les commandants de l'armée, pendant que je suis absent.

Vous m'apporterez le chiffre qu'aura le vice-roi, puisqu'on sera obligé de chiffrer beaucoup à cause des partis de Cosaques.

Assurez-vous que le duc de Bellune a un chiffre, afin de pouvoir écrire dans les lettres quelques mots en chiffre, qui empêchent que ces lettres ne soient utiles à l'ennemi, dans le cas où elles tomberaient dans ses mains; cette mesure est indispensable, vu la quantité de Cosaques qui vont se trouver partout.

Je n'ose vous écrire, même en chiffres, parce qu'il y a à Paris et à Londres des hommes qui déchiffrent tout, mais soyez bien persuadé que je ne vous perds pas de vue. »

Dès 1861, le Major prussien Kasiki avait publié une brochure traitant des procédés de lecture des chiffres à double clef.

Pendant la guerre de 1866, les Prussiens, comme les Autrichiens, faisaient usage de dictionnaires chiffrés. L'ouvrage du grand Etat-major autrichien contient une dépêche prussienne, composée au moyen de ce système, et qui fut déchiffrée par les Autrichiens.

Pendant la campagne de 1870, nous trouvons les traces officielles suivantes d'emploi de la cryptographie aux armées:

A la date du 20 Juillet, le major général de l'armée du Rhin, envoie aux commandants de corps le nouveau chiffre, et annonce que le chiffre dont on s'est servi jusqu'à présent, doit être réservé pour les relations avec les autorités de l'intérieur.

Le 21 Juillet, le commandant du 5e Corps de l'armée du Rhin signale « que le chiffre spécial destiné à la transmission des dépêches est très incommode, et ne renferme aucun

des mots techniques de la guerre. Il faudrait qu'il fût changé. » (1)

Le 23 Août, le commandant de la division territoriale de Châlons écrit au Ministre de la guerre: «Par erreur, mon chiffre a été envoyé avec mes archives à Château-Thierry. Impossible de traduire la dépêche. Prière de l'envoyer en clair avant 8 heures du matin, moment auquel je pars pour Rheims, d'après les ordres du maréchal Mac-Mahon » (2) Après la bataille de Wœrth, le major général de l'armée du Rhin demande au commandant du 1er corps, de lui faire connaître « s'il y a lieu de supposer que le chiffre qui était entre ses mains a pu tomber au pouvoir de l'ennemi » et lui fait parvenir en même temps un nouveau chiffre.

Pendant le siège de Paris, le gouverneur de Paris fit usage de correspondances chiffrées. On lui attribue même, mais à tort, l'invention d'un nouveau chiffre.

Du côté allemand aussi, la cryptographie était employée. Un déchiffreur habile était attaché au Grand quartier général allemand.

De part et d'autre, on recourait aux dictionnaires chiffrés.

Les relations de la campagne franco-allemande rapportent l'incident suivant, arrivé au général Werder: Ayant reçu, le 8 janvier 1871, un télégramme du Grand quartier général prussien, il ne put le déchiffrer, parce que le dictionnaire se trouvait dans une voiture éloignée.

Pendant la guerre turco-russe, l'usage des chiffres se réduisait toujours à l'emploi de dictionnaires.

A. COLLON

Lieutenant d'artillerie adjoint d'Etat-Major.

(A suivre).

(1) Extrait du journal historique du 5e Corps français.

(2) Pierron. Les méthodes de guerre actuelles.

ETUDE

SUR LA

CRYPTOGRAPHIE

Son emploi à la guerre et dans la diplomatie. *

CHAPITRE II. — CLASSIFICATIONS.

1° PRINCIPES DU CHIFFREMENT ET DU DÉCHIFFREMENT.

En cryptographie, il y a trois procédés généraux de chiffrement : monolittéral, monosyllabique et polysyllabique ou idéographique.

Le premier, qui est le plus ancien, s'est présenté tout naturellement à la pensée des cryptologues, puisqu'il permet la représentation des idées secrètes par les éléments propres du discours. Ce sont les systèmes littéraux ou numéraux obtenus par la transposition ou l'interversion des lettres du texte clair, ou par la substitution de lettres ou signes numériques et autres, aux lettres du langage clair, c'est-à-dire l'emploi d'alphabets conventionnels.

De là, deux classes de systèmes généraux, comme suit :

Première classe { *a* système par transposition / *b* système par interversion } des lettres du texte clair.

Les lettres sont brouillées, dispersées, mais elles gardent

(*) Suite. (voir Tome II de la 24e année.)

leurs noms; c'est la méthode des anagrammes si connue par les problèmes soumis au public par les journaux illustrés.

Seconde classe	*a* système littéral	substitution de lettres	aux lettres du texte clair
	b système numéral	substitution de chiffres	
	c système par signaux	substitution de signes	

C'est la transposition ou l'interversion appliquée aux *lettres de l'alphabet*, contrairement aux systèmes de la première classe où ces opérations s'adressent aux lettres du *texte même*. Dans cette seconde classe, l'ordre alphabétique des signes est donc remplacé par un ordre conventionnel : ce sont des alphabets de convention.

Le deuxième procédé général est le chiffrement du texte par syllabes.

Il comprend deux classes : 1° On peut chiffrer un groupe de deux lettres quelconques ; le nombre maximum de séquences est celui des combinaisons avec répétition de 26 lettres, deux à deux ou $26^2 = 676$.

2° On peut représenter tous les sons de la langue, ou du moins, tous les groupements prononçables possibles, quel que soit le nombre de leurs lettres, par environ 3, 4, 5 mille groupes, en français.

Dans le premier cas, une séquence pourra être représentée par 3 chiffres; celui indiquant la colonne et les deux chiffres nécessaires pour mentionner le rang dans la colonne. Dans le second cas, il faut au moins 4 chiffres (30, 40, 50 séries de 100 figures), pour chiffrer un groupe du texte.

Si l'on adopte pour chaque groupe plusieurs représentants chiffrés pour diminuer les répétitions, on peut au moyen de quatre chiffres obtenir 10,000 figures.

Le troisième procédé général comprend trois classes, savoir :

1re classe, système des dictionnaires littéraux.

2e classe, système des dictionnaires numéraux,

3e classe, système des mots conventionnels (stéganographie).

Dans le système polysyllabique littéral, les mots sont toujours figurés par un groupe de trois lettres, puisque les combinaisons à répétition de 26 lettres, trois à trois, produisent $26^3 = 17576$ groupes, nombre suffisant pour représenter les principaux mots et expressions de la langue.

Dans le système numéral, un dictionnaire comportant 10.000 mots exige des séries de quatre chiffres pour leur figuration ; un dictionnaire de plus de 10.000 mots, jusque 100.000 mots, nécessite des nombres de cinq chiffres. Si le dictionnaire se réduit à un nombre de mots ou d'idées inférieur à mille, il y a possibilité de représenter chaque objet par trois chiffres seulement.

On peut rattacher au procédé idéographique, celui où l'on a adopté des mots de convention comme signes représentatifs des lettres, des syllabes ou des mots.

La classification précédente, établie uniquement au point de vue abstrait, se transforme quelque peu, si l'on considère cette énumération au point de vue militaire et diplomatique. Nous sommes conduits alors à faire deux grandes catégories :

1° Celle comprenant les systèmes *qui ne font pas usage* de livres ou documents, appareils, etc., *exigeant le secret.*

2° Celle qui renferme les systèmes *faisant usage* de livres, documents, appareils, etc., *exigeant le secret.*

La première catégorie renferme les systèmes à clef proprement dite, littérale ou numérique, et les systèmes reposant sur une clef convention mnémonique, sans intervention de clef littérale ou numérique.

La deuxième catégorie englobe, en général, les systèmes monosyllabiques et polysyllabiques, les appareils cryptogra-

phiques ; enfin les méthodes qui rentrent dans le système par signaux sténographiques (c) de la seconde classe du procédé général alphabétique.

Les *procédés de déchiffrement* sont basés sur les procédés de chiffrement. Si une loi a présidé au chiffrement (système à clefs) la découverte de cette loi conduira au déchiffrement.

Si aucune loi n'a guidé le chiffreur, par exemple dans les dictionnaires chiffrés ou les alphabets conventionnels par signaux, la recherche de la méthode de déchiffrement paraît moins aisée ; mais certains procédés spéciaux conduisent encore au résultat cherché, parce que la constitution d'un alphabet ou d'un dictionnaire comporte en soi l'existence de lois analogues à celles qui distinguent la langue elle-même, et permettent ainsi le déchiffrement, plus rapidement souvent que dans un système à clef proprement dite, même si le dictionnaire ou l'alphabet sont tout à fait arbitraires.

La répétition ou la fréquence des signes d'un texte est la base des investigations du déchiffreur. Elles servent aussi de contrôle à toute hypothèse.

Si le chiffreur a fait usage d'un chiffre où tous les signes ont une fréquence identique, où l'on aura multiplié les homophones, ou bien encore, si l'on fait disparaître les répétitions, le cryptologue, manquant de points d'appui et de jalons pour sillonner la voie à suivre, rencontrera des difficultés considérables, insurmontables même, en raison directe du soin qu'on aura mis à dissimuler les fréquences.

Quoi qu'il en soit, dans les recherches, la valeur attribuée à une découverte, ne peut être admise *avec certitude* que lorsque l'application du principe des répétitions se traduit logiquement par les mêmes signes, lettres, syllabes ou mots.

La première chose à connaître est donc la langue véhiculaire de la correspondance, car les lois linguistiques à invoquer dépendent de cette connaissance.

Viète et après lui, Vesin ont prétendu que la connaissance de la langue n'était pas nécessaire au déchiffreur ; cependant, il est incontestable que cette connaissance, ou tout au moins celle des particularités linguistiques qui distinguent les idiomes, faciliteront grandement la tâche du cryptologue.

De nombreux indices permettent de déceler la langue employée. Si aucune indication extérieure ne vient révéler le dialecte des correspondants, une étude préliminaire du texte s'impose afin de le déterminer.

Au point de vue militaire cette question a moins d'importance, puisqu'en général l'ennemi ne peut guère envoyer de messages que dans sa propre langue.

La deuxième question à résoudre est la détermination du procédé général, et subsidiairement du système et de la méthode employés pour cryptographier une dépêche.

Si l'on a entre les mains une partie du texte clair, la comparaison du nombre de signes des deux textes sera une indication précieuse; mais le plus souvent on ne possédera pas ce renseignement, et l'on devra recourir à d'autres méthodes d'investigation que nous allons examiner.

La première chose à faire est de compter le nombre de signes de chaque espèce, lettres ou chiffres.

I. Le cryptogramme ne se compose que de lettres.

a. Si une ou plusieurs lettres ont une fréquence supérieure aux autres, on a un indice de l'emploi d'un système monoalphabétique.

b. Si les lettres dominantes sont celles qui ont la plus grande fréquence dans la langue, on a la preuve qu'on se trouve devant une méthode à transposition ou interversion des lettres du texte clair.

c. Si les lettres dominantes ne sont pas celles qui ont le *chiffre fréquenciel* le plus élevé, on peut en conclure qu'on a affaire à un système par substitution.

d. Si au lieu de lettres isolées, ce sont certaines séries de deux ou trois lettres qui se répètent fréquemment, et qui sont distantes entre elles d'un multiple de deux ou trois, on est amené à admettre le chiffrement par groupes binaires ou ternaires.

Ces groupements peuvent être produits par un dictionnaire littéral, binaire ou ternaire, ou par un système par substitution où chaque lettre du texte clair est représentée par une combinaison de deux ou trois lettres. Les dictionnaires à groupements binaires alphabétiques sont exceptionnels, à cause du petit nombre de représentants qu'ils peuvent fournir ($26^2 = 676$).

e. Lorsque le texte chiffré renferme plusieurs lettres à fréquence élevée semblable, on attribuera le cryptogramme au chiffrement polyalphabétique.

f. Si ce nombre de lettres à fréquences semblables est petit, on se trouve généralement en présence d'un système à clef périodique courte.

g. Si ce nombre est assez grand, on a affaire à un système à clef périodique longue ou à un système à clef variable.

h. Si la fréquence de toutes les lettres de l'alphabet est identique ou à peu près, on est en présence d'un système à clef continue, ou basé sur le principe d'un nombre de signes de substitution (pour chaque lettre), proportionnel au chiffre fréquenciel.

II. Le cryptogramme ne contient que des chiffres. Le système employé est évidemment celui par substitution.

a. Si le nombre de signes est égal à 26 et si un, deux ou trois d'entre eux ont une fréquence supérieure aux autres, on a affaire à un système monoalphabétique.

b. Si certains groupes de chiffres ont une fréquence supérieure aux autres, et se répètent, à des intervalles mul-

tiples du nombre de chiffres de la série, c'est un système à répertoire, dont l'espèce est indiquée, par la différence entre les nombres extrêmes contenus dans le texte.

c. Si, au lieu de certains nombres isolés, quelques-uns ont un maximum fréquenciel identique, ou à peu près, on se trouvera, comme pour les procédés littéraux, en face d'un système à clef périodique courte ou longue, ou variable suivant les cas.

d. Si la fréquence de tous les nombres est semblable ou à peu près, le cryptogramme provient d'un système à clef continue, ou d'une méthode où le nombre de signes employés est proportionnel à la fréquence respective de chacun d'eux.

Ces notions générales exposées, ce sont les particularités des langues qui vont permettre au déchiffreur d'appliquer les principes qui feront reconnaître les procédés de chiffrement employés, et trouver les méthodes de déchiffrement à essayer pour réduire les cryptogrammes.

Outre la connaissance approfondie de ce que nous nommerons la partie matérielle, scientifique du chiffrement et du déchiffrement des écritures secrètes, le déchiffreur doit posséder des qualités morales que nous allons examiner et résumer brièvement.

2° QUALITÉS ET MATÉRIEL DU DÉCHIFFREUR.

A. *Qualités du déchiffreur.* L'art du déchiffreur demande des dispositions spéciales telles que la sagacité et une patience opiniâtre.

La première qualité est celle qui permettra au chercheur de trouver les moyens nécessaires pour arriver à la connaissance de la vérité; elle exige un esprit déductif, observateur, habitué aux mathématiques, ayant fait une étude approfondie des particularités des langues et des méthodes de chiffrement et de déchiffrement.

La sagacité (le flair) contribue à limiter le champ des recherches et à réduire le temps si précieux consacré au déchiffrement.

L'esprit d'observation a pour effet de ne négliger aucun indice dont l'induction tirera profit, pour en inférer les hypothèses les plus rationnelles et les plus certaines. Ces indices, ces renseignements, sont d'une manière générale :

1° Date, lieu et heure de la transmission et de l'interception des dépêches; lieu de destination;

2° Nom et qualité du signataire et du destinataire;

3° Connaissance approximative des sujets traités dans le texte par la connaissance des événements ambiants. On en déduira la langue employée, le sujet de la correspondance et aussi le genre de chiffrement, en facilitant l'analyse générale que nous venons d'exposer. Ces notions ont une importance capitale pour le déchiffrement des cryptogrammes provenant des méthodes à répertoire, et ils sont toujours d'une grande utilité pour les autres.

La seconde vertu, patience à toute épreuve, donnera au cryptologue la liberté d'esprit et la volonté opiniâtre nécessaires pour abstraire son esprit du milieu où il vit, et pour recommencer les opérations vingt fois s'il le faut, jusqu'à ce qu'il ait acquis la preuve presque certaine que ses recherches seront impuissantes, ou qu'elles aboutiront.

B. *Matériel du déchiffreur.*

1° Un dictionnaire ordinaire de petit format.

2° Un dictionnaire des rimes.

3° Un dictionnaire des synonymes.

4° Des répertoires des particularités de la langue, fréquences, séquences, etc.

5° Tous les dictionnaires chiffrés et tables chiffrantes en usage dans le commerce.

6° Les tableaux appartenant aux méthodes qui en comportent.

CHAPITRE III. — PARTICULARITÉS DE LA LANGUE.

A. *Classification des lettres*

Les lettres sont divisées en voyelles, au nombre de 6 (a, e, i, o, u, y) et en 20 consonnes. Souvent en cryptographie, on range l'y parmi les consonnes.

Au point de vue de l'émission des sons, la classification des consonnes est la suivante :

a° les *dentales : d* et *t.*

b° les *gutturales :* g, j, c devant a, o, u et devant une consonne.

c° les *labiales :* b, p, f, v.

d° les *sifflantes :* s, ç, x, z et c. (devant e ou i).

e° les *liquides :* l, m, n, r.

f° l'aspirée : h.

En français, la fréquence des lettres sur 1000 peut être indiquée par le tableau B ci-contre :

B. *Tableau de fréquence des lettres.*

D'après Valério.	D'après Kerckhoffs.	D'après une police de typographe	D'après nous (moyennes de 10000 lettres)
E = 170.0	E = 185	E = 184	E = 170
N = 87.3	S = 88	S = 94	A = 73
A = 72.6	R = 78	R = 86	I = 72
I = 68.6	I = 74	N = 75	U = 70
R = 68.6	A = 72	T = 72	N = 70
S = 68.6	N = 71	A = 70	S = 70
T = 67.3	T = 65	I = 58	T = 69
U = 66.6	O = 57	O = 58	R = 68
O = 66.0	U = 52	U = 58	O = 66
L = 48.6	L = 46	L = 45	L = 49
D = 46.0	D = 42	D = 36	D = 42
C = 35.3	M = 36	P = 33	C = 34
M = 30.6	C = 34	C = 33	M = 33
P = 28.0	P = 24	M = 28	P = 30
V = 18.0	V = 16	F = 12	V = 19
F = 12.6	F = 14	G = 11	F = 11
B = 9.3	Q = 10	V = 11	B = 10
G = 7.3	G = 8	Q = 10	Q = 10
Q = 7.3	X = 7	B = 7	G = 9
H = 5.3	J = 6	X = 7	H = 9
X = 5.3	B = 5	H = 4	X = 5
J = 3.3	H = 4	J = 4	J = 4
Y = 3.3	Z = 3	Y = 3	Y = 4
Z = 2.7	Y = 1	Z = 1	Z = 3
K = 0.0	K = 0	K = 0	K = 0
W = 0.0	W = 0	W = 0	W = 0
Voyelles	Voyelles	Voyelles	Voyelles
E = 170	E = 185	E = 184	E = 170
A = 72.6	A = 72	A = 70	A = 73
I = 68.6	I = 74	I = 58	I = 72
U = 66.6	U = 52	U = 58	U = 70
O = 66.0	O = 57	O = 58	O = 66
443.8	440	428	451 (1)

(1) Nous adopterons comme pour cent des voyelles 45.00 ; ce chiffre peut cependant varier entre 30 et 60 p. 100.

Fréquence des bigrammes.

Remarques.—Dans le tableau C ci-après, les lettres de la ligne horizontale sont les premières des bigrammes ; celles de la ligne verticale sont les secondes.

Les nombres à l'intersection des colonnes indiquent la fréquence des bigrammes ; ainsi le bigramme O L s'est présenté 11 fois, le bigramme L O, 21 fois sur 10.000 lettres de texte.

Les arrangements avec répétitions des lettres deux à deux sont au nombre de $26^2 = 676$, mais la langue n'en emploie réellement qu'une bonne moitié. Ainsi sur divers textes comportant 10.000 lettres, nous n'avons obtenu que 380 arrangements, comme on peut le constater dans le tableau C. ; encore, 77 combinaisons ne se présentent-elles qu'une fois. On peut donc admettre en pratique qu'il n'y a pas plus de 300 arrangements de lettres deux à deux.

La connaissance des bigrammes les plus fréquents, par ordre de fréquence, offre une grande utilité ; nous en donnons la liste ci-dessous :

E S = 293	S E = 142	E M = 101
E N = 252	I T = 135	E U = 101
L E = 237	T E = 124	T A = 100
D E = 233	M E = 123	U E = 98
O N = 177	A I = 119	U R = 98
E R = 165	N E = 118	L A = 95
R E = 165	E D = 117	Q U = 93
N T = 163	A N = 107	C E = 90
E L = 153	E T = 106	T I = 90
O U = 150	I E = 103	N S = 86

	1702	746	720	699	672	696	696	694	680	486	418	337	328
	E	A	I	U	O	N	S	T	R	L	D	C	M
E	63	3	103	98	1	118	142	124	165	237	233	90	123
A	47	4	11	21	2	49	64	100	79	95	49	37	54
I	14	119	8	80	63	22	59	90	66	20	41	20	28
U	101	64	1	3	150	10	32	25	14	18	42	19	9
O	23		54	13	1	35	40	30	54	21	23	78	28
N	252	107	80	61	177	44	5	9	9	3			
S	293	30	80	57	35	86	74	45	36	11	5	3	
T	106	55	135	39	21	163	54	39	50	1		25	
R	165	83	49	98	68	6	10	63	14	1	15	11	
L	153	49	75	41	11	1	49	40	48	56		5	
D	117	19	17	15	7	60	63	64	41	2	3	1	
C	83	37	12	25	9	50	34	8	23	4		13	
M	101	18	15	19	49	1	13	17	17	5	3	1	13
P	60	43	6	44	10	12	16	14	13				50
V	31	38	19	30	34	8	5	3	19				
F	30	9	7	11	10	11	11	1	4	2			
B	13	21	7	5	10	1	2	1	3	1			22
Q	23	10	13			5	15	12	13	1		1	
G	11	29	21	5	9	8	5	1	9	1			
H	10				1		1	4	1	3	3	33	
X	7	1	7	27		2							
J	5	5		6		1	1	3	1	1	1		
Y	1	1			4	3	1	1	1	3			1
Z	3	1		1									
K													
W													
	E	A	I	U	O	N	S	T	R	L	D	C	M

des bigrammes (10,000 lettres.)

288	184	114	101	94	92	87	51	43	39	33	0	0	
P	V	F	B	Q	G	H	X	J	Y	Z	K	W	
52	59	17	8		38	41	7	14	5	1			E
50	37	23	17	1	11	14	3	5	4	3			A
9	26	7	9		3	7	9	1	3	2			I
15	6	6	5	93	5	5	1	6	1	1			U
54	33	21	7		1	15		17	3	4			O
2	1		1		13					2			N
11			4		1		7		3	3			S
7	1				1		8		2	3			T
45	11	10	7		10	2			1	1			R
17	6	13	34		3		6		1	2			L
3		1	2		1		4		2	1			D
			1				2		1	1			C
1	1				1		2		1	2			M
8	1						1		4	2			P
1			2						1	2			V
1		15							3	2			F
1			1						1	1			B
1													Q
		1			2				1				G
7			1		1		1		1				H
													X
			2						1				J
3					1	3							Y
													Z
													K
													W
P	V	F	B	Q	G	H	X	J	Y	Z	K	W	

Analyse sommaire de la table C.

Sur 1702 fois que se présente la lettre *e*, elle n'est précédée que 268 fois, et suivie que 249 fois, d'une autre voyelle; donc 6 fois sur 7 elle est en séquence avec une consonne, soit avant, soit après elle. Elle est la seule qui puisse se trouver en combinaison avec toutes les lettres de l'alphabet et qui puisse être doublée à la fin d'un mot.

Les autres voyelles sont rarement redoublées dans un mot.

Quand un mot a pour avant-dernière lettre un *e*, la dernière lettre est en général un *s*, un *r* ou un *z*; quand la dernière et la quatrième à partir de la fin sont des *e*, l'avant-dernière sera ordinairement un *c* ou un *t*, l'avant-pénultième sera un *n*, comme affluence, vente.

Les remarques les plus intéressantes, après les grandes généralités, sont les combinaisons les moins fréquentes :

h est généralement précédée de *c*, souvent de *r* et quelquefois de *p* et de *t*; elle est presque toujours suivie de *e* et assez souvent de *o*, très rarement d'une consonne.

k et *w* ne se rencontrent que dans les mots d'origine étrangère.

z est généralement placée à la fin des mots et précédée de *e*.

Dans le corps d'un mot, elle est en général, suivie de *o*, *a*, ou *i*.

y, dans un mot, est généralement précédée de *o*, *e*, *a* : elle est souvent isolée, et peut être suivie de presque toutes les autres lettres.

x est généralement précédée de *u* et quelquefois de *e* ou de *i*. Elle est fréquemment suivie de *e*, *i*, *t*, *s* ou *l*.

v est presque toujours précédée d'une voyelle parfois de *r* ou *n*; elle est généralement suivie de *e* et souvent de *a*, *o*, *i*.

q est généralement précédée de *e*, souvent de *s*, assez souvent de *t*, *r*, *i* ou *a* ; elle est toujours suivie de *u*.

Une lettre de faible fréquence précédant toujours une voyelle probable répond au *q*.

j est généralement précédée de *e*, *a*, *u* ou *t*, et presque toujours suivie de *o* ou *e*, plus rarement des autres voyelles ; jamais d'une consonne.

Il n'y a pas de mots français sans voyelle ; il n'y a pas de mots de plus de trois lettres sans consonne. Aucun mot ne renferme de séquences de cinq consonnes. Si dans un texte on rencontre une succession de cinq lettres consonnes, on peut dire que cette séquence est due à la terminaison d'un mot par un trigramme, suivi d'un bigramme-consonne initial. La troisième lettre de succession de cinq consonnes sera un *s*, la cinquième généralement un *l* ou un *r* (exceptionnellement un *c*, *p*, *t*, ou *h*).

Les seuls mots monogrammes sont *a*, *à*, *o* (très rarement) et *y*.

Aucun mot ne forme de séquence de plus de quatre voyelles : ayions.

Lorsque deux mots monogrammes se suivent, ce sont : *y a* ou *a à*.

Les consonnes isolées sont des lettres apostrophées : *c*, *d*, *j*, *l*, *m*, *n*, *s* et *t* ; la lettre qui suit une apostrophe est toujours une voyelle ou une *h* ; si l'apostrophe est suivie d'un bigramme, ce sera un des suivants : *j'ai*, *l'ai*, *n'ai*, *l'an*, *d'an*, *d'au*, *j'en*, *l'en*, *m'en*, *n'en*, *s'en*, *t'en*, *l'es*, *t'es*, *l'ex*, *s'il*, *l'on*, *d'or*, *l'or*, *d'os*, *l'os*, *d'un*, *l'un* ; si l'apostrophe se trouve après un bigramme, ce n'est qu'avec les bigrammes : *qu'au*, *qu'en*, *qu'il*, *qu'on*, *qu'un* ou *qu'or*.

Les mots bigrammes sont ; *ah*, *ai*, *an*, *as*, *au*, *ay*, *bi*, *bu*, *çà*, *ce*, *ci*, *co*, *de*, *du*, *eh*, *en*, *es*, *et*, *eu*, *ex*, *fi*, *ho*, *il*, *je*, *la*, *là*, *le*, *lu*, *ma*, *me*, *mi*, *mû*, *n'a*, *ne*, *ni*, *nu*, *oh !* *on*, *or*, *os*,

ou, où, pu, sa, se, si, su, ta, te, tu, un, us, va, vu.

Lorsque deux bigrammes identiques se suivent, ce sont *en en.*

Deux bigrammes se suivant avec un redoublement au milieu sont : *il le, en ne, on ne, un nu, et te.*

Nous donnons encore, les notes et règles linguistiques ci-après. Elles permettront au cryptologue de diriger et de poursuivre ses recherches rationnellement, avec la certitude d'arriver au résultat, chaque fois que le système à déchiffrer offre la moindre prise au déchiffrement.

Pour être complet, il faudrait encore reproduire le remarquable mais long répertoire des mots, classés par familles d'articulations, dû au capitaine Valério ; nous croyons qu'il pourra à l'occasion être d'un grand secours. Mais le chercheur qui possède les qualités et les règles que nous avons énumérées, et que nous allons développer encore, sera suffisamment armé pour s'exercer à la pratique du déchiffrement.

Les nomenclatures du capitaine Valério peuvent être parcourues ou consultées avec le plus grand fruit, mais ne peuvent trouver place dans notre étude ; nous y renvoyons le lecteur qui désire pousser plus avant l'étude des lois du déchiffrement par la déformation des sons et des mots.

Nous indiquerons plus loin le résumé des règles qui ont été déduites de ce travail si considérable.

D. *Etude particulière des bigrammes.* — Un bigramme peut se composer : I° de deux voyelles ; II°, d'une voyelle et d'une consonne ; III°, de deux consonnes.

I° *Bigrammes voyelles.* — Les arrangements possibles sont :

A A	E A	I A	O A	U A
A E	E E	I E	O E	U E
A I	E I	I I	O I	U I
A O	E O	I O	O O	U O
A U	E U	I U	O U	U U

D'après l'examen du tableau C, on peut considérer comme rares les bigrammes :

EI, EO, IA, UA, UO ;

comme très rares ou exceptionnels :

AA, AE, AO, II, IU, OA, OE, OO, UU.

II. *Bigrammes mixtes.* — Les voyelles peuvent, en général, précéder ou suivre toutes les consonnes.

On peut admettre comme rares les bigrammes :

AF, AQ; EH, EZ; IB, IF, IP, IX; OB, OC, OD, OF, OG, OL, OP; UB, UG, UJ.

Les bigrammes suivants et toutes les combinaisons de l'Y avec les voyelles peuvent être considérées comme très rares :

AH, AJ, AX, AZ; EJ; IH, IJ, IZ; OH, OJ, OQ, OX, OZ; UH, UQ, UZ.

III. *Bigrammes consonnes.* — Une succession de deux consonnes peut exister :

1° Au commencement d'un mot;

2° Dans le corps d'un mot;

3° A la fin d'un mot;

4° Par la réunion de la consonne finale d'un mot et de la consonne initiale du mot suivant.

1° *Bigrammes consonnes initiaux.* — Ils proviennent :

a. des articulations doubles composées d'une labiale, d'une gutturale ou d'une dentale, suivie des liquides l ou r :

bl pl	fl phl vl	cl chl gl	
br pr	fr phr vr	cr chr gr	dr, tr

b. des articulations diverses ci-après :

ch, ph, th, mn, ps,
sc, sp, sph, sq, st, sv.

2° *Bigrammes consonnes dans le corps des mots.* — Ils sont produits :

a. par redoublement (1) de la même lettre :

(1) Les lettres doublées sont généralement des consonnes ; elles sont généralement précédées et suivies d'une voyelle, d'un *l* ou d'un *r*.

bb (1), cc, dd (1), ff, gg (1), ll, mm, nn, pp, rr, ss, tt.

b. par les bigrammes consonnes initiaux et divers qui viennent d'être indiqués, et par les articulations simples ci-après :

ck, cq, gm, gn

c. par les articulations composées provenant des combinaisons principales suivantes :

bc, bd, bh, bj, bm, bn, bs ;

ct ;

dh, dj, dm, dv ;

nc, nd, nf, ng, nj, nl, nq, nr, ns, nv;

pt, pht;

rc, rf, rm, rn, rp, rq, rs, rv ;

provenant en général de la réunion d'une préfixe avec un radical commençant par une consonne.

d. des articulations composées provenant de la séquence des liquides l, n, r, de la dentale t et des sifflantes s, x, z, avec les autres consonnes qu'elles peuvent en général précéder ou suivre toutes (2).

3° *Bigrammes consonnes finaux.*

Les bigrammes consonnes finaux sont :

ch, cq, ct, gt, mp, nc, ng, nq, ns, nt, rc, rd, rg, sc, ss, st.

Les plus fréquents sont : nt, ns et rt.

4° *Bigrammes formés des consonnes finales et initiales des mots.* — Les consonnes se classent, d'après leur ordre de fréquence finale, de la manière suivante :

Fréquentes : L, N, R, S, T, X, Z ;

Rares : C, D, F ;

Exceptionnelles : G, M, P, Q ;

Plus exceptionnelles encore : B, H, J, K, V et W.

---

(1) Exceptionnels.

(2) Les exceptions ressortiront d'un examen attentif du tableau C et de l'analyse sommaire que nous avons faite précédemment. Il en est de même des quelques bigrammes qui ne rentrent pas dans la classification précédente.

Les lettres finales les plus fréquentes, par ordre de fréquence, sont :

E, S, T, R, A, N, L, I, U, D, C, X.

Les mots peuvent commencer par une consonne quelconque (rarement par x ou z).

Les lettres initiales les plus fréquentes par ordre de fréquence sont :

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

Comme les consonnes finales les plus fréquentes sont : S, T, R, N, L, D, nous devons considérer comme très probables les combinaisons dont ces lettres forment le premier terme, et les consonnes initiales les plus fréquentes, le second : D, L, P, C, S, M, R, F, Q, N, T.

E. *Etude des trigrammes.*

Les arrangements des 26 lettres de l'alphabet trois à trois ou trigrammes, sont au nombre de $26^3 = 17576$; sur divers textes d'une valeur de 10,000 lettres, il ne s'en est présenté que 1927 différents, encore 1140 trigrammes ne se produisirent-ils qu'une seule fois.

Les nombres de trigrammes différents fournis par chaque lettre ont été les suivants :

E	A	I	S	T	U	R	O	N	L	D	C	M
280	173	151	133	122	116	108	103	98	90	74	69	66

P	V	F	B	Q	G	H	X	J	Y	Z	K	W
57	52	47	43	40	23	21	19	16	11	10	0	0

Les trigrammes les plus usités, par ordre de fréquence sont indiqués dans le tableau ci-après :

F. *Tableau de fréquence des trigrammes.*

ENT	=105	DES	=36	TEN	=26	NTA	=20	LAR	=16
LES	= 80	ELA	=36	DEC	=25	LEM	=19	SCO	=16
QUE	= 72	ELE	=36	RIE	=25	LEU	=19	DON	=15
EDE	= 70	SDE	=36	ERI	=25	REL	=19	TLE	=15
ION	= 57	EQU	=35	IRE	=25	ATI	=19	NTL	=15
AIT	= 57	DAN	=34	ESS	=25	CHE	=19	ISE	=15
EME	= 55	SON	=33	NCE	=24	COM	=19	RQU	=15
LLE	= 52	OND	=33	ONT	=23	ETA	=18	LED	=14
MEN	= 45	ANT	=33	TDE	=22	ESO	=18	IEU	=14
NTE	= 45	ERE	=32	NEN	=22	LEN	=18	EMI	=14
EUR	= 44	AIS	=30	OUS	=22	ESD	=18	ORT	=14
TIO	= 44	CES	=30	NTD	=23	ESC	=18	NER	=14
EST	= 43	UEL	=29	SES	=22	RES	=17	EES	=13
ESE	= 43	SLE	=29	TES	= 22	ONN	=17	SLA	=13
DEL	= 38	PAR	=28	NES	=22	NSL	=17	VAI	=13
TER	= 38	TOU	=28	END	=21	TAI	=17	ENN	=13
ONS	= 38	SEN	=28	EAU	=21	ECO	=16	EPO	=12
QUI	= 38	OUR	=28	ERA	=21	ENE	=16	RET	=12
ANS	= 37	SSE	=27	SER	=21	ITI	=16	DET	=12
ELL	= 36	RLE	=27	BLE	=21	ART	=16	CON	=12

Notes. Lorsque dans un trigramme la première lettre est un *e*, le mot sera le plus souvent *est* et parfois, *eau, eux, écu, ému, épi, élu*;

si la deuxième lettre est un *e*, ce sera *ces, cet, des* ou *les*;

si l'*e* est la troisième lettre, le trigramme sera *que* ou *une*.

Les trigrammes qui ont la troisième lettre égale à la première sont : *été, ici, non, ses, sis, sus, tôt, têt, agu* (chef), *ana* (recueil) et *ara* (perroquet).

Le trigramme avec redoublement de l'*e* est *bée*.

H. *Tableau des Trigrammes (VVV, VVC, CVV, CVC).*

	A	E	I	O	U	Y	P	F	B	V	C	Q	G	J	T	D	S	Z	X	M	N	L	R	H	
A				U			E	I	E	EI	EIO	U	EU		EIU	I	EIU			EI	EIU	EIU	EI	E	A
E	I			IU			I	I	I	IOU	IOU	U	IU		IU	IU	IU		I	IU	EIU	AEIU	EIU	EI	E
I		U	AE	EU	AE		AEOU	AEOU	AEO	AEO	AEOU	U	AOU	AOU	AEOU	AOU	AEOU			AEO	AEOU	AEOU	AEOU	AO	I
O				U			I			I	I	U	EIU		IU	I	EI		I		I	I	EI		O
U		A	AE	E	E	E	AEO	AEO	AEO	AEO	AEO		AEO	AEO	AEO	EO	AEO			AEO	AEO	AEO	AEO	AEO	U
Y							AU	U		O	U			O		O	AU			O	A	AO	AOU		Y
P	U			U	I		AEO		A	A	AEIOU				AI	EIOU	AEIOU			AE	AI	AIOU	AEIOU	AIO	P
F	IU		E	IU	I					I	AO				EI	EI	IU			EI	EIOU	AEI	EIO	EI	F
B	IU	AU	A	U	A		AU	A	A	AI	AIU		AI		AIO	AE	AIOU		I	AO	AEIO	AFI	AEIOU	AI	B
V	IU	U	E	U	I		I	AE		I	AEI		I		I	AEI	AE			O	AEIO	AEI	AEIO	AEI	V
C	IU		AEO	U	I		AEIO	AEI	AU	AEIO	AEIO		AO	E	AEIO	AEIOU	AEOU		AE	AEIO	AEI	AEIOU	AEIOU	AE	C
Q				U			AIO	AI		AEO			I		AI		EI			O	I	AEIO	AEI	A	Q
G	IU	I	AE	IU	A		AU	IU	A	AEIO	AIO			U	AEIO	AI	AIO		AI	AEO	AEIO	AEIO	AEIO	AO	G
J	U			U												E	EU			A			EO		J
T	IU	AIU	AEO	IU	AEI		AEIOU	AEIU	AEIOU	AEIO	AEIOU		AEI	E	AEIOU	AEO	AEIO			AEIOU	AEIOU	AEIOU	AEIOU	AEIOU	T
D	IU	U	E	U	AI		IU	EI	AU	AI	AEIO		AE	U	AIU	AEI	AEIU			AEIO	AE	AIU	EIOU	EI	D
S	IU	U	E	IU	EIO		AIO	AEIOU	AEIOU	AEIO	EIU		AE	EU	AEI	EIOU	AEIU		I	AEIOU	EIO	AEIOU	AEIOU	AEIO	S
Z		I		U									A			I	E						EO	E	Z
X	IU	U		I				I		E					E	I	I			AI	E	AEU	I		X
M	IU	A	AE				AEO	AEU	IO	E	AEIOU		EIU	A	AEIOU	AEIO	AEIOU		AEI	E	AEIOU	AEIOU	AEIOU	AEIO	M
N	I	AIU	AE	I	AEI		AEIO	AEIOU	AIO	AEI	AEIOU		AEIO	AO	AEIOU	AEIO	AEIOU	O	A	AEIOU	AEIO	AEIOU	AEIOU	AEIO	N
L	I	IU	AE	AIU	AEI		AEIOU	AEIO	AEIOU	AEIOU	AEIOU		AEIU	A	AEIOU	EIOU	AEIOU	E	AI	AEIOU	AEOU		AEIOU	AEIO	L
R	IU	IU	AE	IU	AEI		AEIOU	AEIOO	AEIOU	AEIO	AEIOU		AEIOU	AU	AEIOU	AEIOU	AEIOU		AE	AEIOU	EIOU	AEIOU	AEIOU	AEIOU	R
H							A			A	AO					E							E		H
	A	E	I	O	U	Y	P	F	B	V	C	Q	G	J	T	D	S	Z	X	M	N	L	R	H	

G. Analyse schématique des trigrammes. (1)

On rencontre un trigramme de trois manières différentes :

a. Il peut se trouver dans le corps d'un mot ;

b. Il peut se composer de la lettre finale d'un mot et des deux premières lettres du mot suivant ;

c. Il peut comprendre les deux dernières lettres d'un mot et la lettre initiale du mot suivant.

Les catégories *b* et *c* chevauchent donc sur deux mots.

a. Trigramme dans le corps d'un mot.

Ces trigrammes se présenteront toujours sous l'une des formes schématiques suivantes, ou la lettre *V* représente une voyelle et *C* une consonne :

1re catégorie : VVV VVC, CVV CVC

2e catégorie : VCV VCC, CCV CCC.

Les trigrammes de la premières catégorie où une voyelle occupe le cœur du trigramme, sont renseignés dans le tableau H. ci-annexé.

Remarques. La ligne horizontale supérieure du tableau H comprend les premières lettres; les lignes verticales à droite et à gauche, en dehors du tableau, comprennent les troisièmes lettres; à l'intersection, se trouvent les voyelles du centre. Ainsi la combinaison P-B fournit, avec les voyelles A-U, les trigrammes P A B, P U B; la combinaison L-M, les trigrammes L A M, L E M, L I M, L O M, L U M.

Les trigrammes de la deuxième catégorie, où une consonne occupe le cœur du trigramme, sont renseignés dans chacune des tables I 1°, 2°, 3°, et 4°.

(1) D'après Valério. Cryptographie. Journal des sciences militaires 1893.

I. *Tables des trigrammes V C V, V C C, C C V, C C C.* — 1° *V C V* (1).

	ABA		ADA		AGA			ALA	AMA	ANA	APA		ARA	ASA	ATA	AVA			
		ACE	ADE		AGE		AJE	ALE	AME	ANE	APE		ARE	ASE	ATE	AVE	AXE		
A	ABI	ACI	ADI	AFI	AGI			ALI	AMI	ANI	API		ARI	ASI	ATI	AVI	AXI		
	ABO	ACO	ADO				AJO	ALO	AMO	ANO	APO		ARO		ATO	AVO			
		ACU	ADU					ALU	AMU			AQU	ARU		ATU				
	EBA	ECA	EDA	EFA	EGA		EJA	ELA	EMA	ENA	EPA		ERA	ESA	ETA	EVA	EXA		
		ECE	EDE	EFE	EGE	EHE	EJE	ELE	EME	ENE	EPE		ERE	ESE	ETE	EVE			
E		ECI	EDI	EFI	EGI			ELI	EMI	ENI	EPI		ERI	ESI	ETI	EVI	EXI		
	EBO	ECO	EDO	EFO			EJO	ELO	EMO	ENO	EPO		ERO	ESO	ETO	EVO			
		ECU	EDU	EFU	EGU			ELU	EMU	ENU	EPU	EQU		ESU	ETU				
		ICA	IDA		IGA			ILA	IMA	INA	IPA		IRA	ISA	ITA	IVA	IXA		
I	IBE	ICE	IDE		IGE			ILE	IME	INE	IPE		IRE	ISE	ITE	IVE	IXE		
	IBI	ICI	IDI	IFI	IGI			ILI	IMI	INI	IPI			ISI	ITI	IVI			
								ILO	IMO	INO	IPO		IRO	ISO	ITO	IVO			
	IBU	ICU			IGU				IMU	INU		IQU			ITU				
	OBA							OLA	OMA	ONA			ORA	OSA	OTA				
	OBE	OCE	ODE				OHE	OJE	OLE	OME	ONE		ORE	OSE	OTE	OVE	OXE		
0		OCI	ODI				OHI		OLI	OMI	ONI								
									OLO	OMO	ONO								
		OCU	ODU						OLU	OMU		OQU							
			UDA				UHA		ULA	UMA	UNA			URA	USA	UTA			
	UBE		UDE		UGE				ULE	UME	UNE	UPE		URE	USE	UTE	UVE		
U	UBI		UDI						ULI	UMI	UNI			URI	USI	UTI			
	UBO	UCO						UJO	ULO					URO	USO	UTO			
		UCU								UMU					USU	UTU			

2° *V C C.*

La forme VCC peut provenir :

1° De la réunion d'une voyelle et d'une des consonnes doubles bl, br, cl, cr, ch, ct, cc, fl, fr, ff, gl, gr, gn, gm, pl, pr, pt, pp, sc, sp, st, ss, tr, th, tt, vr. Mais toutes les combinaisons sont loin de se présenter fréquemment ; voici les plus usitées :

ABL, ABR; EBR ; IBL, IBR ; OBL ; UBL.

ACL, ACR, ACH, ACT, ACC, ACQ; ECL, ECR, ECH, ECT ; ICL, ICT; OCL, OCR, OCH, OCT, OCC ; UCH, UCT, UCC.

ADR ; EDR ; UDR.

AFF ; EFL, EFR, EFF ; OFF ; UFF.

AGR, AGN ; EGR, EGN ; IGR, IGN ; OGR ; UGN, UGM.

APL, APR, APH, APT, APP ; EPL, EPR ; EPT, IPL, IPR, IPT ; OPT ; OPP, UPL, UPR, UPT, UPP.

ASP, AST, ASS, ESP, ESC, EST, ESS ; ISP, ISC, IST, ISS ; OST, OSS ; USP, USC, UST, USS.

ATR, ATH, ATT ; ETR, ETH, ETT ; ITR, ITT ; OTR, OTH ; UTR, UTT.

AVR ; IVR ; UVR.

2° Des deux dernières lettres d'une syllabe nasale ou liquide et de la première lettre de la syllabe suivante :

AMB, AMP, AMM, AMN; EMB, EMP, EMM, EMN; IMB, IMP, IMM, OMB, OMP, OMM, OMN.

ANC, AND, ANF, ANG, ANN, ANQ, ANS, ANT ; ENC, END, ENF, ENG, ENN, ENQ, ENR, ENS, ENT, ENV ; INC, IND, INF, ING, INS, INT, INN ; ONC, OND, ONF, ONG, ONN, ONQ, ONS, ONT, ONV.

ALR, ALG, ALH, ALL, ALM, ALS, ALT, ALV ; ELC, ELL, ELQ ; ILL, ILS ; OLD, OLL, OLT, OLV ; ULB, ULG, ULL, ULP, ULS, ULT.

ARB, ARC, ARD, ARF, ARG, ARL, ARM, ARQ,

ARR, ARS, ART, ARV ; ERC, ERD, ERF, ERG, ERJ, ERM, ERN, ERP, ERQ, ERR, ERT, ERV ; IRM, IRR; ORC, ORD, ORG, ORM, ORR, ORS, ORT, ORV ; URB, URC, URD, URG, URM, URN, URR, URS, URT, URV.

3° Des trigrammes formés au moyen des particules ab, ad, ob, sub; exemple :

AB-D-H-J-S-; AD-H-J-M- ; EX-C-H-P-T; OB-J-S-T; UB-D-S.

3° *C C V.*

La forme CCV peut provenir :

1° D'une articulation double ou d'une consonne doublée, suivie d'une voyelle. Ces combinaisons se présentent presque toutes à l'exception de :

BLU, GLU, GRU, GNU, VRU, PHA, PHO, PHU, THA, THI, THU, FFU, PPI, TTU.

2° De la dernière lettre d'une syllabe nasale ou liquide et des deux premières lettres de la syllabe suivante :

LBU	LCO	NDA	LFA	LGA	NJE	LLA	MMA	NNA	LPA	RRA	LSA	LTA	LVA
MBA	LCU	NDE	LFE	LGE	NJO	LLE	MME	NNE	LPE	RRE	NSA	LTE	LVE
MBE	NCA	NDI	NFA	LGU	NJU	LLI	MMI	NNI	MPA	RRI	NSE	LTI	NVA
MBI	NCE	NDU	NFE	NGA	RJE	LLO	MMO	NNO	MPE	RRO	NSI	LTU	NVE
RBI	NCI	RDA	NFI	NGE		LLU	MMU	NNU	MPO	RRU	NSO	NTA	NVI
RBO	NCO	RDE	NFO	NGU		NLE	RMA		MPU		NSU	NTE	NVO
	RCE	RDI	NFU	RGA		RLA	RME		RPA		RSA	NTI	RVA
	RCI	RDO	RFA	RGE		RLE	RMI		RPE		RSE	NTO	RVE
	RCO		RFE			RLO	RMO		RPI		RSI	NTU	RVI
	RCU		RFI				RMU		RPO		RSO	RTA	
			RFO								RSU	RTE	
			RFU									RTI	
												RTO	
												RTU	

3° Des trigrammes formés au moyen des particules ab, ad, ob, sub, exemple :

XCE	BDI	BHO	BJE	DME	XPE	BSE	BTE
XCI		DHE	DJO	DMI	XPO	BSO	XTE
		XHO	DJU	SME		BSU	XTU
				SMI		BSI	

4° *C C C.*

Le tableau ci-dessous des trigrammes de la forme c c c suffit, après ce qui vient d'être dit, pour faire ressortir la manière dont ils sont formés :

MBL	PPL	MPHL	NFL	NVR	GGL	CCL	NDR	TTR
MBR	PPR	LPHR	NFR		GGR	CCR	RDR	NTR
RBR	MPL				NGL	NCL		RTR
	MPR				NGR	NCR		STR
	RPL				SGR	NCT		XTR
	RPR				NGT	NCH		
	MPT	NTHR				RCH		
	RPS					RCL		
	SPL					RCR		
	XPL					SCR		
	XPR					XCL		

Les trigrammes consonnes finaux sont : cts, mps, ncs, nds, ngs, rcs, rds, rgs, rts. On peut remarquer qu'ils se terminent tous par un *s*.

J. *Trigrammes entre deux mots.*

b. Trigrammes composés de la lettre finale d'un mot, et des deux premières lettres du mot suivant ;

c. Trigrammes composés des deux dernières lettres d'un mot et de la lettre initiale du mot suivant.

Nous savons que la finale des mots est généralement formée par l'une des lettres suivantes : a, e, i, u, l, n, r, s, t, x, z ; ces lettres forment les combinaisons binaires finales :

AL, EL, IL ; AN, EN, IN, ON, UN ; AR, ER, IR, UR ; AS, ES, IS, US, LS, NS, RS, TS ; AT, ET, IT, OT, UT, NT, RT, ST ; UX, EZ ; ajoutons encore IF et ND.

CA, DA, EA, FA, HA, JA, LA, MA, NA, PA, RA, SA, TA, UA, VA.

CE, DE, EE, FE, GE, HE, IE, JE, LE, ME, NE, PE, RE, SE, TE, UE, VE.

AI, CI, DI, LI, MI, NI, OI, RI, SI, TI, UI, VI.

AU, CU, DU, EU, LU, MU, NU, OU, PU, RU, SU, TU, VU.

Nous savons également que les mots peuvent commencer par toutes les lettres de l'alphabet, exceptionnellement par X et Y; quant au bigramme initial des mots, si la première lettre est une consonne, toutes les combinaisons CV se présentent, sauf JI (Q est toujours suivi d'un U); les combinaisons CC se présentent toutes également et proviennent des articulations doubles.

Quant aux combinaisons VC, en voici le tableau :

AB, AC, AD, AF, AG, AJ, AL, AM, AN, AP, AR, AS, AT, AV.

EB, EC, ED, EF, EG, EH, EL, EM, EN, EP, EQ, ER, ES, ET, EV, EX.

IC, ID, IG, IL, IM, IN, IR, IS, IT, IV.

OB, OC, OF, OM, ON, OP, OR, OS, OT, OV.

UL, UN, UR, US, UT.

K. *Remarque importante sur les liquides.*

Si l'on observe que, dans les trigrammes à l'intérieur des mots, jamais une liquide n'occupe la place centrale, que la première lettre d'un mot commençant par deux consonnes n'est jamais une liquide, qu'il en est de même de la dernière lettre d'un mot finissant par deux consonnes, on conclura que la liquide est toujours soit suivie, soit précédée d'une voyelle.

L	précède	297	fois	une voyelle, et la	suit	63	fois
M	—	117	—	—	—	29	—
N	—	163	—	—	—	258	—
R	—	196	—	—	—	147	—

Cette remarque peut être utilisée avec avantage, pour la découverte des liquides ou des voyelles, dans la lecture des textes chiffrés par les méthodes par substitution.

L. *Notes linguistiques particulières*

OF dans le corps d'un mot est toujours précédé de *pr*, à moins que la lettre suivante ne soit un *f*.

Les trigrammes de la forme MBA, NPE, NVI, etc., proviennent en général de mots composés, les particules initiales étant CON ou COM, EN ou EM, IN ou IM.

RV dans le corps d'un mot est généralement précédé d'un E, quelquefois d'un U ou d'un A, etc., etc.

La terminaison *tion* peut être précédée d'une des lettres *a, i, u, n, c, p, r, s ;* exceptionnellement *o*.

La terminaison *ation* peut être précédée par l'une des lettres : *t, r, c, n, s, l, g, i, d, m, p, u, b, v, x ;*

Elle ne l'est jamais par *a, e, f, h, j, k, o, q, w, y, z*, (exc. : création)

BATION peut être précédé de *o* ou de *r*.

CATION est généralement précédé d'un *i*, quelquefois d'un *o*, assez rarement d'un *r* ou d'un *u ;* la finale se complète fréquemment en *ification*.

DATION précédé de *n, i, e, a*.

GATION précédé de *i, e, o, a, l, n, r*.

IATION précédé souvent d'un *c*, quelquefois d'un *l*, d'un *r* ou d'un *d*.

LATION assez souvent d'un *u*, puis *e* ou *l*, rarement *i* et *o*.

MATION *a, r* et *i*.

NATION souvent d'un *i*, quelquefois d'un *g*, rarement *a* et *o*.

PATION, *i, u, r*.

RATION souvent d'un *e*, assez souvent d'un *o, i, u, a*. On trouve aussi STR, TR, GR, BR.

SATION souvent précédé de *i*, quelquefois de *r*, exceptionnellement *n* ou *u*.

Se complète assez souvent en *alisation*.

TATION souvent précédé de *i* et *n*, assez souvent de *u* et *r*, quelquefois *s*, *c*, *e* ; exceptionnellement *o*, *p*, *l*.

UATION, *n*, *t*, *l*, *c*.

VATION, *a*, *e*, *o*, *r*.

XATION, *a*, *e*.

La terminaison ABLE est précédée souvent de *t*, *r*, *s*, *n* ; assez souvent *i*, *l*, *m*, *c*, *d* ; rarement *e*, *p*, *u*, *v*, *y*, *b* et *h*.

PRE commence un grand nombre de mots; est suivi de *c*, *d*, *f*, *j*, *l*, *m*, *n*, *o*, *p*, *r*, *s*, *t*, *u*, *v*.

PRO commence un grand nombre de mots ; est suivi de *b*, *c*, *d*, *f*, *g*, *h*, *i*, *j*, *l*, *m*, *n*, *p*, *r*, *s*, *t*, *u*, *v*, *x*.

L'aspiration *h* sert à former les articulations *ch*, *ph*, *th* ; on la rencontre isolée dans les quelques mots suivants : *ahurir*, *déharnacher* ; *ap-com-ré-préhension*, *incohérence*, *prohiber*, *souhaiter*, *malheur*, *silhouette*, *bonheur*, *déshabiller*, *déshabituer*, *déshérence*, *déshonnête*, *déshonneur*.

M. *Notes sur les polygrammes.*

La collection de polygrammes recueillis par Monsieur Vesin, dans son ouvrage : La cryptographie dévoilée (1) fournit une aide précieuse au cryptologue qui doit quelquefois prendre d'assaut, pour ainsi dire, les premiers mots d'un texte chiffré, ou faire choix d'un ou plusieurs mots parmi ceux à contexture semblable, pour contribuer au déchiffrement par la symétrie de position.

A ce titre nous croyons que ces notes méritent de figurer dans le tableau des particularités de la langue dont elles complètent l'étude au point de vue cryptologique. Nous les avons complétées et mises au point pour notre époque.

(1) Bruxelles, Deprez-Parent, 1847.

a. Trigrammes. — Age, aie, ail, air, ait, âme, ami, âne, ans, are, arc, ars, art, aux, axe.

Bac, bah !, bai, bal, ban, bar, bas, bât, bec, bel, bis, blé, boa, bol, bon, bot, bru, bue, bus, but.

car, cas, cep, ces, cet, cil, col, cul, coq, cou, crée, cri, cru, coi, cor.

des, dis, dit, dix, dom, don, dos, dot, dru, duc, due, duo, dur, dus, dut.

eau, écu, élu, ému, ère, est, été, eut, eux.

fer, feu, fil, fin, fis, fit, foi, fol, fou, for, fut, fût, fus, fui, fur.

gai, gaz, gré, gel, glu, gui, gué.

haï

ici, ifs, île, ils, ire.

jet, jeu, jus.

lac, las, les, lie, lié, lis, lit, loi, lui, lut, lot, lys.

mai, mal, mat, mer, mes, mil, mie, mis, mit, moi, mon, mot, met, mûr, mue.

nef, net, nez, nid, Nil, nie, nom, non, nos, nue, nul.

ont, oui, ode, oie, ose, ôté, œil, ouï.

par, pas, peu, pic, pis, pie, pin, pli, plu, pot, pré, pus, put, pue.

que, qui

ras, rat, rez, ris, riz, roi, rue, rut, roc, rôt.

sac, sec, sel, ses, sis, six, soc, soi, sol, son, sot, suc, sue, sué, sud, sur, sus, sut.

tac, tel, thé, toi, ton, tôt, tue, tué, tic, tir, tuf.

une, uni, uns, use, usé.

ver, vêt, vau, vie, vif, vil, vin, vis, vos, vue, vol.

zig-zag, zoé.

b. Tétragrammes : 1° Ayant la première lettre égale à la troisième :

Ajan (Afrique) Ajax, aman, amas, anal, aval, ceci, coca, êtes, gage, rare, rire, tâté, têtu, vive;

2° Ayant la première lettre égale à la quatrième :

aléa, alfa, alma, chic, choc, crac, cric, croc, être, fief, irai, nain, ruer, sais, sans, sens, sois, sous, suis, tact, tait, tant, toit, tort, tout, trot;

3° Ayant un redoublement médial :

abbé, allé, Anne, inné, issu, réel;

4° Ayant la deuxième lettre égale à la quatrième :

aéré, bête, cène, état, fête, feue, fini, gala, gelé, gêne, géré, jeté, lésé, levé, mêlé, mené, mère, midi, pelé, pène, père, pesé, rêne, semé, sève, sexe, vexé zélé;

5° Ayant, outre un redoublement médial, la première lettre égale à la quatrième :

Adda, elle, erre, esse.

6° Ayant un redoublement final :

abée, crée, idée, nuée, ruée, suée, tuée ;

7° Composés des deux mêmes syllabes :

baba, coco, même, tête, papa, dodo.

c. Pentagrammes. — 1° Ayant 3 lettres de la même valeur :

avala, ébène, élève, épelé ;

2° Ayant un redoublement : colle, comme, connu, cosse, cossu ;

3° Ayant 3 lettres égales dont une redoublée :

assis, errer, Lille, nonne;

4° Ayant un redoublement entre 2 mêmes lettres :

allant, appas, appât, Arras, belle, celle, cesse, cette, créer, dette, effet, elles, femme, ferré, gréer, messe, nette, pelle, selle, serre, telle, terre, verre;

5° Ayant 2 mêmes lettres se répétant :

aérer, échec, papal, sensé, texte;

6° Ayant deux redoublements : allée, année, innée.

d. Hexagrammes, — 1° Ayant 3 lettres de la même valeur :

Canada, décidé, décélé, déféré, démêlé, dételé, élégie,

élever, enlevé, entêté, épeler, espèce, espéré, évêché, évêque, éventé, excédé, exerce, Genève, infini, Malaga, Nankin, récelé, référé, rejeté, relevé, remède, repère, répété, révéré, statut, sursis, tantôt, vénéré ; (1)

2° Ayant 3 lettres égales y compris un redoublement :

accroc, assise, barrer, basses, cassis, dessus, erreur, passés, serrer, Suisse, tasses, tissus;

3° Ayant 3 lettres égales et un redoublement d'autre lettre : amassa, amarra, emmené;

4° Ayant 2 redoublements :

allées, années, déesse, innées, réelle, vallée.

e. Heptagrammes. — 1° Ayant 3 lettres de la même valeur :

avalant, Catalan, célèbre, céleste, déceler, décerné, déférer, délégué, démêler, dépêche, déréglé, élément, enlever, espèces, espérer, excéder, exemple, exercer, fenêtre, indivis, pénétré, préféré, prélevé, recéler, refermé, référer, régence régente, rejeter, relever, remèdes, répéter, requête, réserve, retenue, révéler, rêverie, secrète, sereine, statuts, suspens, tempête, tentant, végéter;

2° Ayant 3 lettres égales dont une redoublée :

annonce, Apennin, arrêter, arrière, arrivée, arroser, assisté, atteint, attente, attrait, battant, cellule, erreurs, nourrir, presse, session, sonnant, trotter;

3° Ayant 3 lettres et un redoublement d'autres lettres :

apparat, essence, éveille, recette, vedette;

4° Ayant 3 lettres égales : Suisse;

5° Ayant 2 redoublements :

alliées, assommé, atterré, déesses, réelles, vallée;

6° Ayant la 1re lettre égale à la 5e, la 2e égale à la 6e, et la 3e égale à la 7e :

cherche, quelque.

(1) Remarquer que les trois lettres égales sont presque toujours des *a* ou des *e*.

f. Octogrammes. — 1° Ayant 4 lettres égales : dégénéré, inimitié, régénéré;

2° Ayant 2 redoublements :

assiette, assommer, bouffées, cannelle, carrosse, cassette, desserré, illettré, mollesse, sonnette, terrasse, tonnelle, tonnerre.

g. Mots ayant 2 redoublements identiques :

assassin (et ses dérivés), assesseur, possesseur, possession.

Ces redoublements sont généralement en *s*; il y a une exception : intellectuelle.

Mots ayant un redoublement médial en *e* :

agréer, créer, européen, gréer, recréer, réélection, réellement.

h. Mots ayant un redoublement médial en *o* :

coopération, coordonner, épizootie, zoologie.

N. *Remarques spéciales aux méthodes idéographiques.*

Le déchiffrement des cryptogrammes provenant du procédé général polygrammatique ou idéographique exige, outre les connaissances qui précèdent, celles relatives au rapport du nombre de mots *pleins* aux mots *vides*. Les premiers sont fonction du sujet traité et sont essentiellement variables avec lui; leur recherche échappe à toute investigation, tant que le déchiffreur ne connaît pas la nature de la correspondance; ce sont les substantifs, les adjectifs qualificatifs, les adjectifs numéraux, les verbes et un certain nombre d'adverbes.

Les mots *vides* ne présentent aucun sens à l'esprit, mais ils sont les véhicules inséparables du discours ; ce sont les articles, les adjectifs déterminatifs (sauf les numéraux), les pronoms, les verbes auxiliaires, la plupart des adverbes, les prépositions et les conjonctions.

Si le système est littéral, l'examen du texte chiffré fera reconnaître des trigrammes semblables, distants d'un multiple de 3.

Si le système est numéral, et par groupes de quatre chiffres, des tétragrammes semblables, distants d'un multiple de 4, vont se présenter.

De même, le système numéral par groupes de 5, présentera des groupes de chiffres semblables distants d'un multiple de 5.

Les procédés employés pour supprimer les répétitions peuvent cependant modifier ces données et, dans ce cas, le diagnostic devient moins aisé.

Dès lors, deux résultats sont acquis; nous connaissons la méthode employée, et nous avons pu, par les chiffres fréquenciels, déterminer la signification probable des nombres correspondant aux mots vides. Ceux-ci jalonnent pour ainsi dire le discours; les règles de la grammaire et les documents que nous pourrons nous procurer sur la dépêche, nous aideront alors à trouver les mots pleins en relation avec les mots vides.

Dans le but de faciliter la recherche des mots pleins et des mots vides, nous avons construit la table O, ci-après, où les nombres proportionnels qui se rapportent aux mots les plus usuels du discours, en style normal, ont été calculés sur des textes de 1,000 mots, ayant trait à des sujets différents. La moyenne du nombre de mots *vides* est de 450 sur 1.000, avec un écart de 29 en plus, et de 49 en moins; la moyenne du nombre de mots *pleins* est de 550 sur 1.000, avec un écart de 49 en plus, et de 44 en moins.

En style militaire le nombre des mots pleins augmente assez bien; en style télégraphique (ordres, instructions, rapports) la moyenne du nombre de mots *pleins* atteint 65 %.

A. COLLON

Lieutenant d'artillerie adjoint d'Etat-Major.

(A suivre).

O. *Table proportionnelle des mots pleins et des mots vides.*

NATURE DES MOTS	NATURE DES TEXTES					
	STYLE MILITAIRE DES ORDRES	HISTOIRE MILITAIRE	STYLE DIPLOMATIQUE	HISTOIRE POLITIQUE	ETUDE POLITIQUE	ARTICLE LITTÉRAIRE
pleins	557	491	438	432	398	476
vides	443	509	562	568	602	524
divers	32	67	49	69	89	54
d'	10	13	25	13	10	10
de	74	61	55	59	56	39
du	16	9	21	11	8	13
des	11	11	10	10	9	27
l' (le)	7	16	17	20	11	14
l' (la)	14	7	18	26	13	5
le	16	34	39	14	14	30
la	57	30	41	43	25	20
les	25	20	19	23	23	20
et	27	33	24	19	48	27
ou, où	4	5	1	2	5	13
un, une	5	10	21	27	9	17
à	38	26	12	26	30	24
au	14	10	12	11	8	9
il (s), elle (s)	6	16	17	10	36	19
s' (se)	12	13	1	12	8	8
Autres pronoms personnels	7	1	12	4	6	14
possessifs	10	4	15	20	22	33
démonstratifs (ce, ces, cette)	6	17	14	20	21	15
qui	3	6	7	13	10	7
que, qu'	6	13	25	20	34	9
autres relatifs	»	»	2	»	4	5
dans	1	6	15	8	3	5
en	6	15	7	8	11	17
par	12	11	8	7	7	7
pour	7	7	9	2	6	10
ne	1	6	9	15	17	7
pas	»	1	3	8	9	3
plus	1	2	2	3	7	2
tout	2	5	4	7	9	6
avoir (auxiliaire)	1	10	25	16	16	19
être (id.)	12	17	23	19	14	15
on	»	7	3	3	5	1

ETUDE

SUR LA

CRYPTOGRAPHIE

Son emploi à la guerre et dans la diplomatie. (1)

TITRE II.

LA CRYPTOGRAPHIE ACTUELLE

Les méthodes de chiffrement et de déchiffrement.

PREMIÈRE PARTIE.

PROCÉDÉ GÉNÉRAL MONOLITTÉRAL.

Première classe : Systèmes par transposition ou interversion des lettres du texte clair.

CHAPITRE I. — MÉTHODES A CLEFS LITTÉRALES OU NUMÉRIQUES.

A. *Systèmes par transposition.*

La transposition simple, consiste dans la transcription des lettres d'un texte dans un autre ordre. On peut écrire une dépêche en la renversant, c'est-à-dire en écrivant ses lettres dans leur ordre régulier, mais à partir de la droite, ou par la n^{ième} lettre, à partir de la droite. Ainsi la phrase: « La place est abondamment pourvue de vivres » trans-

---

(1) Suite. — Voir 24^{e} année Tomes II et III.

posée en écrivant ses lettres dans l'ordre inverse, à partir de la 10e lettre à droite, sera :

uvrnoptnemmadnobatseecalpalservivede.

En groupant par 5 lettres, pour la transmission télégraphique, nous aurons :

uvrno — ptnem — madno — batse — ecalp — alser — vived — e.

On peut encore recopier la dépêche, en écrivant d'abord les lettres paires, puis les lettres impaires, ou de tel autre rang, suivant convention. La méthode est analogue.

La loi qui préside à la transposition des lettres constitue la clef des méthodes par transposition simple.

La *lecture* de cryptogrammes semblables se fait en reconstituant les lettres dans leur ordre normal.

Le déchiffrement n'offre pas la moindre difficulté; la fréquence des voyelles et leur alternance avec les consonnes, dévoilent immédiatement la clef de la méthode employée.

B. Systèmes par interversion.

Le *système par interversion* consiste dans le relèvement des lettres dans un ordre irrégulier, produit par l'emploi d'une clef littérale ou numérique, ou par une convention qui constitue alors la clef; d'où deux genres de méthodes :

I. les méthodes à clefs littérales ou numériques.

II. les méthodes à clefs-convention.

Méthodes a clefs littérales — ou numériques.

1° *Méthode des diviseurs à simple clef ou méthode des marchands.* On dispose les lettres du texte clair en autant de colonnes verticales que la clef comporte de lettres.

Si le nombre des lettres n'est pas un multiple exact du nombre des lettres de la clef, on ajoute à la dernière ligne horizontale le nombre voulu de lettres nulles, pour compléter le tableau. Ainsi, la phrase : « L'ennemi est signalé dans la direction de Tongres », cryptographiée avec la clef *Jean*, comprendra quatre colonnes verticales de 11 lettres, complétées par des nulles x, y, z, soulignées.

On pourrait intervertir les colonnes d'une façon arbitraire, suivant une clef numérique donnée. Ainsi, au lieu de les écrire dans l'ordre naturel 1, 2, 3, 4, on les écrira 1, 3, 2, 4 ou 4, 1, 2, 3, etc.

Mais comme il faut un effort de mémoire pour retenir cette clef numérique, surtout si le nombre des colonnes est grand, on emploie toujours une clef littérale qu'on change facilement en clef numérique.

Cette clef littérale est un mot ou une phrase, qui se retient sans notes écrites.

On transforme la clef littérale *Jean* en formule numérique, en numérotant les lettres de ce mot suivant le rang alphabétique des caractères qui le composent. Sous la clef, on écrit le texte à chiffer de la manière indiquée ci-après (fig. 1), puis on relève ces colonnes de lettres dans leur ordre naturel, et l'on obtient (fig. 2) :

J	E	A	N
3	2	1	4
l	e	n	n
e	m	i	e
s	t	s	i
g	n	a	l
e	d	a	n
s	l	a	d
i	r	e	c
t	i	o	n
d	e	t	o
n	g	r	e
s	*x*	*y*	*z*

(fig. 1.)

A	E	J	N
1	2	3	4
n	e	l	n
i	m	e	e
s	t	s	i
a	n	g	l
a	d	e	n
a	l	s	d
e	r	i	c
o	i	t	n
t	e	d	o
r	g	n	e
y	*x*	s	*z*

(fig. 2.)

Ce qui fournit le cryptogramme :

nelni — meest — siang — laden — alsde — ricoi — tnted — orgne — yxsz.

La *lecture* de ce chiffre se fait en répartissant les caractères qui le composent, en autant de colonnes verticales qu'il y a de lettres dans le mot-clef. Puis on rétablit l'ordre dans la disposition des colonnes, en les rangeant d'après la place des lettres dans le mot clef.

Le nom de cette méthode provient de ce que les marchands marquent souvent en caractères secrets le prix de revient de leurs marchandises, afin de connaître la mesure de leurs concessions, lors du marchandage.

La clef de ce moyen mnémonique est un membre de phrase, ou mieux un mot suffisamment long, pour y trouver 10 lettres différentes numérotées dans l'ordre de leur rang alphabétique, pour figurer les 10 chiffres.

Ainsi, si *champigone* est le mot-clef, on numérote ses lettres de la manière suivante :

c h a m p i g o n e
2 5 1 7 0 6 4 9 8 3

Déchiffrement. — Soit à déchiffrer le cryptogramme usjee — voran — iveru — ndies — msett — ioniv — dresv — macis — depzn — ckgt.

L'opération comprend deux séries de tâtonnements: la première consiste à déterminer le nombre de lettres de la clef.

La dépêche comprend 49 caractères. Or, $49=7^2$, d'où l'on peut conclure que la clef est composée de 7 lettres. Lorsque le nombre de lettres de la clef est multiple de plusieurs facteurs premiers, les premiers tâtonnements sont un peu plus longs. On en est réduit à essayer plusieurs diviseurs, mais l'application des principes résultant de la connaissance des particularités de la langue, réduit ces préliminaires dans une large mesure.

Le nombre de lettres 49, peut d'ailleurs n'être pas réel, et provenir du texte suivi d'un certain nombre de nulles.

Pour s'assurer de la rectitude de l'essai, on dispose les lettres du cryptogramme en colonnes verticales, qui, si le nombre de lettres du mot-clef est exact, sont précisément la disposition des colonnes, transposées dans l'ordre naturel des chiffres.

Dans la deuxième série des recherches, il s'agit de placer les rangées de chiffres dans l'ordre indiqué par les lettres de la clef. Nous ne pouvons avoir que les tableaux *a* et *b* :

Tableau *a*.

1	2	3	4	5	6	7
u	r	u	s	i	m	p
s	a	n	e	v	a	z
j	n	d	t	d	e	n
e	i	i	t	r	i	c
e	v	e	i	e	s	k
v	e	s	o	s	d	g
o	r	m	n	v	e	t

Tableau *b*.

1	2	3	4	5	6	7
u	s	j	e	e	v	o
r	a	n	i	v	e	r
u	n	d	i	e	s	m
s	e	t	t	i	o	n
i	v	d	r	e	s	v
m	a	e	i	s	d	e
p	z	n	e	k	g	t

Nous savons que le pourcent des voyelles est 45.00, mais que l'écart peut le faire varier entre 30 % et 60 %. Le texte comprend ici 19 voyelles, sur 49 lettres. Comme il y a 7 lignes, cela fait une moyenne de 2.71 par ligne. Dans le tableau *a*, ce nombre de voyelles, dans les diverses lignes, est respectivement de 3/7, 3/7, 1/7, 4/7, 4/7, 2/7, 2/7. Dans le tableau *b*, ces nombres sont respectivement 4/7, 3/7, 3/7, 3/7, 2/7, 4/7, 0/7.

A considérer ces deux séries de fractions, leurs différences avec 2.71/7, pourraient nous amener à rejeter la seconde, à cause de l'écart maximum 0-2.71. Mais si l'on réserve ce chiffre, en admettant que la dernière ligne contienne les nulles, on remarque que l'écart moyen est plus petit, dans la seconde série (tableau b), que dans la première (tableau a). Ces comparaisons et ces constatations seront d'autant plus aisées que le texte sera plus long.

Si le nombre de lignes horizontales n'est pas le même dans les tableaux d'essai, on prendra la moyenne des voyelles par ligne, afin d'établir l'écart moyen correspondant, ce qui permettra encore la *comparaison* et le *choix*, par exclusion.

Admettons que le tableau b soit le bon. Pour rétablir les colonnes dans leur ordre normal, on essayera de constituer un sens par l'interversion logique des lettres d'une ligne; lorsque ce résultat sera obtenu, le rétablissement des colonnes sera un fait accompli.

Nous chercherons d'abord à juxtaposer les colonnes en faisant usage des particularités connues de la langue.

Les premiers essais doivent être tentés sur les lettres qui offrent peu de combinaisons, telles que *Q, X, H, J, E, Y*, que le capitaine Valério dénomme *indicatrices*. Le tableau n'offre ici ni *Q*, ni *X*.

La première ligne présente cependant un *J*, qui est toujours suivi d'une voyelle.

Les combinaisons 3-1, 3-4, 3-5 et 3-7 sont donc admissibles à priori; mais il faut rejeter 3-1 qui fournit à la fois les bigrammes *nr* et *ts*, et 3-7 qui donne les bigrammes *nr, dm, tn, dv;* il reste donc les combinaisons 3-4 et 3-5; la première fournit les bigrammes peu fréquents dr, ei; 3-5 sera donc la plus probable. (Nous n'avons pas tenu compte de la dernière ligne, puisque nous avons supposé qu'elle contenait les nulles).

Rétablissons ces colonnes, nous aurons : (tableau c).

3	5		1	2	4	6	7
j	e		u	s	e	v	o
n	v		r	a	i	e	r
d	e		u	n	i	s	m
t	i		s	e	t	o	n
d	e		i	v	r	s	v
e	s		m	a	j	d	e
n	k		p	z	c	g	t

Il faut ensuite déterminer les trigrammes. Le bigramme *je* est presque toujours suivi d'une consonne; un trigramme s'annonce dès lors sur la première ligne 3-5-2 et-3-5-6 ; le bigramme *de* est dans le même cas que *je*. Cela nous conduit à rejeter 3-5-2, après essai (*des* est d'ailleurs beaucoup plus fréquent que *den* ou *dex*), et à adopter 3-5-6, qui répond à toutes les exigences et donne : (tableau *d*).

3	5	6
j	e	v
n	v	e
d	e	s
t	i	o
d	e	s
e	s	d
n	k	g

1	2	4	7
u	s	e	o
r	a	i	r
u	n	i	m
s	e	t	n
i	v	r	v
m	a	i	e
p	z	e	t

Arrivé à ce point, on remarque que le trigramme *n r e* ne peut admettre que la lettre *r*, ce qui annonce les combinaisons 3-5-6-1 ou 3-5-6-7 ; *tio* appelle sûrement *n*, ce qui nous amène à adopter 3-5-6-7 ; nous aurons : (tableau *e*).

3	5	6	7	1	2	4
J	e	v	o	u	s	e
n	v	e	r	r	a	i
d	e	s	m	u	n	i
t	i	o	n	s	l	t
d	e	s	v	i	v	r
e	s	d	e	m	a	i
n	k	g	t	p	z	e

Ces fragments du tableau *e* se juxtaposent aisément pour former la phrase: « Je vous enverrai des munitions et des vivres demain », suivie des six nulles k, g, t, p, z, e.

Lorsqu'on a à déchiffrer à la fois, plusieurs cryptogrammes

composés avec la même clef, le problème est beaucoup plus facile. Si dans un chiffre, plusieurs combinaisons binaires ou ternaires sont possibles, il faudra adopter celle, ou une de celles qui se présentent dans chaque dépêche.

2° *Méthode des diviseurs à double clef.* — On peut intervertir à la fois l'ordre des colonnes verticales et celui des colonnes horizontales. Il faut prendre une clef double pour donner quelque sécurité au système.

Soit à chiffrer le texte : « Je vous enverrai des munitions et des vivres demain ».

Prenons comme clef verticale, le mot *Louvain*, nous aurons le tableau (n° 1). Le relèvement de ces colonnes de lettres, dans leur ordre naturel, donne le tableau (n° 2).

L	O	U	V	A	I	N
3	5	6	7	1	2	4
j	e	v	o	u	s	e
n	v	e	r	r	a	i
d	e	s	m	u	n	i
t	i	o	n	s	e	t
d	e	s	v	i	v	r
e	s	d	e	m	a	i
n	k	g	t	p	r	c

(N° 1)

A	I	L	N	O	U	V
1	2	3	4	5	6	7
u	s	j	e	e	v	o
r	a	n	i	v	e	r
u	n	d	i	e	s	m
s	e	t	t	i	o	n
i	v	d	r	e	s	v
m	a	e	i	s	d	e
p	r	n	c	k	g	t

(N° 2)

Pour la seconde clef, nous devons choisir un membre de phrase assez long, pour qu'on puisse y trouver au minimum, autant de lettres qu'il y a de colonnes horizontales, afin qu'on ne soit jamais arrêté dans le chiffrement, par la longueur de la dépêche. Nous adopterons par exemple : « Bruxelles est la capitale de la Belgique. » Notre cryptogramme, mis en colonnes, comporte 7 lignes horizontales ; la clef verticale sera donc composée des sept premières lettres : Bruxell, qui transformée, en clef numérique donne :

b	e	l	l	r	u	x
1	2	3	4	5	6	7

et nous aurons le tableau suivant : (n° 3).

	A	I	L	N	O	U	V
	1	2	3	4	5	6	7
B	1	u	s	j	e	e	v	o
R	5	r	a	n	i	v	e	r
U	6	u	u	d	i	e	s	m
X	7	s	e	t	t	i	o	n
E	2	i	v	d	r	e	s	v
L	3	m	a	e	i	s	d	e
L	4	p	z	n	c	k	g	t

n° 3

qui transformé par la clef verticale donne : (n° 4).

	A	I	L	N	O	U	V
	1	2	3	4	5	6	7
B	1	u	s	j	e	e	v	o
E	2	i	v	d	r	e	s	v
L	3	m	a	e	i	s	d	e
L	4	p	z	n	c	k	g	t
R	5	r	a	n	i	v	e	r
U	6	u	u	d	i	e	s	m
X	7	s	e	t	t	i	o	n

n° 4

et fournit le cryptogramme ci-après :

usjee — voivd — resvm — aeisd — epzne — kgtra — niver — uudie — smset — tion.

La *lecture* d'un tel cryptogramme s'obtient comme précédemment, en disposant les lettres en colonnes verticales et lignes horizontales, et en rétablissant l'ordre normal, d'après celui des lettres des mots-clefs.

Remarque. Lorsque la longueur de la dépêche à chiffrer est telle, que le nombre total des lettres dépasse le produit du nombre de lettres de chacune des clefs horizontale et verticale, on cryptographie le texte en plusieurs parties. Le nombre de colonnes verticales ne varie pas; le chiffrement

du reste, se fait en réduisant le nombre de lignes horizontales à ce qui est nécessaire, et en complétant, s'il y a lieu, la dernière par des nulles.

3° *Méthode à triple clef.*—Si nous appliquons la méthode précédente à un texte déjà chiffré dans un autre système, nous aurons un texte cryptographié avec une triple clef.

Déchiffrement d'un cryptogramme chiffré par la méthode à double clef. — Soit le cryptogramme : exhng — ydfqw —lrree — nicim —tsnsl— gacce -- hrite — ntris— icabe —reldn—nceuu—onane— lzvrv — inroe — nsane — tvoce — sxaru — vienn — oneud — neeih — smana — uesal — udeld — namse — uveoe — ctrov — scaer — rlurp — oiirr — uaiap — irqte — daebs — rleec — mssar — uuqrt — sonei — if.

Le chiffre contient 182 lettres, dont 76 voyelles. $182 = 2 \times 7 \times 13$. Il est très probable que la clef contient plus de deux lettres ; les clefs possibles sont donc 7, 13, 14 ou 26.

Essayons d'abord la clef 7. Par cela même, nous essayons la clef 26, puisque $7 \times 26 = 182$.

Etablissons donc les deux tableaux qui peuvent être obtenus par l'emploi de ces deux clefs, le texte pouvant avoir été écrit horizontalement ou verticalement.

Tableau *a*.

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

	1	2	3	4	5	6	7
14	n	e	u	d	n	e	e
15	i	h	s	m	a	n	a
16	u	e	s	a	l	u	d
17	e	l	d	n	a	m	s
18	e	u	v	e	o	e	c
19	t	r	o	v	s	e	a
20	e	r	r	l	u	r	p
21	o	i	i	r	r	u	a
22	i	a	p	i	r	q	t
23	e	d	a	e	b	s	r
24	l	e	e	c	m	s	s
25	a	r	u	u	q	r	t
26	s	o	n	e	i	i	f

Tableau *b*.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	e	x	h	n	g	y	d	f	q	w	l	r	r	e	e	n	i	e	i	m	t	s	n	s	l	g
2	a	e	c	c	h	r	i	t	e	n	t	r	i	s	i	e	a	b	e	r	e	l	d	n	n	c
3	e	u	u	o	n	a	n	e	l	z	v	r	v	i	n	r	o	e	n	s	a	n	e	t	v	o
4	c	e	s	x	a	r	u	v	i	e	n	n	o	n	e	u	d	n	e	e	i	h	s	m	a	n
5	a	u	e	s	a	l	u	d	e	l	d	n	a	m	s	e	u	v	e	o	e	c	t	r	o	v
6	s	c	a	e	r	r	l	u	r	p	o	i	i	r	r	u	a	i	a	p	i	r	q	t	e	d
7	a	e	b	s	r	l	e	e	c	m	s	s	a	r	u	u	q	r	t	s	o	n	e	i	i	f

Le tableau *a* comprenant 26 lignes, chacune de celle-ci devra contenir $\frac{79}{26} = 3.04$ voyelles; le tableau *b*, $\frac{79}{7} = 11.28$ voyelles.

A l'inspection du tableau *a*, on voit, dès les premières lignes, que les écarts sont fort grands; nous excluons donc la clef de 7 chiffres de nos recherches.

Dans le tableau *b*, nous remarquons que, sauf pour la première ligne, le nombre de voyelles de chaque ligne est à peu près le même : 6, 11, 13, 13, 13, 12, 11. La grande différence de la première ligne provient sans doute des nulles qui ont été ajoutées au texte transposé. Si cette hypothèse se vérifie, ce sera un indice de ce que les lignes horizontales ont été interverties. Si l'on réserve la 1re ligne, on remarque que 6 lignes contiennent 73 voyelles, soit une moyenne de 12.17, ce qui équivaut à peu près, à ce que nous avons trouvé plus haut.

Nous allons donc admettre une clef horizontale de 26 lettres, et nous allons encore vérifier si le texte n'a pas été transcrit en colonnes verticales. Nous trouvons pour les premières colonnes verticales du tableau *b*, respectivement :

5, 5, 2, 2, 2, 1, 4, 4, etc., voyelles au lieu de 3 en moyenne, ce qui, à cause de ces écarts trop sensibles, confirme notre supposition; si nous faisons le compte des fréquences en supposant une clef horizontale de 13 lettres, ou 6.08 voyelles

par ligne, nous trouvons respectivement 7, 9, 7, 7, 5, 6, 6, 10; il en résulte que quelle que soit la clef horizontale, 13 ou 26 lettres, le texte a été transcrit horizontalement.

Nous ne travaillerons pas ferme pour le moment sur la première ligne, à cause des nulles que nous croyons y avoir découvert; la 4e ligne contient une *x*, généralement précédée de *a*, la 6e et la 7e comprennent un q, toujours suivi de u ; les combinaisons 7-4, 16-4, 26-4 (4e ligne); 23-8, 23-16 (6e ligne) 17-15, 17-16 (7e ligne) paraissent possibles ; mais 26-4 (oo, v s, f s) ; 23-8 (n f, dt, sv, td) sont improbables ; 17-16 (ae et ua), et 16-4 (ue, cc) sont moins probables que 7-4. Nous retenons donc 7-4, 23-16 et 17-15 : La 2e et la 5e lignes contiennent une *h*, (la 1re aussi, pour mémoire), la 3e ligne comprend un *z*. Les combinaisons 3-5, 4-5, 26-5 (2e ligne), 1-22 (4e ligne), 3-1, 3-14, 3-15, 3-18 (1e ligne) ; 5-3, 5-4, 5-9, 5-16, 5-19, 5-21 (2e ligne) ; 22-2, 22-10, 22-15, 22-19, 22-20 (4e ligne) ; 1-10, 8-10, 18-10, 23-10 (3e ligne) sont possibles. Mais 4-5 (sr), 26-5 (fr), 1-2 (sr), 3-1 (sc), 3-16 (cs, sn), 3-18 (cb, sn), 5-3 (aa), 5-4 (hc, rs), 5-9 (nl, rc), 5-16 (nr), 5-19 (rt), 5-21 (ae), 22-2 (rc), 22-10 (ln), 22-15 (cs), 22-20 (lr, ns), 8-10 (tn, dc), 18-10 (bn), 23-10 (qp) sont improbables ; 5-21 (ae), est peu probable.

De ces observations, nous concluons momentanément à la probabilité des combinaisaisons 7-4, 23-16, 17-15, d'une part; pour x et q, et 3-5, 1-10, 3-15, d'autre part, pour h et z. Nous remarquons aussi que jusqu'ici, aucune séquence n'a trouvé de possibilité entre les nombres inférieurs et supérieurs de la série 1 à 26. Nous déduisons de là la probabilité d'avoir une clef de $\frac{26}{2} = 13$ lettres, et à partir de ce moment, nous allons opérer d'après cette nouvelle hypothèse. Si nous avons commis une erreur, nous nous en apercevrons bientôt, et cela ne fera aucun tort à nos re-

cherches. Disposons donc le cryptogramme suivant le tableau c ci-dessous :

Tableau *c*.

	1	2	3	4	5	6	7	8	9	10	11	12	13
1	e	x	h	n	g	y	d	f	q	w	l	r	r
2	e	e	n	i	e	i	m	t	s	n	s	l	g
3	a	e	c	c	h	r	i	t	e	n	t	r	i
4	s	i	e	a	b	e	r	e	l	d	n	n	c
5	c	u	u	o	n	a	n	e	l	z	v	r	v
6	i	n	r	o	e	n	s	a	n	e	t	v	o
7	c	e	s	x	a	r	u	v	i	e	n	n	o
8	n	e	u	d	n	e	e	i	h	s	m	a	u
9	a	u	e	s	a	l	u	d	e	l	d	n	a
10	m	s	e	u	v	e	o	e	c	t	r	o	v
11	s	c	a	e	r	r	l	u	r	p	o	i	i
12	r	r	u	a	i	a	p	i	r	q	t	e	d
13	a	e	b	s	r	l	e	e	c	m	s	s	a
14	r	u	u	q	r	t	s	o	n	e	i	i	f

Réunissons actuellement les colonnes-séquences déduites de nos raisonnements; excluons 3-15, et nous aurons 1-10, 10-3, 3-5, 7-4 et 4-2, (17-15) :

Tableau *d*.

	1-10	10-3	3-5	7-4	4-2	6	8	9	11	12	13
1	e-w	w-h	h-g	d-n	n-x	y	f	q	l	r	r
2	e-n	n-n	n-e	m-i	i-e	i	t	s	s	l	g
3	a-n	n-c	c-h	i-c	c-e	r	t	e	t	r	i
4	s-d	d-e	e-b	r-a	a-i	e	e	l	n	n	c
5	c-z	z-u	u-n	n-o	o-u	a	e	l	v	r	v
6	i-e	e-r	r-e	s-o	o-n	n	a	n	t	v	o
7	c-e	e-s	s-a	u-x	x-e	r	v	i	n	n	o
8	n-s	s-u	u-n	e-d	d-e	e	i	h	m	a	u
9	a-l	l-e	e-a	u-s	s-u	l	d	e	d	n	a
10	m-t	t-e	e-v	o-u	u-s	e	e	c	r	o	v
11	s-p	p-a	a-r	l-e	e-c	r	u	r	o	i	i
12	r-q	q-u	u-i	p-a	a-r	a	i	r	t	e	d
13	a-m	m-b	b-r	e-s	s-e	l	e	c	s	s	a
14	r-e	e-u	u-r	s-q	p-n	t	o	n	i	i	f

Nous allons maintenant essayer d'unir les quatrigrammes 1-10-3-5 aux trigrammes 7-4-2, et aux lettres des colonnes encore disponibles.

A la 2e ligne, nous remarquons que le quatrigramme *enne* s'unit parfaitement au trigramme *mie*, et qu'il en est de même des suivants. Nous obtenons donc 7 colonnes verticales, et nous remarquons, à la 14e ligne, le bigramme *qu* qui demande après lui une voyelle, d'où 11 ou 12 (parce que *quo* est moins probable); à la 11e ligne *ec* demande une voyelle, par suite du polygramme *parle* qui précède, d'où 11-12 ou 11-13; le bigramme *co*, le plus fréquent des trois, est le plus probable. Cela est confirmé par le peu de probabilité de la séquence *co* après *ux* (7e ligne). Joignons la 11e colonne, et nous obtenons :

Tableau *e*.

	1-10	3-5	7-4	2	11	6	8	9	12	13
1	e w	h g	d n	x	l	y	f	q	r	r
2	e n	n e	m i	e	s	i	t	s	l	g
3	a n	c h	i c	e	t	r	t	e	r	i
4	s d	e b	r a	i	n	c	e	l	n	c
5	e z	u n	n o	u	v	a	e	l	r	v
6	i e	r e	s o	n	t	n	a	n	v	o
7	c e	s a	u x	e	n	r	v	i	n	o
8	n s	u n	e d	e	m	e	i	h	a	u
9	a l	e a	u s	u	d	l	d	e	n	a
10	m t	e v	o u	s	r	e	c	c	o	v
11	s p	a r	l e	c	o	r	u	r	i	i
12	r q	u i	p a	r	t	a	i	r	e	d
13	a m	b r	e s	e	s	l	e	c	s	a
14	r e	u r	s q	u	i	t	o	n	i	f

Les mots formés par la réunion des colonnes donnent de sérieuses indications pour achever le travail : A la 3e ligne *c e t* sera suivi de *te* ; la colonne 11 sera donc suivie de 8-9

ou de 11-9; *nouv* (5e ligne) sera suivi probablement de *e*, donc 11-8; au *sud* sera suivi probablement de *de* donc 11-8 (9e ligne); *qui part* sera probablement suivi de *ira*, donc 11-8-9-6 (12e ligne).

En adoptant 11-8-9-6, on conclut (11e ligne), à *courrier*, d'où 11-8-9-6-12 ou 13; à la 5e ligne, *nouve-l a v-* 12 ou 13; à la 6e ligne, *sont ann* -13.

Nous avons dès lors le tableau f:

Tableau *f*.

	1	10	3	5	7	4	2	11	8	9	6	13	12
1	e	w	h	g	d	n	x	l	f	q	y	r	r
2	e	n	n	e	m	i	e	s	t	s	i	g	l
3	a	n	c	h	i	c	e	t	t	e	r	i	r
4	s	d	e	b	r	a	i	n	e	l	e	c	n
5	e	z	u	n	n	o	u	v	e	l	a	v	r
6	i	e	r	e	s	o	n	t	a	n	n	o	v
7	c	e	s	a	u	x	e	n	v	i	r	o	n
8	n	s	u	n	e	d	e	m	i	h	e	u	a
9	a	l	e	a	u	s	u	d	b	e	l	a	n
10	m	t	e	v	o	u	s	r	e	c	e	v	o
11	s	p	a	r	l	e	c	o	u	r	r	i	i
12	r	q	u	i	p	a	r	t	i	r	a	d	e
13	a	m	b	r	e	s	e	s	e	e	l	a	s
14	r	e	u	r	s	q	u	i	o	n	t	f	i

Nous constatons que les séquences 13-12 ne sont pas admissibles pour la plupart, mais que si l'on reporte la 12e colonne à la gauche de la 1e, les bigrammes 12-1 répondent à toutes les exigences.

Il ne nous reste plus dès lors qu'à intervertir l'ordre des lignes horizontales pour former un sens continu.

En reportant la 1re ligne après la 14e, nous voyons

que la 2e ligne s'accorde en sens, avec la 9e qui demande après elle la 13e, et ainsi de suite.

Nous constatons encore que le cryptogramme n'a pas été écrit suivant les colonnes verticales.

Le cryptogramme déchiffré fournit enfin la phrase : « L'ennemi est signalé au sud de la Sambre; ses éclaireurs, qui ont franchi cette rivière, sont annoncés aux environs de Braine-le-Comte; vous recevrez un nouvel avis par le courrier qui partira dans une demi-heure, » suivie des nulles w, h, g, d, n, n, l, f, q, y, r.

Les explications fort longues qui accompagnent cette méthode de déchiffrement ne doivent pas faire croire à la longueur des opérations. Celles-ci ne durent guère pour le cryptologue exercé. On dispose de tableaux et de chiffons de papier « ad-hoc », et les résultats obtenus s'y inscrivent au fur et à mesure de leur obtention.

On s'assimilera le sens de cette méthode en se rendant compte de ce qu'un chiffre donné ne peut quitter, ni sa colonne verticale, ni sa ligne horizontale ; par conséquent, tous les caractères qui se trouvent sur une ligne ou dans une colonne, sont liés les uns aux autres; ils ne subissent entre eux que des permutations qu'il s'agit de rétablir dans leur ordre initial, par l'application des lois linguistes vues précédemment.

4° *Méthode par tronçonnement.* — On choisit dans un livre usuel, une clef littérale assez longue, de manière à pouvoir la transformer en clef numérique de 10, 20, 30..... 100 nombres consécutifs.

Soit la clef littérale, copiée du Règlement sur le service en campagne : « En cas de mort, de rappel, de démission ou d'absence temporaire, tout titulaire d'un commandement est provisoirement remplacé par l'officier le plus ancien parmi les officiers du grade le plus élevé que comprend ce commandement. »

Supposons qu'il soit convenu de composer la clef

numérique de 50 nombres, de 1 à 50 ; nous écrirons les 50 premières lettres de la phrase ci-dessus, et nous les numéroterons suivant leur rang alphabétique. Nous obtenons :

E n c a s d e m o r t d e r a p p e l
14 30 6 1 44 9 15 27 33 40 48 10 16 41 2 37 38 17 26
d e d e m i s s i o n o u d a b s c e
11 18 12 19 28 23 45 46 24 34 31 35 50 13 3 5 47 7 20
n c e t e m p o r a i r
32 8 21 49 22 29 39 36 42 4 25 43

La dépêche est divisée en tronçons de moins de 50 lettres; chaque tronçon est suivi de quelques nulles, afin de séparer nettement le texte réel des nulles qui seront ajoutées pour compléter le cryptogramme.

L'adjonction de ces nulles a pour objet d'augmenter la résistance au déchiffrement et de dérouter le déchiffreur ; mais pour ne pas offrir à ce dernier des points de repère provenant de la fréquence anormale de certaines lettres, les nulles sont choisies dans une phrase auxiliaire telle que : « L'armée fait la force d'une nation autant que sa richesse ». Ces nulles sont inscrites à la suite des lettres de la dépêche, par colonnes verticales, jusqu'à ce que les cases soient remplies.

Soit à cryptographier : « La place n'a plus que pour dix jours de vivres ; les munitions se font rares ; il faut absolument que nous soyons secourus avant la fin du mois. »

La dépêche est transcrite en clair, par tronçons, sur une feuille de papier préparée à cet effet, et divisée en colonnes pouvant contenir 5 caractères. A la partie inférieure des colonnes, on inscrit les chiffres de la clef numérique, dans l'ordre indiqué plus haut. On obtient : (Tableau n° 1.)

l a p l a	c e n a p	l u s q u
l e s m u	n i t i o	n s s e f
q u e n o	u s s o y	o n s s e
14. 30. 6. 1. 44.	9. 15. 27. 33. 40.	48. 10. 16. 41. 2.

e p o u r	d i x j o	u r s d e
o n t r a	r e s i l	f a u t a
c o u r u	s a v a n	t l a f i
37. 38. 17. 26. 11.	18. 12. 19. 28. 23.	45. 46. 24. 34. 31.
v i v r e	s *x* *y* *p* *t*	*l* *r* *e* *a* *l*
b s o l u	m e n t *k*	*w* *x* *e* *i* *a*
n d u m o	i s *y* *k* *p*	*a* *m* *f* *t* *f*
35. 50. 13. 3. 5.	47. 7. 20. 32. 8.	21. 49. 22. 29. 39.

o *e* *n* *a* *o*
r *d* *e* *t* *n*
c *a* *n* *i* *a*

36. 42. 4. 25. 43.

Un tableau de transposition comprenant des portées horizontales, reçoit la dépêche ; en rangeant les colonnes dans l'ordre numérique, nous obtenons : (Tableau n° 2).

Portée du 1er tronçon.

1 2 3 4 5 6 7 8 9 10 11 12 13 14
26 27 28 29 30 31 32 33 34 35 36 37 38
l u e n e p x t e u r i v l
u n j a a e p a d v o e p
15 16 17 18 19 20 21 22 23 24 25
39 40 41 42 43 44 45 46 47 48 49 50
e s o d x y l e o s a
l p q e o a u r s l r i

Portée du 2e tronçon.

m f l e u s e k n s a e l l
r t i i e a t i t b r o n
i s t r s n w e l u t
a o e d n u f a m n x s

Portée du 3e tronçon.

n e m n o c s p u n u a u q
r s a t u i k o f n c c o
s s u s v y a f n a i
f y s u a o t l i o m d

On relève les lettres du texte transposé par groupes de cinq caractères, comme précédemment, en commençant par la première portée, et l'on obtient :

luene — pxteu — rivle — sodxy — leosa — unjaa —
epadv — oeplp — qeoau — rslri — mfleu — sekns —
aelli — strsn — welut — rtiic — atitb — ronao —
ednuf — amnxs — nemno — espun — uauqs — susvy —
afnai — rsatu — ikofn — ccofy — suaot — liomd.

La *lecture* d'un pareil cryptogramme se fait en divisant le texte chiffré, en tronçons de 50 caractères qu'on écrit les uns en dessous des autres, de manière que les colonnes verticales se correspondent exactement. Celles-ci sont numérotées de 1 à 50.

5 10 15 20 25
l u e n e — p x t e n — r i v l e — s o d x y — l e o s a
m f l e u — s e k n s — a e l l i — s t r s n — w e l u t
m e m n o — e s p u n — u a u q s — s u s v y — a f n a i

30 35 40 45 50
u n j a a — e p a d v — o e p l p — q e o a u — r s l r i
r t i i c — a t i t b — r o n a o — e d n u f — a m n x s
r s a t u — i k o f n — c c o f y — s u a o t — l i o m d

On rétablit ensuite l'ordre indiqué par la clef littérale numérotée ; on obtient : (Tableau n° 3.)

14. 30. 6. 1. 44. 9. 15. 27. 33. 40. 48. 10. 16. 41. 2. 37. 38.
l a p l a c e n a p l u s q u e p
l e s m u u i t i o n s s e f o n
q u e n o u s s o y o n s s e c o

17. 26. 11. 18. 12. 19. 28. 23. 45. 46. 24. 34. 31. 35. 50. 13.
o u r d i x j o u r s d e v i v
t r a r e s i l f a u t a b s o
u r u s a v a n t l a f i n d u
3. 5. 47. 7. 20. 32. 8. 21. 49. 22. 29. 39. 36. 42. 4. 25. 43
r e s *x y p t l r*
l u m e n t *k w x e*
m o i s *y k p a*

Dès que les nulles se déclarent, il est inutile de continuer la transposition.

Déchiffrement. — Cette méthode est longue, laborieuse et exige une grande attention. Rien que pour ces motifs, son emploi n'est pas à recommander. Les complications apparentes auxquelles on a recours, n'empêchent pas ces cryptogrammes d'être aisément déchiffrables. Le nombre de lettres du chiffre est un premier indice, et le chercheur aura bientôt fait de découvrir le nombre de lettres de la clef, ce qui permettra la mise en colonnes du cryptogramme.

Dès lors, les règles linguistiques sur la séquence des lettres indiqueront au cryptologue les essais de permutation à faire entre les colonnes, et après quelques tâtonnements, le déchiffrement sera opéré. Le procédé suivi pour le cas d'interversion irrégulière, examiné précédemment, (méthode des diviseurs à simple clef) est entièrement applicable ici.

5° *Taquin cryptographique* (1). Le capitaine d'artillerie Delauney a imaginé un système d'inversion des lettres du texte clair par l'utilisation des cubes en bois du jeu de « taquin », très en faveur il y a quelques années.

La méthode consiste à faire choix d'une clef de 16 lettres par le mode indiqué précédemment. Les lettres répétées seront marquées d'un indice pour les distinguer des précé-

(1) Voir à ce sujet le grand dictionnaire Larousse — tome XVII.

dentes. On inscrit une lettre de la clef sur chacun des cubes du taquin. Soit la clef :

Louvain	e	s	t	u	n	c	h	e	f	-	lieu.
1234567	8	9	10	11	12	13	14	15	16		

Nous aurons (tableau *a*) :

L	O	U_1	V
A	I	N_1	E_1
S	T	U^2	N_2
C	H	E_2	F

On inscrit ensuite successivement les 16 premiers caractères du texte clair dans les 16 cases du taquin ; puis la seconde série de 16, à gauche ou à droite des premiers, et ainsi de suite.

Le texte transposé, on replace les cubes dans la boîte en intervertissant l'ordre dans les lignes et les colonnes, et l'on fait parvenir le jeu à son correspondant.

Soit à cryptographier la phrase : « La ville s'est rendue. Nous avons fait prisonniers six mille hommes. » Nous aurons (tableau *b*) :

L ilee	O sanh	U_1 ovoo	V nium
A nlsm	I ilac	N_1 eevs	E_1 rsos
S senp	T ssso	U_2 itfk	N_2 xrau
C meiv	H intb	E_2 ldpc	F lurd

Si le texte doit être télégraphié, nous obtiendrons le cryptogramme :

ilees — anhov — ooniu — mnlsm — ilaee — evsrs — ossen — pssso — itıkx — raume — ivint — bldpc — lurd —

Il faut avoir soin d'ajouter des *nulles* pour compléter les cases, sinon l'existence de groupes incomplets offrirait un premier indice pour la traduction.

La *lecture* se fait en disposant les cubes suivant l'ordre des lettres de la clef.

Déchiffrement. — Si la dépêche a été transmise télégraphiquement, il suffit de diviser le nombre de lettres par 16 pour obtenir le nombre de signes de chaque série. On dispose les lettres de chacune de celles-ci en colonnes, de gauche à droite, et l'on aura : (tableau *c*) :

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	i	s	o	n	n	i	e	r	s	s	i	x	m	i	l	l
2	l	a	v	i	l	l	e	s	e	s	t	r	e	n	d	u
3	e	n	o	u	s	a	v	o	n	s	f	a	i	t	p	r
4	e	h	o	m	m	e	s	s	p	o	k	u	v	b	c	d

Certes, personne ne se hasardera à expédier tel quel, un cryptogramme aussi bénévolement déchiffrable ; mais le procédé de déchiffrement réside dans la disposition que nous venons d'indiquer.

Si les groupes ont été brouillés en vue de la transmission télégraphique, ou pendant le transport dans la boîte, les colonnes 1 à 16 se présenteront dans un ordre quelconque que nous traiterons comme une méthode irrégulière de chiffrement à simple clef.

Si le transport s'est fait dans une boîte, on travaillera sur les lettres de la clef, qui offriront encore moins de résistance à la juxtaposition que les lettres du texte ; on appliquera le principe des séquences, et cela d'autant mieux qu'il y aura plus de lettres marquées d'un indice.

L'emploi de taquin de 25, 36, 49 cubes n'augmente pas beaucoup la difficulté de la traduction ; c'est toujours la réduction d'un chiffrement par une méthode à simple clef, facilitée par le groupement solidaire d'un certain nombre de lettres qui limite les essais et les tâtonnements.

6° Méthode du télégraphe aérien. — Cette méthode est basée sur le principe suivant : Trois signes quelconques 1, 2, 3, admettent $(3 \times 2 \times 1) = 6$ combinaisons : 1 2 3, 1 3 2, 2 1 3, 2 3 1, 3 1 2 et 3 2 1. Ecrivons chacun des chiffres de la première combinaison 1 2 3, en tête de trois colonnes verticales, et soit à chiffrer la phrase suivante : « L'ennemi est signalé sur la rive gauche de l'Escaut. Sa cavalerie a franchi ce fleuve à Audenarde et à Tournai ». On divise la dépêche en groupes de trois lettres en commençant par la gauche. Nous aurons :

len — nem — ies — tsi — gna — les — url — ari — veg — auc — hed — cle — sca — uts — aca — val — eri — caf — ran — chi — cef — leu — vea — and — ena — rde — eta — tou — rna — i *x z*. On ajoute des nulles au dernier groupe pour le compléter.

On transcrit ensuite et successivement chacun des groupes de lettres dans les colonnes à ce destinées, dans l'ordre indiqué par celui des chiffres de la colonne de gauche. Ainsi le premier groupe *len*, sera décomposé en inscrivant la première lettre *l*, dans la case 1, la 2e dans la case 3, et la 3e dans la case 2 ; le 2e groupe *nem* dispersera ses lettres respectivement dans les 2e, 1re et 3e cases, et ainsi de suite, jusqu'à ce que toute la dépêche soit transposée.

Lorsque la série des combinaisons a été épuisée une fois, on recommence, et l'on inscrit les nouvelles lettres à côté de celles qui sont déjà dans les colonnes. Nous aurons ainsi le tableau suivant :

Tableau n° 1.

	1	2	3
1 3 2	l l h v e r	n s d e f e	e c e a e d
2 1 3	e r l r c t	n u e c l e	m l e i n a
2 3 1	e r c a e o	s i a f a u	i a s e w t
3 1 2	i g s n d a	t v u r a r	s e t a u n
3 2 1	a c a i a z	n u c h n x	g a a c e i

On obtient le cryptogramme relevé et disposé pour la transmission en réunissant les lettres par groupes de 5, suivant les lignes horizontales ou les colonnes verticales, d'après convention. Nous avons alors :

lhve — rnsdl — feeee — acder — lrctn — ueele — mlein — aerca — eosia — fania — sevti — gsnda — tvura — rseta — dnaca — iaznn — chnxg — aacei.

Ceux qui manquent d'habitude pourraient se tromper dans la répartition variable des colonnes combinées ; nous leur conseillons d'écrire d'abord le texte en dispersant les groupes de trois lettres, suivant l'ordre naturel des colonnes, de la manière suivante :

Tableau n° 2.

1	2	3
l l h v e r	e e e a e d	n s d l f e
n u e e l e	e r l r c t	m l e i n a
i a s e v t	e r c a e o	s i a f a u
t v u r a r	s e t a u n	i g s n d a
g a a c e i	n n c h n *x*	a c a i a *z*

puis d'opérer les combinaisons marquées par la colonne de gauche du tableau n° 1 :

Tableau n° 3

l l h v e r	n s d l f e	e e e a e d
e r l r c t	n u e e l e	m l e i n a
e r c a e o	s i a f a u	i a s e v t
i g s n d a	t v u r a r	s e t a u n
a c a i a *z*	n a c h n *x*	g a a c e i

et nous remarquons que par l'emploi de ce petit artifice, nous sommes arrivés beaucoup plus facilement au chiffrement indiqué plus haut.

Pour lire un semblable chiffre, on compte les lettres du cryptogramme. Le nombre de lignes horizontales étant

toujours cinq et celui des colonnes étant trois, le nombre total des caractères divisé par 15 (5 × 3),fournit le nombre de lettres de chaque groupe. Si le quotient n'est pas exact, il doit être augmenté de *un* pour tenir compte du reste.

On peut dès lors écrire les groupes horizontalement ou verticalement, suivant que le relèvement a été fait d'après un de ces deux modes.

Pour la transcription horizontale, on écrit les groupes dans leurs colonnes respectives en suivant l'ordre naturel ; le reste divisé par 3 indique, le cas, échéant, le nombre de groupes qui doivent contenir un caractère de plus que les suivants.

Pour la transcription verticale, le nombre total des lettres divisé par 3, donne celui de chaque colonne. Ce nouveau chiffre divisé par 5, nombre de lignes horizontales, indique celui de chaque groupe ; le reste annonce le nombre de groupes (lignes) qui doivent contenir un caractère de plus.

Si l'on avait employé une combinaison de 4 ou 5 chiffres, on aurait dû grouper les lettres du texte clair par tranches de 4 ou 5, et introduire ces facteurs dans tous les calculs.

Au lieu de chiffres on pourrait aussi se servir de combinaisons de lettres, mais les risques d'erreurs sont plus grands.

Déchiffrement. — Le déchiffrement d'un cryptogramme chiffré par la méthode du télégraphe aérien est très simple, comme nous allons le montrer. Nous avons remarqué que le nombre des lignes horizontales et des colonnes verticales est fixe, et dépend du genre de combinaison choisi ; (3 ou 4 chiffres qui fournissent respectivement 3 ou 4 colonnes verticales et (6—1) ou (24—1) lignes horizontales). Les combinaisons de 2 lettres ne fournissent que 2 colonnes et 2 lignes; celles de 5 lettres, que 5 colonnes et (120—1) lignes. On voit donc que le champ des variations des clefs numériques est singulièrement restreint. On peut dès lors consi-

dérer que le produit du nombre de colonnes par celui du nombre de lignes est fixe et égal à 15 ou 92. (1)

Le quotient de la division du nombre total de lettres du texte par 15 ou 92, donnera donc le nombre de caractères contenus dans une horizontale de colonne, ou ce nombre moins un, s'il y a un reste. Ce résultat connu, on partage le cryptogramme en tranches de lettres égales à l'un de ces deux nombres, suivant le cas, et dès lors le texte clair peut être trouvé immédiatement, quelle que soit la manière dont les chiffres aient été relevés.

En effet, remplaçons les lettres du tableau n° 1 par les chiffres représentant leurs rangs dans le texte clair; nous aurons le tableau n° 4 ci-dessous.

Tableau n° 4.

1,16,31,46,61,76	3,18,33,48,63,78	2,17,32,47,62,77
5,20,35,50,65,80	4,19,34,49,64,79	6,21,36,51,66,81
8,23,38,53,68,83	9,24,39,54,69,84	7,22,37,52,67,82
12,27,42,57,72,87	10,25,40,55,70,85	11,26,41,56,71,86
15,30,45,60,75,90	14,29,44,59,74,89	13,28,43,58,73,88

Tous les nombres de ce tableau sont en progression par différence, dont la raison est 15, avec le premier chiffre de chaque horizontale de tableau.

Si le relèvement se fait horizontalement, les séries de progressions se suivent dans l'ordre : 1, 3, 2 — 5, 4, 6 — 8, 9, 7— 12, 10, 11— 15, 14, 13. Si le relèvement se fait verticalement, les séries de progressions se succèdent dans l'ordre: 1, 5, 8, 12, 15—3, 4, 9, 10, 14—2, 6, 7, 11, 13.

Dès lors, après certains tâtonnements consistant à juxtaposer quelques lettres de 15 en 15, vers la droite et vers la gauche, ou à s'assurer que le relèvement des caractères n'a pas été fait en employant une seconde clef-convention ; on s'apercevra bien vite de cet artifice, lorsqu'on aura vu les méthodes spéciales de transcription de ce genre. Le déchiffrement s'accomplira dès ce moment presqu'aussi vite que la lecture par les correspondants.

(1) 3 (6—1 ou 4 (24—1 .

Chapitre II. — Méthodes a clef-convention.

A. *Méthodes régulières des diviseurs à simple clef-convention.*

1. On peut convenir d'écrire les dépêches en clair sur un certain nombre de lignes horizontales ou de colonnes verticales ; on ajoute des nulles pour parfaire la dernière ligne.

On peut disposer le texte en commençant par la gauche ou par la droite, par le haut ou par le bas.

2. On peut aussi disperser les caractères du langage clair en boustrophédon ou en zig-zag, c'est-à-dire en inscrivant alternativement les lettres dans un sens, puis immédiatement après, sur la ligne ou dans la colonne suivante, en sens inverse.

3. On peut encore transposer les lettres d'une phrase suivant les diagonales d'un parallélogramme en sens direct, inverse, par le haut, par le bas.

4. Enfin on peut appliquer aux méthodes 3, les méthodes 2.

Supposons que la convention adoptée entre deux agents, soit d'écrire le texte clair sur six lignes.

Soit à cryptographier la phrase ; « L'ennemi est signalé au sud de la Sambre ; une pointe a atteint Thuin. »

On compte le nombre de lettres du texte (53) ; on le divise par 6 ce qui fait pour quotient 8, et pour reste 5 ; on ajoute à ce dernier une nulle et l'on a 6 lignes de 9 lettres.

Le cryptogramme peut donc être disposé d'une des manières indiquées dans les tableaux ci-après. Nous y remplacerons les lettres par leurs rangs dans la phrase.

1. Méthodes rectangulaires simples.

A. Horizontale.

1

1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27
28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54

2

9	8	7	6	5	4	3	2	1
18	17	16	15	14	13	12	11	10
27	26	25	24	23	22	21	20	19
36	35	34	33	32	31	30	29	28
45	44	43	42	41	40	39	38	37
54	53	52	51	50	49	48	47	46

3

46	47	48	49	50	51	52	53	54
37	38	39	40	41	42	43	44	45
28	29	30	31	32	33	34	35	36
19	20	21	22	23	24	25	26	27
10	11	12	13	14	15	16	17	18
1	2	3	4	5	6	7	8	9

4

54	53	52	51	50	49	48	47	46
45	44	43	42	41	40	39	38	37
36	35	34	33	32	31	30	29	28
27	26	25	24	23	22	21	20	19
18	17	16	15	14	13	12	11	10
9	8	7	6	5	4	3	2	1

B. Verticale.

5

1	7	13	19	25	31	37	43	49
2	8	14	20	26	32	38	44	50
3	9	15	21	27	33	39	45	51
4	10	16	22	28	34	40	46	52
5	11	17	23	29	35	41	47	53
6	12	18	24	30	36	42	48	54

6

49	43	37	31	25	19	13	7	1
50	44	38	32	26	20	14	8	2
51	45	39	33	27	21	15	9	3
52	46	40	34	28	22	16	10	4
53	47	41	35	29	23	17	11	5
54	48	42	36	30	24	18	12	6

7

6	12	18	24	30	36	42	48	54
5	11	17	23	29	35	41	47	53
4	10	16	22	28	34	40	46	52
3	9	15	21	27	33	39	45	51
2	8	14	20	26	32	38	44	50
1	7	13	19	25	31	37	43	49

8

54	48	42	36	30	24	18	12	6
53	47	41	35	29	23	17	11	5
52	46	40	34	28	22	16	10	4
51	45	39	33	27	21	15	9	3
50	44	38	32	26	20	14	8	2
49	43	37	31	25	19	13	7	1

2. *Méthodes rectangulaires en boustrophédon* (1).

A. Horizontale.

1

1	2	3	4	5	6	7	8	9
18	17	16	15	14	13	12	11	10
19	20	21	22	23	24	25	26	27
36	35	34	33	32	31	30	29	28
37	38	39	40	41	42	43	44	45
54	53	52	51	50	49	48	47	46

2

9	8	7	6	5	4	3	2	1
10	11	12	13	14	15	16	17	18
27	26	25	24	23	22	21	20	19
28	29	30	31	32	33	34	35	36
45	44	43	42	41	40	39	38	37
46	47	48	49	50	51	52	53	54

3

54	53	52	51	50	49	48	47	46
37	38	39	40	41	42	43	44	45
36	35	34	33	32	31	30	29	28
19	20	21	22	23	24	25	26	27
18	17	16	15	14	13	12	11	10
1	2	3	4	5	6	7	8	9

4

46	47	48	49	50	51	52	53	54
45	44	43	42	41	40	39	38	37
28	29	30	31	32	33	34	35	36
27	26	25	24	23	22	21	20	19
10	11	12	13	14	15	16	17	18
9	8	7	6	5	4	3	2	1

B. Verticale.

5

1	12	13	24	25	36	37	48	49
2	11	14	23	26	35	38	47	50
3	10	15	22	27	34	39	46	51
4	9	16	21	28	33	40	45	52
5	8	17	20	29	32	41	44	53
6	7	18	19	30	31	42	43	54

6

49	48	37	36	25	24	13	12	1
50	47	38	35	26	23	14	11	2
51	46	39	34	27	22	15	10	3
52	45	40	33	28	21	16	9	4
53	44	41	32	29	20	17	8	5
54	43	42	31	30	19	18	7	6

7

6	7	18	19	30	31	42	43	54
5	8	17	20	29	32	41	44	53
4	9	16	21	28	33	40	45	52
3	10	15	22	27	34	39	46	51
2	11	14	23	26	35	38	47	50
1	12	13	24	25	36	37	48	49

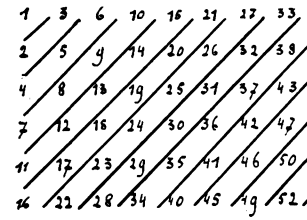
8

54	43	42	31	30	19	18	7	6
53	44	41	32	29	20	17	8	5
52	45	40	33	28	21	16	9	4
51	46	39	34	27	22	15	10	3
50	47	38	35	26	23	14	11	2
49	48	37	36	25	24	13	12	1

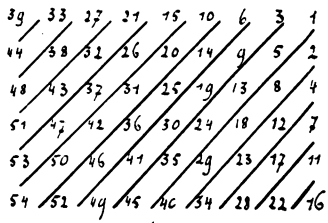
(1) En zig-zag.

3. Méthodes parallélogrammiques simples.

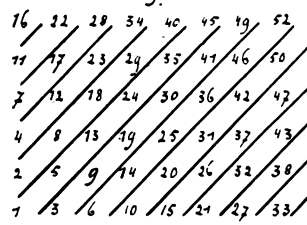
1.



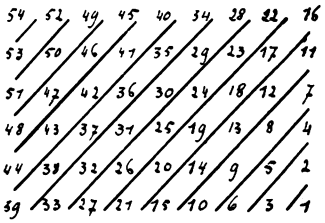
2.



3.

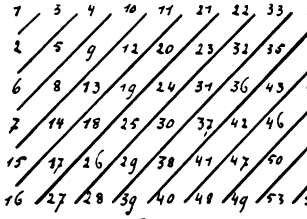


4.

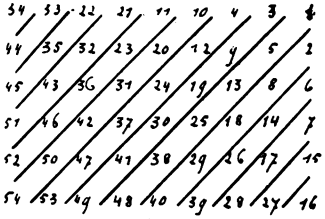


4. Méthodes parallélogrammiques en Boustrophédon.

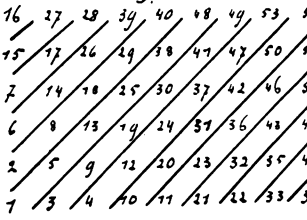
1.



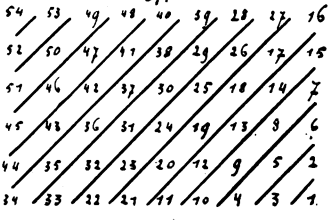
2.



3.



4.



Le relèvement des lettres dans chacun des 24 tableaux précédents, se fait aussi d'après une nouvelle convention : horizontalement, verticalement, obliquement ou en boustrophédon (1), par chacun des angles des tableaux.

On voit le grand nombre de combinaisons auxquelles se prêtent les méthodes à diviseurs réguliers ; mais, comme nous allons le montrer, ce grand nombre n'est nullement facteur proportionnel de la résistance au déchiffrement.

L'examen des tableaux montre que :

1° Le relèvement direct ou en boustrophédon, vertical, horizontal et oblique, commencé par les extrémités opposées d'une même diagonale, mais en *sens inverse, fournit des cryptogrammes identiques, comme structure générale*, mais *inversés.*

2° Le relèvement direct ou en boustrophédon, vertical et horizontal, commencé par les extrémités opposées d'une même verticale ou d'une même horizontale, mais en sens inverse, fournit des *cryptogrammes identiques, comme structure générale*, mais dans lesquels *les lettres de chaque tranche verticale ou horizontale sont inversées.*

3° Le relèvement direct ou en boustrophédon, vertical et horizontal, commencé par les extrémités opposées d'une même verticale, d'une même horizontale, dans le même sens, fournit des *cryptogrammes identiques comme structure générale*, mais inversés, et les *lettres de chaque tranche verticale ou horizontale sont également inversées.*

4° Le relèvement direct ou en boustrophédon diagonal, commencé par les extrémités d'une même verticale ou d'une même horizontale (dans le même sens ou en sens inverse), forme des *cryptogrammes à structure générale différente.*

Ces remarques réduisent nos observations à l'étude des

(1) En zig-zag.

premiers tableaux seuls de chacune des séries 1_1, 1_5; 2_1, 2_5, 3_1 et 4_1 et à celle du relèvement oblique, différent de la transcription, particularités que nous exposerons immédiatement après celles qui concernent le relevé non oblique.

A. *Relèvement direct vertical.*

1_1—1.10.19.28.37.46—2.11.20.29.38.47—3.12.21.30.39.48—4.13.22.31.40.49, etc.

+1_5—1,2.3.4.5.6—7.8.9.10.11.12—13.14.15.16.17.18—19.20.21.22.23.24.—25.26.27.28, etc.

2_1—1.18.19.36.37.54—2.17.20.35.38.53—3.16.21.34.39.52.—4.15.22.33,40.51, etc.

O.2_5—1.2.3.4.5.6—12.11.10.9.8.7—13.14.15.16.17.18—24.23.22.21.20.19—25.26.27.28.29. etc

3_1—$\overline{1.2.4.7}$.11.16—$\overline{3.5.8}$.12.17.22—$\overline{6.9}$.13.18.23.28—$\overline{10}$.14.19.24.29.34—15.20.25.30. etc.

4_1—$\overline{1.2.6.7}$.15.16—$\overline{3.5.8}$.14.17.27—$\overline{4.9}$.13.18.26.28—$\overline{10}$.12.19.25.29.39—11.20.24.30. etc.

B. *Relèvement direct horizontal.*

+1_1—1.2.3.4.5.6.7.8.9—10.11.12.13.14.15.16.17.18—19.20.21.22.23.24.25. etc.

1_5—1.7.13.19.25.31.37.43.49—2.8.14.20.26.32.38.44.50—9.15.21.27.33. etc.

O.2_1—1.2.3.4.5.6.7.8.9—18.17.16.15.14.13.12.11.10—19.20 21.22.23.24.25.26.27. etc.

2_5—1.12.13.24.25.36.37.48.49—2.11.14.23.26.35.38.47.50—3.10.15.22.27.34.39.46. etc.

3_1—$\overline{1.3.6.10}$.15.21.27.33.39—$\overline{2.5.9}$.14.20.26.32.38.44—$\overline{4.8}$.13.19.25.31.37.43.48—$\overline{7}$. etc.

4_1—$\overline{1.3.4.10}$.11.21.22.33.34.45—$\overline{2.5.9}$.12.20.23.32.35.44—$\overline{6.8}$.13.19.24.31.36.43.45. etc.

C. *Relèvement direct diagonal.*

1_1—1—10.2—19.11.3—28.20.12.4—37.29.21.13.5—46.38.30.22.14.6—47.39.31.23.15.7. etc.

1_5—1—2.7—3.8.13—4.9.14.19—5.10.15.20.25—6.11.16. 21.26.31—12.17.22.27.32.37. etc.

2_1—1—18.2—19.17.3—36.20.16.4—37.35.21.15.5—54. 38.34.22.14.6—53.39.33.23.13. etc.

2_5—1—2.12—3.11.13—4.10.14.24—5.9.15.23.25—6.8. 16.22.26.36—7.17.21.27.35.37—18 etc.

+ 3_1—1—2.3—4.5.6—7.8.9.10—11.12.13.14.15—16.17.18. 19.20.21—22.23.24.25.26.27. etc.

O. 4_1—1—2.3—6.5.4—7.8.9.10—15.14.13.12.11—16.17.18. 19.20.21—27.26.25.24.23.22. etc.

D. *Relèvement en boustrophédon vertical.*

1_1—1.10.19.28.37.46—47.38.29.20.11.2—3.12.21.30.39. 48—49.40.31.22.13.4—5.14. etc.

O. 1_5—1.2.3.4.5.6—12.11.10.9.8.7—13.14.15.16.17.18—24. 23.22.21.20.19—25.26.27.28.29. etc.

2_1—1.18.19.36.37.54—53.38.35.20.17.2—3.16.21.34.39. 52—51.40.33.22.15.4. etc.

+ 2_5—1.2.3.4.5.6—7.8.9.10.11.12—13.14.15.16.17.18—19. 20.21.22.23.24. etc.

3_1—$\overline{1.2.4.7}$.11.16—22.17.12.$\overline{8.5.3}$—$\overline{6.9}$.13.18.23.28—34. 29.24.19.14.$\overline{10}$—15.20.25. etc.

4_1—$\overline{1.2.6.7}$.15.16—27.17.14.$\overline{8.5.3}$—$\overline{4.9}$.13.18.26.28—39. 29.25.19.12.$\overline{10}$—11.20.24 etc.

E. *Relèvement en boustrophédon horizontal.*

O. 1_1—1.2.3.4.5.6.7.8.9—18.17.16.15.14.13.12.11.10—19.20. 21.22.23.24.25.26.27. etc.

1_5—1.7.13.19.25.31.37.43.49—50.44.38.32.26.20.14.8.2 —3.9.15.21.27.33.39.45.51 etc.

+ 2_1—1.2.3.4.5.6.7.8.9—10.11.12.13.14.15.16.17.18—19.20. 21.22.23.24.25.26.27. etc.

2_5—1.12.13.24.25.36.37.48.49—50.47.38.35.26.23.14.11. 2—3.10.15.22.27.34.39. etc.

3_1—$\overline{1.3.6.10}$.15.21.27.33.39—44.38.32.26.20.14.$\overline{9.5.2}$—
$\overline{4.8}$.13.19.25.31.37.43.48. etc.

4_1—$\overline{1.3.4.10}$.11.21.22.33.34—44.35.32.23.20.12.$\overline{9.5.2}$—
$\overline{6.8}$.13.19.24.31.36.43.45. etc.

F. *Relèvement en boustrophédon diagonal.*

1_1—1—10.2—3.11.19—28.20.12.4—5.13.21.29.37—46.
38.30.22.14.6—7.15.23.31.39.47. etc.

1_5—1—2.7—3.8.13—19.14.9.4—5.10.15.20.25—31.26.
21.16.11.6—12.17.22.27.32.37. etc.

2_1—1—18.2—3.17.19—36.20.16.4—5.15.21.35.37—54.
38.34.22.14.6—7.13.23.33.39.53. etc.

2_5—1—2.12—13.11.3—4.10.14.24—25.23.15.9.5—6.8.
16.22.26.36—37.35.27.21.17.7. etc.

O. 3_1—1—2.3—6.5.4—7.8.9.10—15.14.13.12.11—16.17.18.
19.20.21—27.26.25.24—23.22. etc.

+4_1—1—2.3—4.5.6—7.8.9.10—11.12.13.14.15—16.17.18.
19.20.21—22.23.24.25.26.27. etc.

G. *Relèvement direct diagonal* commencé par l'angle inférieur gauche opposé à l'angle supérieur gauche (extrémités opposées d'une même ligne verticale).

1_1—46—37.47—28.38.48—19.29.39.49—10.20.30.40.50
1.11.21.31.41.51—2.12.22.32.42.52. etc.

1_5—6.5.12—4.11.18—3.10.17.24—2.9.16.23.30—1.8.15.
22.29.36—7.14.21.28.35.42. etc.

2_1—54—37.53—36.38.52—19.35.39.51—18.20.34.40.50
1.17.21.33.41.49. etc.

2_5—$\overline{6}$—$\overline{5.7}$—$\overline{4.8}$.18—$\overline{3.9}$.17.19—$\overline{2.10}$.16.20.30—$\overline{1}$.11.15.
21.29.31—12.14.22.28.32.42. etc.

3_1—16—11.22—$\overline{7}$.17.28—$\overline{4}$.12.23.34—$\overline{2.8}$.18.29.40—1.
$\overline{5}$.13.24.35.45—$\overline{3.9}$.19.30.41.49. etc.

4_1—16—15.27—$\overline{7}$.17.28—$\overline{6}$.14.26.39—$\overline{2.8}$.18.29.40—1.
$\overline{5}$.13.25.38.48—$\overline{3.9}$.19.30.41.49. etc.

H. *Relèvement en boustrophédon diagonal*, commencé comme dans le tableau G.

1_1—46—37.47—48.38.28—19.29.39.49—50.40.30.20.10—11.21.31.41.51. etc.

1_5—6—$\overline{5}$.12—18.11.$\overline{4}$—$\overline{3.10}$.17.24—30.23.16.$\overline{9.2}$—$\overline{1.8}$. 15.22.29.36. etc.

2_1—54.37.53—52.38.36—19.35.51—50.40.34.20.18—1. 17.21.33.41.49. etc.

2_5—$\overline{6}$—$\overline{5.7}$—18.$\overline{8.4}$—$\overline{3.9}$.17.19—30.20.16.$\overline{10.2}$—$\overline{1}$.11.15. 21.29.31—42.32.28.22.14.12. etc.

3_1—16—11.22—28.17.$\overline{7}$—$\overline{4}$.12.23.34—40.29.18.8.2—$\overline{1}$. $\overline{5}$.13.24.35.45—49.41.30.19.$\overline{9.3}$. etc.

4_1—16—15.27—28.17.$\overline{7}$—$\overline{6}$.14.26.39—40.29.18.$\overline{8.2}$—$\overline{1}$. $\overline{5}$.13.25.38.48.49.41.30.19.$\overline{9.3}$. etc.

L'examen des tableaux de relèvement amène les remarques suivantes :

1° Dans les relèvements verticaux et horizontaux (directs ou en boustrophédon), les cryptogrammes peuvent être divisés en tranches d'autant de lettres qu'il y a de lignes verticales ou horizontales, suivant que le relevé s'est fait verticalement ou horizontalement.

2° Dans les relèvements diagonaux (directs ou en boustrophédon), les cryptogrammes peuvent être divisés en tranches d'un nombre de lettres croissant depuis 1 jusqu'au nombre des lignes horizontales, à partir des deux extrémités du cryptogramme.

Ces observations indiquent le premier genre de tâtonnements du travail.

En conséquence, la première chose à faire sera de numéroter les caractères du texte chiffré et de transcrire celui-ci en triple expédition.

Lorsqu'on voudra essayer une combinaison $a \times b$ relative au nombre respectif de lignes verticales et horizon-

tales d'un texte à déchiffrer, on partagera la première expédition en tranches de a chiffres correspondant au nombre de lignes verticales ; la deuxième, en tranches de b chiffres répondant au nombre de lignes horizontales ; enfin la troisième expédition sera partagée en tranches croissantes et décroissantes de 1 à a et de a à 1, ou de 1 à b et de b à 1.

A partir de ce moment, on fera subir au texte ainsi préparé, les essais que nous allons développer en analysant les séries de cryptogrammes A à H.

a. Dans chacun des tableaux A à F, il y a un relèvement (marqué du signe +) qui fournit la suite naturelle des lettres du texte clair ; il ne sera donc pas employé par le chiffreur

Un autre (marqué du signe o) reproduit le texte clair dans lequel les tranches paires (relevés verticaux et horizontaux), les tranches impaires de la suite naturelle des nombres (à partir de la 3e seulement, dans les relevés obliques), ont été inversées.

Nous pouvons aussi l'écarter de nos recherches.

Il ne nous reste donc plus à examiner que quatre cryptogrammes dans chaque série, de A à F, et six dans les séries G et H.

b. Si l'on compare les cryptogrammes des séries A, B et C à ceux des séries D, E et F, on constate qu'ils sont identiques, sauf que les tranches paires (pour les relèvements verticaux et horizontaux) et les tranches impaires (pour les relèvements diagonaux) sont inversées dans les séries D, E et F par rapport aux séries correspondantes de A, B et C.

Il faut encore écarter ces chiffres de nos recherches, ou du moins, il faut en retenir la règle, l'essai éventuel du renversement des séries susmentionnées, pour tenir compte du relèvement en boustrophédon.

c. Si l'on compare les cryptogrammes des séries G et H, on voit que ceux de cette dernière sont aussi identiques à ceux qui leur correspondent dans la série précédente, sauf

que les groupes impairs, à partir du 3e sont inversés. De plus, les chiffres de 3_1 et 4_1 présentent la particularité d'avoir leurs tranches impaires identiques.

L'étude de la structure générale des cryptogrammes obtenus (A à H) va nous permettre de réunir les éléments suffisants pour achever d'établir les principes de déchiffrement des méthodes régulières à diviseurs, à simple clef-convention, en montrant l'analogie des résultats du chiffrement, quels que soient le dispositif de tableau et le mode de relèvement adoptés.

Sauf quelques restrictions, qu'une comparaison attentive des relèvements fera ressortir immédiatement, nous pouvons poser en principe, que la transcription et le relèvement des tableaux amènent des cryptogrammes où les lettres de même rang, dans chaque tranche successive, se suivent, et quelquefois se précèdent, dans le texte clair.

Lorsque le relèvement n'a pas été fait à partir de l'angle de transcription, les tranches impaires des relèvements provenant des tableaux parallélogrammiques, sont toujours identiques; les chiffres des tranches paires et ceux des tranches impaires deux à deux, se suivent ou se précèdent dans le texte clair; les autres relèvements suivent la règle générale.

Remarques. — 1. Dans les relevés des tableaux rectangulaires, le premier chiffre de chaque tranche, à partir de la droite ou de la gauche, suivant le cas, marque la suite naturelle des nombres.

2. Le relèvement direct ou en boustrophédon, vertical ou horizontal, des tableaux parallélogrammes, fournit des cryptogrammes où les 10 premières lettres sont placées dans les quatre premières tranches : les 10 dernières dans les quatre dernières; ou inversement à raison de 4, 3, 2 et 1, à partir des extrémités, dans un ordre toujours le même pour chaque espèce de relèvement.

3. Dans tous les relèvements en boustrophédon, les lettres à égale distance du point de séparation d'une double tranche paire-impaire, se suivent dans le texte clair.

4. Dans les relèvements en boustrophédon D, E et F, des tableaux rectangulaires ou parallélogrammiques, l'ordre des chiffres des tranches paires est inversé.

Nous allons appliquer ces préceptes au déchiffrement d'un texte donné.

Soit le chiffre : lento — sdsau — sorse — perve — atine — iheev — jvdea — uemco — seeim — evegt — ounme — itoup — brnun — rrric —

Il contient 70 lettres ou $70 = 2 \times 5 \times 7$.

Nous pouvons admettre comme les plus probables, les combinaisons 7×10 et 10×7, avec une préférence en faveur de la première.

Nous aurons :

1° pour la répartition en tranches de 10 chiffres :
lentosdsau — sorseperve — atineiheev — jvdeauemco — seeimevegt — ounmeitoup — brnunrrrie —

2° pour la subdivision en tranches de 7 chiffres :
lentosd — sausors — epervea — tineihe — evjvdea — uemcose — eimeveg — tounmei — toupbrn — unrrrie —

3° pour la division en tranches suivant la série naturelle des nombres (le groupement croissant jusque 7 est seul possible) :
l—en—tos—dsau—sorse — pervea— tineihe — evjvdea — uemcose—eimeveg—tounme—itoup—brnu—nrr— ri—e

Si nous essayons les différentes combinaisons contenues dans les relevés A à G qui précèdent, nous reconnaîtrons bientôt que le cryptogramme provient de la transposition par le tableau 2_8 (méthode rectangulaire en boustrophédon vertical) et par le relèvement en boustrophédon diagonal :
1-20-003-4000-00005-600000-0000007-8000000 etc.
l -en -tos -dsau -sorse -pervea -tineihe -evjvdea
d'où 1 2 3 4 5 6 7 8
l e s d e p e e

Nous pouvons construire le tableau 2_5 et effectuer le relèvement ; nous obtiendrons ainsi le développement de la combinaison du chiffre.

Mais si nous tenons compte du principe général en vertu duquel nous avons reconnu que les lettres de même rang, dans les tranches successives, se suivent ou se précèdent dans le texte clair ; si d'autre part, nous remarquons que les tranches impaires sont inversées, nous achèverons aisément le déchiffrement, sans reconstruire le tableau 2_5.

« Les dépêches sont arrivées. Je vous envoie immédiatement un nouveau courrier r b p t g ».

Soit encore le cryptogramme :

rasve— vdlyn— eosrl— reoro— snuve— eczne — utoso — zstsd—cvrnu—diive—uenl.

Il contient 54 lettres. $54 = 2 \times 3 \times 3 \times 3$.

Les combinaisons 2×27 et 3×18 sont peu probables. Les essais ne donnent d'ailleurs aucun résultat. Reste donc 6×9 ou 9×6.

Nous aurons :

1° pour la répartition en 6 tranches de neuf lettres :

rasvev — dlyneo — srlreo — rosnuv — eeczne — utosoz— stsdcv—rnudii—ceuenl—

2° pour la subdvision en 9 tranches de six lettres.

rasvevdly—neosrlreo— rosnuveec— zneutosoz— stsdcvrnu — diieeuenl —

3° pour la division d'après l'ordre naturel (le groupement croissant jusque 6 est seul possible) :

r—as— vev— dlyn— eosrl— reoros— nuveec— zneuto — sozsts — devrn — udii — eeu — en — l.

Si nous essayons les combinaisons des relevés A à G, nous ne découvrons pas l'origine du cryptogramme ; nous en concluons qu'il appartient aux modes indiqués par les relevés G et H.

Si nous mettons les tranches impaires d'une part, et les tranches paires d'autre part en colonnes, nous aurons :

Tranches impaires.	Tranches paires.
r	a s
v e v	d e y n
e o s r l	r e o r o s
n u v e e c	z n e u t o
s o z s t s	d c v r n
u d i i	e e u
e n	e

Si nous relevons les colonnes verticales lues par le haut, alternativement dans les tranches paires et impaires, nous obtenons le texte clair :

r-en-dez-vous-alond-resvou-syrece-vrezde-nouvel-lesin-stru-cti-on-s.

Les remarques que nous avons faites au cours de cette discussion, et la simplicité des déchiffrements, montrent que le système régulier des diviseurs à simple clef-convention n'offre pas de sérieuse résistance au cryptologue et que le nombre considérable de combinaisons qu'il présente ne l'empêche nullement de livrer bien vite ses secrets.

A. COLLON

Lieutenant d'artillerie adjoint d'Etat-Major

(A suivre).

ETUDE

SUR LA

CRYPTOGRAPHIE

Son emploi à la guerre et dans la diplomatie (1).

TITRE I.

LA CRYPTOGRAPHIE ACTUELLE

Les méthodes de chiffrement et de déchiffrement.

PREMIÈRE PARTIE.

PROCÉDÉ GÉNÉRAL MONOLITTÉRAL.

Première classe : Systèmes par transposition ou interversion des lettres du texte clair.

CHAPITRE II. — MÉTHODES A CLEF-CONVENTION.

A. Méthodes régulières des diviseurs à simple clef-convention. (Suite).

Outre les modes de disposition et de relèvement provenant des méthodes régulières des diviseurs à simple clef convention, qui viennent d'être exposées, il est une catégorie particulière d'intervertions qui méritent une mention spéciale, et que nous allons examiner.

Nous pouvons ajouter aux quatre dispositifs généraux: rectangulaires et parallélogrammiques, simples ou en boustrophédon, vus précédemment, les tableaux en spirale ci-contre :

(1) Voir 2ᵉ année Tomes II, III et IV.

5. *Méthodes en spirale.*

A. Horizontale.

1

1	2	3	4	5	6	7	8	9
26	27	28	29	30	31	32	33	10
25	44	45	46	47	48	49	34	11
24	43	54	53	52	51	50	35	12
23	42	41	40	39	38	37	36	13
22	21	20	19	18	17	16	15	14

2

9	8	7	6	5	4	3	2	1
10	33	32	31	30	29	28	27	26
11	34	49	48	47	46	45	44	25
12	35	50	51	52	53	54	43	24
13	36	37	38	39	40	41	42	23
14	15	16	17	18	19	20	21	22

3

22	21	20	19	18	17	16	15	14
23	42	41	40	39	38	37	36	13
24	43	54	53	52	51	50	35	12
25	44	45	46	47	48	49	34	11
26	27	28	29	30	31	32	33	10
1	2	3	4	5	6	7	8	9

4

14	15	16	17	18	19	20	21	22
13	36	37	38	39	40	41	42	23
12	35	50	51	52	53	54	43	24
11	34	49	48	47	46	45	44	25
10	33	32	31	30	29	28	27	26
9	8	7	6	5	4	3	2	1

B. Verticale.

5

1	26	25	24	23	22	21	20	19
2	27	44	43	42	41	40	39	18
3	28	45	54	53	52	51	38	17
4	29	46	47	48	49	50	37	16
5	30	31	32	33	34	35	36	15
6	7	8	9	10	11	12	13	14

6

19	20	21	22	23	24	25	26	1
18	39	40	41	42	43	44	27	2
17	38	51	52	53	54	45	28	3
16	37	50	49	48	47	46	29	4
15	36	35	34	33	32	31	30	5
14	13	12	11	10	9	8	7	6

7

6	7	8	9	10	11	12	13	14
5	30	31	32	33	34	35	36	15
4	29	46	47	48	49	50	37	16
3	28	45	54	53	52	51	38	17
2	27	44	43	42	41	40	39	18
1	26	25	24	23	22	21	20	19

8

14	13	12	11	10	9	8	7	6
15	36	35	34	33	32	31	30	5
16	37	50	49	48	47	46	29	4
17	38	51	52	53	54	45	28	3
18	39	40	41	42	43	44	27	2
19	20	21	22	23	24	25	26	1

Le relèvement des tableaux des méthodes en spirale peut se faire par un des procédés qui ont été mentionnés, en observant que les quatre remarques conclusives émises à la suite de ces tableaux, leur sont applicables; le travail est donc réduit à l'étude des premiers tableaux 5_1 et 5_5, des séries A et B, et des relèvements G et H; nous obtenons ainsi:

A. *Relèvement direct vertical.*

5_1—1.26.25.24.23.22.—2.27.44.43.42.21.—3.28.45.54.41.20.—4.29.46.53.40.19.—5.30.47.52.39.18.—6.31.48.51.38.17.—7.32.49.50.37.16.—8.33.34.35.36.15.—9.10.11.12.13.14.

5_5—1.2.3.4.5.6—26.27.28.29.30.7—25.44.45.46.31.8—24.43.54.47.32.9—23.42.53.48.33.10—22.41.52.49.34.11.—21.40.51.50.35.12—20.39.38.37.36.13—19.18.17.16 15.14.

B. *Relèvement direct horizontal.*

5_1—1.2.3.4.5.6.7.8.9—26.27.28.29.30.31.32.33.10—25.44.45.46.47.48.49.34.11—24.43.54.53.52.51.50.35.12.23.42.41.40.39.38.37.36.13—22.21.20.19.18.17.16.15.14.

5_5—1.26.25.24.23.22.21.20.19—2.27.44.43.42.41.40.39.18.3.28.45.54.53.52.51.38.17—4.29.46.47.48.49.50.37.16.5.30.31.32.33.34.35.36.15—6.7.8.9.10.11.12.13.14.

C. *Relèvement direct diagonal.*

5_1—1—26.2—25.27.3—24.44.28.4—23.43.45.29.5—22.42.54.46.30.6—21.41.53.47.31.7—20.40.52.48.32.8—19.39.51.49.33.9—18.38.50.34.10—17.37.35.11—16.36.12—15.13—14.

5_5—1—2.26—3.27.25—4.28.44.24—5.29.45.43.23—6.30.46.54.42.22—7.31.47.53.41.21—8.32.48.52.40.20—9.33.49.51.39.19—10.34.50.38.18—11.35.37.17—12.36.16—13.15—14.

D. *Relèvement en boustrophédon vertical.*

5_1 — 1.26.25.24.23.22 — 21.42.43.44.27.2 — 3.28.45.54.41.20 — 19.40.53.46.29.4 — 5.30.47.52.39.18 — 17.38.51.48.31.6 — 7.32.49.50.37.16 — 15.36.35.34.33.8 — 9.10.11.12.13.14.

5_5 — 1.2.3.4.5.6 — 7.30.29.28.27.26 — 25.44.45.46.31.8 — 9.32.47.54.43.24 — 23.42.53.48.33.10 — 11,34.49.52.41.22 — 21.40.51.50.35.12 — 13.36.37.38.39.20 — 19.18.17.16.15.14.

E. *Relèvement en boustrophédon horizontal.*

5_1 — 1.2.3.4.5.6.7.8.9 — 10.33.32.31.30.29.28.27.26 — 25.44.45.46.47.48.49.34.11 — 12.35.50.51.52.53.54.43.24 — 23.42.41.40.39.38.37.36.13 — 14.15.16.17.18.19.20.21.22.

5_5 — 1.26.25.24.23.22.21.20.19 — 18.39.40.41.42.43.44.27.2 — 3.28.45.54.53.52.51.38.17 — 16.37.50.49.48.47.46.29.4 — 5.30.31.32.33.34.35.36.15 — 14.13.12.11.10.9.8.7.6.

F. *Relèvement en boustrophédon diagonal.*

5_1 — 1 — 26.2 — 3.27.25 — 24,44.28.4 — 5.29.45.43.23 — 22.42.54.46.30.6 — 7.31.47.53.41.21 — 20.40.52,48.32.8 — 9.33.49.51.39.19 — 18.38.50.34.10 — 11.35.37.17. — 16.36.12 — 13.15 — 14.

5_5 1 — 2.26 — 25.27.3 — 4.28.44.24 — 23.43.45.29.5 — 6.30.46.54.42.22 — 21.41.53.47.31.7 — 8.32.48.52.40.20 — 19.39.51.49.33.9 — 10.34.50.38.18 — 17.37.35.11. — 12.36.16 — 15.13 — 14.

G. *Relèvement direct diagonal* commencé par l'angle inférieur gauche opposé à l'angle supérieur gauche (extrémités opposées d'une même verticale.)

5_1—22—23.21—24.42.20—25.43.41.19—26.44.54.40.18—1.27.45.53.39.17—2.28.46.52.38.16—3.29.47.51.37.15—4.30.48.50.36.14—5.31.49.35.13—6.32.34.12.—7.33.11—8.10—9.

5_5—6—5.7—4.30.8—3.29.31.9—2.28.46.32.10—1.27.45 ? 47.33.11—26.44.54.48.34.12—25.43.53.49.35.13—24.42.52.50.36.14—23.41.51.37.15—22.40.38.16.21.39.17—20.18—19.

H. *Relèvement en boustrophédon diagonal*, commencé comme dans le relevé G.

5_1—22—23.21—20.42.24—25.43.41.19—18.40.54.44.26—1.27.45.53.39.17—16.38.52.46.28.2—3.29.47.51.37.15—14.36.50.48.30.4—5.31.49.35.13.12.34.32.6.—7.33.11—10.8—9.

5_5—6—5.7—8.30.4—3.29.31.9—10.32.46.28.2—1.27.45.47.33.11—12.34.48.54.44.26—25.43.53.49.35.13—14.36.50.52.42.24—23.41.51.37.15—16.38.40.22.—21.39.17—18.20—19.

Ici encore, comme dans les relevés des tableaux de la première série, analysés précédemment, les mêmes remarques se produisent en général, et réduisent considérablement le nombre de tableaux-types qui doivent servir de base aux essais. Nous laissons au lecteur le soin de faire lui-même ces comparaisons, qui marquent nettement la voie à suivre pour retrouver la trace des opérations auxquelles le texte clair a été soumis.

Outre les combinaisons qui viennent d'être exposées, les tableaux des méthodes à diviseurs à simple clef-convention peuvent encore se relever *en spirale ;* mais un examen préalable de ces dispositifs nous montre que les relevés en spirale des méthodes en spirale sont semblables entre eux, et reproduisent alternativement des fragments *en clair* du texte clair.

Ils ne se différencient que par la transposition de certaines tranches de caractères, vers les extrémités ou dans le corps du relèvement du texte, artifice trop primitif pour offrir la moindre sécurité au chiffeur.

Il ne nous reste donc plus à considérer que les relèvements en spirale des tableaux de la première série.

De cette manière nous obtenons les dispositifs ci-après :

Relèvements en spirale.

1_1

1. 2. 3. 4. 5. 6. 7. 8. 9. 18. 27. 36. 45. 54. 53. 52. 51. 50. 49. 48. 47. 46. 37. 28. 19. 10
11. 12. 13. 14. 15. 16. 17. 26. 35. 44. 43. 42. 41. 40. 39. 38. 29. 20.
21. 22. 23. 24. 25. 34. 33. 32. 31. 30.

1_5

1. 7. 13. 19. 25. 31. 37. 43. 49. 50. 51. 52. 53. 54. 48. 42. 36. 30. 24. 18. 12. 6. 5. 4. 3. 2
8. 14. 20. 26. 32. 38. 44. 45. 46. 47. 41. 35. 29. 23. 17. 11. 10. 9.
15. 21. 27. 33. 39. 40. 34. 28. 22. 16.

2_1

1. 2. 3. 5. 6. 7. 8. 9. 10. 27. 28. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 37. 36. 19. 18.
17. 16. 15. 14. 13. 12. 11. 26. 29. 44. 43. 42. 41. 40. 39. 38. 35. 20.
21. 22. 23. 24 25. 30. 31. 32. 33. 34.

2_5

1. 12. 13. 24. 25. 36. 37. 48. 49. 50. 51. 52. 53. 54. 43. 42. 31. 30. 19. 18. 7. 6. 5. 4. 3. 2.
11. 14. 23. 26. 35. 38. 47. 46. 45. 44. 41. 32. 29. 20, 17. 8. 9. 10.
15. 22. 27. 34. 39. 40. 33. 28. 21. 16.

3_1

1. 3. 6. 10. 15. 21. 27. 33. 39. 44. 48. 51. 53. 54. 52. 49. 45. 40. 34. 28. 22. 16. 11. 7. 4. 2.
5. 9. 14. 20. 26. 32. 38. 43. 47. 50. 46. 41, 35. 29. 23, 17. 12. 8.
13. 19. 25. 31. 37. 42. 36. 30. 24. 18.

4_1

1. 3. 4. 10. 11. 21. 22. 33. 34. 44, 45. 51. 52. 54. 53. 49. 48. 40. 39. 28. 27. 16. 15. 7. 6. 2.
5. 9. 12. 20. 23. 32. 35. 43. 46. 50. 47. 41. 38. 29. 26. 17. 14. 8.
13. 19. 24. 31. 36. 42. 37. 30. 25. 18.

De ces relevés, nous allons déduire les règles de déchiffrement employées pour réduire les cryptogrammes qui proviennent des méthodes de ce genre.

Remarquons que tout relevé en spirale fournit toujours, quel que soit le nombre des signes du tableau, une série de lignes successives différant de 8 caractères.

En effet, si le nombre de figures du texte est a × b, la première ligne du développement en spirale comprendra le pourtour du rectangle (ou du carré), soit (a + b — 2) 2= 2 a + 2 b — 4.

La deuxième ligne, fournira nécessairement le nombre de lettres précédent, diminué de deux sur chaque face du rectangle ou 2 (a + b) — 2 (2 + 4) = 2 a + 2 b — 12.

La troisième ligne, comptera 2 (a + b) — 2 (2 + 4 + 4) = 2 a + 2 b — 20.

Et ainsi de suite.

Cette remarque indique le premier essai à faire subir au texte.

Si maintenant, nous faisons glisser les lettres-chiffres des lignes successives du relèvement, sous la première ligne de celui-ci, de manière à former des groupements caractéristiques, nous obtiendrons une série de relèvements particuliers, qui nous indiqueront les tâtonnements à faire pour réduire aisément toute méthode de cette espèce.

Nous aurons donc le groupe des relevés ci-contre, dont le déchiffreur tirera aisément parti pour guider les essais ultérieurs :

1_1

1. 2. 3. 4. 5. 6. 7. 8. 9. 18. 27. 36. 45. 54. 53. 52. 51. 50. 49. 48. 47. 46. 37. 28. 19. 10
11. 12. 13. 14. 15. 16. 17. 26. 35. 44. 43. 42. 41. 40. 39. 38. 29. 20
21. 22. 23. 24. 25. 34. 33. 32. 31. 30

1_5

1. 7. 13. 19. 25. 31. 37. 43. 49. 50. 51. 52. 53. 54. 48. 42. 36. 30. 24. 18. 12. 6. 5. 4. 3. 2.
8. 14. 20. 26. 32. 38. 44. 45. 46. 47. 41. 35. 29. 23. 17. 11. 10. 9.
15. 21. 27. 33. 39. 40. 34. 28. 22. 16.

2_1

1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 27. 28. 45. 46. 47. 48. 49. 50. 51. 52. 53. 54. 37. 36. 19. 10
17. 16. 15. 14. 13. 12. 11. 26. 29. 44. 43. 42. 41. 40. 39. 38. 35. 20.
21. 22. 23. 25. 30. 31. 32. 33. 34.

2_5

1. 12. 13. 24. 25. 36. 37. 48. 49. 50. 51. 52. 53. 54. 43. 42. 31. 30. 19. 18. 7. 6. 5. 4. 3. 2.
11. 14. 23. 26. 35. 38. 47. 46. 45. 44. 41. 32. 29. 20. 17. 8. 9. 10.
15. 22. 27. 34. 39. 46. 45. 40. 33. 28. 21. 16.

3_1

1. 3. 6. 10. 15. 21. 27. 33. 39. 44. 48. 51. 53. 54. 52. 49. 45. 40. 34. 28. 22. 16. 11. 7. 4. 2.
5. 9. 14. 20. 26. 32. 38. 43. 47. 50. 46. 41. 35. 29. 23. 17. 12. 8.
13. 19. 25. 31. 37. 42. 36. 30. 24. 18.

4_1

1. 3. 4. 10. 11. 21. 22. 33. 34. 44. 45. 51. 52. 54. 53. 49. 48. 40. 39. 28. 27. 16. 15. 7. 6. 2.
5. 9. 12. 20. 23. 32. 35. 43. 46. 50. 47. 41. 38. 29. 26. 17. 14. 8.
13. 19. 24. 31. 36. 42. 37. 30. 25. 18.

B. Méthodes irrégulières à clef-convention.

1° *Deuxième méthode du colonel Roche.* — Sous le nom de « Deuxième méthode du colonel Roche », le capitaine d'artillerie breveté Josse, dans sa brochure sur la cryptographie et ses applications à l'art militaire (1), décrit une méthode à clef convention tenant du procédé des grilles et de la méthode du télégraphe aérien.

Voici en quoi elle consiste :

Le colonel Roche dispose d'un damier formé de huit colonnes horizontales et de dix colonnes verticales ; il se choisit une clef de huit lettres qu'il transforme en clef numérique en composant le tableau ci-dessous :

Tableau I.

c	h	a	m	p	i	g	o	chiffres indiquant les colonnes horizontales
2	4	1	6	8	5	3	7	
1	2	3	4	5	6	7	8	rang des lettres du texte clair

D'après cela, chacune des lettres du texte clair est transposée dans le damier (tableau II) de la manière suivante :

(1) Revue maritime et coloniale, tome 84, mars 1885.

TABLEAU II.

	I	II	III	IV	V	VI	VII	VIII	IX	X
I						3				
II				1						
III							7			
IV	2									
V			6							
VI										4
VII		8								
VIII					5					

la 1re lettre, surmontée du chiffre 2, sera placée dans la 2e ligne horizontale, et dans la 4e case, parce que le nombre qui suit 2 dans le tableau I est 4; la 2e lettre, surmontée du chiffre 4, dans la 4e ligne horizontale et dans la 1re case, parce que dans le tableau I le chiffre 1 suit le chiffre 4; la 3e lettre sera transposée dans la 1re ligne horizontale et dans la 6e case, et ainsi de même pour les 5e, 6e et 7e lettres.

La 4e lettre devrait être placée au 8e rang, d'après la règle générale, mais afin de brouiller davantage les signes, on la rejettera au 10e, et l'on fera de même chaque fois qu'une lettre devra occuper la 8e case.

La 8e lettre prend comme rang de colonne verticale celui indiqué par le 1er chiffre de gauche qui est sensé suivre 7.

Les 8 caractères suivants sont inscrits à la droite des 8 premiers.

Lorsqu'il n'y a pas possibilité de le faire, la lettre descend à la ligne suivante dans la même colonne verticale.

La troisième série de 8 lettres est transposée d'après le même principe, mais à la gauche cette fois des lettres déjà établies ; les autres séries sont placées successivement à la droite et à la gauche des groupes installés. Lorsqu'il n'y a pas moyen d'observer ce principe, on inscrit toujours les caractères à la ligne suivante, comme plus haut. Nous obtenons ainsi le :

TABLEAU III.

	I	II	III	IV	V	VI	VII	VIII	IX	X
I	63	54	43	30	16	3	9	23	36	48
II	44	31	17	1	10	24	37	49	58	66
III	70	64	55	45	32	18	7	11	25	38
IV	2	12	26	39	50	59	67	72	76	79
V	33	19	6	13	27	40	51	60	68	73
VI	80	78	75	71	65	56	46	34	20	4
VII	21	8	14	28	41	52	61	69	74	77
VIII	57	47	35	22	5	15	29	42	53	62

Si le texte ne comporte pas 80 lettres, on ajoute les nulles nécessaires pour parfaire ce nombre. Si celui-ci est dépassé, on recommence l'opération en établissant un nouveau tableau de 80 signes.

La *lecture* d'un damier semblable se fait en transposant les lettres dans un ordre inverse et n'offre pas de difficulté.

Cette méthode, comme toutes ses congénères, demande beaucoup d'attention et de soin ; de plus, elle est fort longue sans assurer l'indéchiffrabilité, comme nous allons le voir.

En effet, si nous faisons glisser les lignes horizontales

du tableau III jusqu'à ce que les 8 premiers chiffres soient en colonne verticale, on obtient le tableau IV, où les lettres se suivent de part et d'autre de la colonne centrale, comme dans le texte clair. C'est cette remarque qui va nous permettre d'opérer la traduction du texte chiffré.

TABLEAU IV.

				30	16	2	9	23	36	48	58	66	72
			63	54	43	31	17	7	10	24	37	49	
				44	32	18	3	11	25	38	50	59	67
		70	64	55	45	33	19	4	12	26	39		
							1	13	27	40	51	60	68	73	76	79
			56	46	34	20	8	14	28	41	52	61	
80	78	75	71	65	57	47	35	21	5				
							22	6	15	29	42	53	62	69	74	77

Déchiffrement. — Soit à déchiffrer le cryptogramme suivant : ttluc— iemsc— exejl—idrau—dimgc—slcca—assra demlc — oeafa — mlcco — xsaeg — aerne— nuode— eftri— lnpev — reesa —

Le texte chiffré ayant 80 caractères, et la fréquence des lettres qui le composent étant normale, il est à présumer que le chiffrement est dû à la deuxième méthode du colonel Roche. Faisons-en l'essai :

Rangeons les signes en 8 lignes de 10 lettres. Nous obtenons : (fig. 1).

FIGURE 1.

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

Essayons les séquences entre la première et la deuxième lignes ; une *x* dans la deuxième ligne nous indique immédiatement qu'elle est précédée de l'*u* de la première ; l'essai des autres bigrammes *le, cl, mi*, etc., confirme cette conclusion.

Entre la deuxième et la troisième lignes, l'*x* doit entrer en séquence avec *i*, *l* ou *s*. Avec *i* nous obtenons les bigrammes *jg*, *lc* fort improbables ; avec *l* et *s*, nous obtenons des bigrammes également probables ; l'*x* ne nous donne aucune indication ; le *j* est habituellement suivi de *o*, *e* ou ou *a* ; les essais nous fournissent des combinaisons toutes aussi probables ; nous sommes donc réduits à rechercher les bigrammes les plus probables entre 2 et 3 (es, le, en, de, nt, er, ou, etc.). Nous avons *es*, *le* et *de* ; les combinaisons des deux *e* de la 2e ligne avec *s* sont admissibles : celles qui proviennent de *l* avec l'*e* de la 9e colonne aussi, celles de la 8e colonne pas (jl, xc) ; celles provenant de *d* avec l'*e* des 9e et 8e colonnes (*js*, *xg*) et (*ls*, *sc*, *xm jc*, *xm*), sont aussi improbables.

La juxtaposition des lignes 2 et 3 ne nous donnant pas immédiatement de résultats, essayons les trigrammes : nous avons pour les deux premières lignes déjà reconstituées :

t t l u c i e m s e
e x e j l i d r a u

Si, après les bigrammes admissibles, nous examinons les trigrammes les plus fréquents (en nous servant du tableau de fréquence F), nous voyons que *el* demande *e*; or nous avons dit plus haut, que les combinaisons provenant de *l* avec *e* (8e colonne) sont inadmissibles; nous optons donc pour *ele* avec *e* (9e colonne).

Ce demande *s*, ce qui cadre avec la conclusion précédente, et nous amène, avec les autres colonnes, des séquences dont la plupart sont très probables. Nous avons dès lors :

t t l u c i e m s e
e x e j l i d r a u
d i m g c s l e e a

La 4e ligne *assrademle*, glissée le long et sous la 3e, fait constater qu'il faut admettre provisoirement la concordance de *l* (7e lettre de la 3e ligne), avec *a* (1re lettre de la 4e ligne), et pour mémoire, la concordance du c (3e lettre de la 4e ligne) avec *a* (1re lettre de la 4e ligne).

La 5e ligne *oeafamleeo*, glissée sous le tableau des quatre premières lignes, fait admettre les séquences provenant de la concordance du premier *o* de la 5e ligne avec le *c* de la 3e, ce qui nous donne déjà le fragment de tableau.

t t l u c i e m s e
e x e j l i d r a u
d i m g c s l e e a
a s s r a d e m l e
o e a f a m l e e o

La 6e ligne *x s a e g a e r n e* se range sous la 5e, de manière à faire correspondre *n* (9e lettre) avec le premier *e* (2e lettre de la 5e ligne).

La 7e et la 8e lignes se rangeront plus facilement encore pour donner finalement le tableau : (fig. n° 2).

FIGURE 2.

19 17 15 13 11 9 7 5 3 1 2 4 6 8 10 12 14 16 18

t t l u c i e m s e

c x e j l i d r a u

d i m g c s l e e a

a s s r a d e m l e

o e a f a m l e e o

x s a e g a e r n e

n u o d e e f t r i

l n p e v r e e s a

Les colonnes centrales ont toutes un sens intelligible, ou du moins des séquences normales, sauf la colonne 1 composée de haut en bas de *ijlaaeuv ;* ce sera celle comprenant les premières lettres du texte dans un ordre à rétablir ; à droite et à gauche, nous trouvons alternativement les lettres suivantes de la dépêche en clair dans leur ordre naturel. Nous aurons donc :

1 2 3 4 5 6

ijlaaeuv—elesfor— cesenne— miesade— uxcorp— sdarmee

7 8 9 10 11 12 13 14

—legen—erales— tmal— adefa— tig— ueet— de— mor—

15 16 17 18 19

a — li — s — e — x.

Le *j* demande avant lui un *e*; après lui, un *o*, un *e* ou un *a* ; le *v*, avant lui, le plus souvent un *e*, souvent un *a*, *i* ou *u* ; après lui, le plus souvent, un *e*, et très souvent, *a*, *i* ou *o*.

Les autres séquences de ces 8 lettres sont toutes aussi fréquentes. C'est donc par les lettres *j* et *v* que nous arriverons à reconstituer ce texte sans aucune difficulté. La présence du *j* dans le premier groupe et l'ensemble de la dépêche paraissent annoncer que le correspondant parle à la première personne, ce qui exige *je* ou *jai ;* le mot suivant se termine par l'*e* du 2e groupe. Il reste *ilaauv* (pour je), ou laeuv (pour jai). Le premier reste ne permet pas la formation d'un mot rationnel ; le second donne un trigramme

rationnel qui s'impose ici, *eva* qui fournit *évalu—e.*

Nous avons enfin le texte clair : « J'ai évalué les forces ennemies à deux corps d'armée. Le général est malade, fatigué et démoralisé. »

Nous n'avons donné tous les détails ci-dessus, que pour bien montrer les différentes phases d'un déchiffrement de ce genre. En pratique, les opérations se réduisent à quelques tâtonnements, consistant à juxtaposer successivement les lignes du tableau de la figure 1, de manière à former un texte compréhensible. Les tableaux des fréquences y aideront énormément.

Si le cryptogramme a été relevé par une des méthodes régulières à simple clef, il faudra, au préalable, rétablir le tableau normal par une série de tâtonnements, qui seront ici un peu plus difficiles, mais qui cependant, n'obligeront jamais qu'à l'essai de quelques combinaisons.

Le mieux sera de mener de front le travail sur les cryptogrammes résultant des relevés direct et en boustrophédon (vertical, horizontal ou oblique). La méthode réellement employée se décèlera bientôt, dès qu'on aura fait glisser l'une sur l'autre les deux ou trois premières lignes horizontales du tableau Roche.

2° *Première méthode du colonel Roche.* — Le capitaine Josse, sous le nom de « Première méthode du colonel Roche », expose encore, dans la Revue maritime et coloniale, un autre procédé de chiffrement à interversion irrégulière, qui tient du système du télégraphe aérien et des grilles, et nous paraît être la réalisation d'un perfectionnement apporté à la « seconde méthode » du colonel, dans le but d'augmenter la difficulté de reconstitution du tableau de la méthode « première. »

Il prend comme exemple un texte renfermant 38 lettres, et divise ce nombre en 8 groupes numérotés de I à VIII. Ces groupes renferment chacun un nombre arbitraire de

lettres, indiqué en chiffres arabes en tête des colonnes du tableau I ci-dessous :

TABLEAU I.

3	5	7	2	4	6	8	3
I	II	III	IV	V	VI	VII	VIII

Les lettres du texte clair sont disposées dans les colonnes par séries ; la première série, par exemple, répartira ses caractères dans les 8 compartiments, à partir de la droite de ceux-ci. Les 7 chiffres suivants seront placés à la droite des chiffres déjà établis ; à partir de la 16e, les lettres seront transcrites, en commençant par la droite, à la gauche des groupes déjà établis ; le groupe suivant est dispersé en commençant de nouveau par la gauche, et ainsi de suite en alternant.

Si le texte n'a pas 38 lettres ou un multiple de 38, on y ajoute des nulles. En opérant ainsi, on obtient le tableau II ci-après :

TABLEAU II.

32.22.1	9.23.31.21.2	10.24.33.37.30.20.3	11.4	12.25.19.5
I	II	III	IV	V

13.26.34.29.18.6	14.27.35.38.36.28.17.7	15.16.8
VI	VII	VIII

On peut aussi chiffrer un nombre de lettres inférieur à 38, en n'utilisant que certains compartiments.

Le capitaine Valério fait remarquer que ce texte chiffré peut être obtenu plus simplement par le tableau III, où les lettres seraient disposées d'après les lois énumérées pour les tableaux I et II, puis relevées par colonnes verticales, en commençant par la gauche, après avoir interverti les lignes dans l'ordre 2.4.6.8.7.5.3.1.

TABLEAU III.

Ordre des colonnes.	I	II	III	IV	V	VI	VII	VIII
Nombre de lettres des colonnes.	3	5	7	2	4	6	8	3
1re ligne.....	1	2	3	4	5	6	7	8
2e »		9	10	11	12	13	14	15
3e »	22	21	20		19	18	17	16
4e »		23	24		25	26	27	
5e »	32	31	30			29	28	
6e »			33			34	35	
7e »			37				36	
8e »							38	

Lecture. — On trace d'abord le tableau I, où l'on transpose les lettres du texte chiffré de la gauche à la droite. Ensuite, on appelle successivement les lettres du cryptogramme, dans l'ordre convenu. On doit avoir soin, comme dans les systèmes analogues, de souligner ou de biffer les lettres au fur et à mesure de leur extraction du tableau.

Déchiffrement. — Si l'on ne possède qu'une dépêche, la traduction se fait comme la lecture, mais l'ordre conventionnel d'extraction des lettres n'étant pas connu, et celles-ci pouvant avoir été brouillées, on fait usage du procédé de glissement et de juxtaposition déjà employé plusieurs fois antérieurement.

Les lettres du cryptogramme étant inscrites dans les cases du tableau, on range les séries en colonnes, de manière que le premier chiffre à droite de chaque compartiment se trouve au-dessous du précédent ; on obtient le tableau IV ci-après :

TABLEAU IV.

7	5	3	1	2	4	6	8
	32	22	1	9	23		
	31	21	2	10	24	33	37
	30	20	3	11			
			4	12	25		
		19	5	13	26	34	
	29	18	6	14	27	35	38
36	28	17	7	15			
		16	8				

Pour une seule dépêche, on ne cherchera pas à reconstituer le tableau II ; mais on opérera en recherchant les coïncidences que le schema IV fait ressortir.

Si l'on a pu recueillir un certain nombre de cryptogrammes, on cherchera à reconstituer le tableau II, et pour cela, on se servira de la remarque suivante due également à Valério :

Suivant que la dépêche a $m \times 38 + 3, + 8, 15, 17, 21, 27, 35, 38$ lettres, on utilisera pour le complément, respectivement 1,2,3,4,5,6,7,8 cases supplémentaires ; or les différences entre les nombres $\mathbf{m \times 38 + A}$ donnent les nombres de lettres de chaque colonne (indiqués en chiffres arabes en tête de celle-ci dans le tableau III).

En conséquence, si l'on possède quelques cryptogrammes, ces différences feront connaître la clef employée, c'est-à-dire le nombre de lettres de chaque case, ou du moins de certains compartiments. Si ces indications ne suffisent pas, les recherches au moyen du tableau IV achèveront le déchiffrement du cryptogramme.

Soit à traduire le cryptogramme :

opvze—meovn—ienru—osudd—dsasu—nednp—nrtev—efexe—etssm—zeuyz—estso—vrou.

Il comporte 59 lettres. Supposons que les indices recueillis ou les tâtonnements nous aient amenés à conclure que le chiffrement est dû à la deuxième méthode Roche.

Recueillons les 38 premiers caractères ; numérotons-les de 1 à 38 et établissons les séries indiquées au tableau IV. Nous aurons : TABLEAU V.

7	5	3	1	2	4	6	8
	o	p	v	z	e		
	m	e	o	v	n	i	e
	n	r	u	o			
			s	u	d		
		d	d	s	a	s	
	u	n	e	d	n	p	n
r	t	e	v	e			
		f	e				

En juxtaposant les colonnes verticales dans l'ordre de leurs numéros, nous obtenons : Vous devez vous défendre pendant un mois. Pren.....

Les 21 lettres restantes auront été chiffrées d'après la règle indiquée plus haut, au moyen des 5 premières cases. Nous allons en retrouver le texte en y appropriant le procédé ordinaire.

Rangeons ces 21 lettres en colonnes ; nous aurons le nouveau tableau ci-après (VI) :

7	5	3	1	2	4	6	8
	x	e	e	t	s		
	s	m	z	e	u	y	z
	e	s	t	s			
			o	v	r		
		o	u				

Nous y lisons le complément du texte précédent : « e z toutes vos mesures x y z. »

A. COLLON
Lieutenant d'artillerie adjoint d'Etat-Major

(A suivre).

ETUDE

SUR LA

CRYPTOGRAPHIE

Son emploi à la guerre et dans la diplomatie (1).

TITRE II.

LA CRYPTOGRAPHIE ACTUELLE

Les méthodes de chiffrement et de déchiffrement.

PREMIÈRE PARTIE.

PROCÉDÉ GÉNÉRAL MONOLITTÉRAL.

Première classe : Systèmes par transposition ou interversion des lettres du texte clair.

CHAPITRE II. — MÉTHODES A CLEF-CONVENTION.

C. Méthodes des grilles proprement dites.

I. *Généralités.* — L'invention des grilles est attribuée au savant mathématicien italien Jérôme Cardan (2). Dans le principe, les grilles avaient pour but de travestir un texte par l'introduction de mots n'ayant aucun rapport avec la dépêche envoyée. C'était une feuille de carton ou de métal

---

(1) Voir Revue de l'armée belge, 2e année Tomes II, III, IV, V.

(2) Son ouvrage « *De subtilitate* » où il consacre un chapitre à cet instrument, a été traduit en français, en 1556, par Richard Leblanc.

dans laquelle on avait découpé irrégulièrement des ouvertures irrégulières. Des points de repère et une flèche indiquaient le sens des transmissions. On inscrivait le texte à expédier dans les découpures, puis on enlevait l'appareil, et l'on remplissait les blancs de mots et de signes quelconques, de manière cependant à leur donner un sens complet qui n'éveillât pas l'attention des lecteurs non prévenus.

Une dépêche transmise sous cette forme aura l'apparence du tableau ci-dessous, où les mots du texte réel sont soulignés :

« Si *vous* pensez que vous *n'avez* presque *rien* de sérieux *à* faire, envoyez-moi des blés sans *craindre* le prix. *Entrez résolument* dans votre rôle et *dans* l'esprit de *la* coutume qui veut qu'un marchand sache dépenser de l'argent au bon moment, afin de profiter de la hausse qui ne manquera pas de se faire sentir bientôt en votre *ville*. »

Pour lire une semblable dépêche, le destinataire se contentait d'appliquer son instrument, identique à l'appareil d'expédition, sur le cryptogramme, et le vrai sens de la transmission apparaissait dans les ouvertures.

On a renoncé presque complètement à ce mode de cryptographie, malgré la sécurité relative que certaines méthodes présentent. La raison en est dans le secret absolu que nécessite son emploi : une grille égarée ou distraite de la possession de son auteur, même un instant, peut interrompre et livrer le secret de la correspondance ; de plus, la multiplicité des relations télégraphiques et leur prix, ne sont pas toujours compatibles avec ce système.

Le principe du procédé ancien peut cependant encore être utilisé, si l'on parvient à disperser les lettres d'un texte dans les cases d'une figure géométrique donnée, suivant une convention qui en constituera la clef.

Si l'ordre dans lequel les cases doivent être remplies est arbitraire, la découverte d'un des instruments-types livre

complètement le secret ; par contre, les cryptogrammes provenant de ce mode de grille, offrent une assez grande résistance aussi longtemps qu'on n'a pas intercepté un grand nombre de dépêches.

Dans les méthodes connues jusqu'à présent, les instruments ont leurs cases numérotées au hasard, mais d'une manière identique. L'expéditeur marque les lettres de sa dépêche et les inscrit à la case indiquée par le numéro correspondant.

Le danger de ce procédé réside par conséquent, dans l'envoi de textes successifs chiffrés avec les mêmes grilles. On sera donc amené à changer fréquemment de grille, ce qui est un grave défaut, ou à modifier l'ordre des transcriptions dans les cases, suivant une convention. Cette dernière manière de faire est préférable, sans toutefois assurer l'indéchiffrabilité, même en admettant que l'instrument et la convention employés restent ignorés du déchiffreur. Nous allons nous en occuper.

Théoriquement, le nombre de grilles est illimité ; en pratique, on n'a employé jusqu'ici que des grilles carrées de faible dimension, de préférence celles comprenant un nombre carré pair de cases.

Grille carrée-type. — Le modèle-type de grille régulière est celui à 36 cases. C'est une plaque carrée (figure I) en métal ou en carton, divisée en 36 compartiments, dont un quart (ceux numérotés sur le dessin) sont découpés à jour.

Pour se servir de cet appareil (fig. I), on trace sur une feuille de papier, un carré identique à celui de la grille, en y marquant les quatre sommets A' B' C' D'.

On applique la grille A B C D sur ce carré, de manière que le côté A B corresponde au côté A' B' du papier ; dans les 9 cases ouvertes, on écrit les 9 premières lettres de la dépêche. On fait ensuite tourner la grille d'un quart de cercle, soit de gauche à droite, soit de droite à gauche, de

Fig. I.

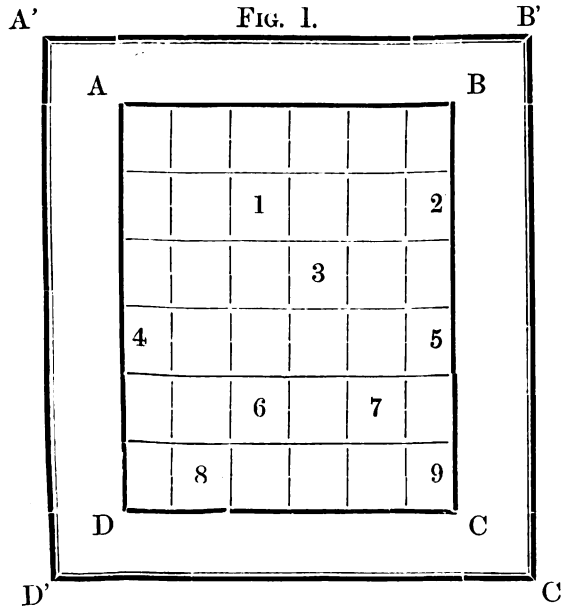


Fig. II.

19	10	28	11	20	12
29	21	1	22	13	2
23	30	14	3	31	24
4	15	25	32	16	5
26	33	6	27	7	17
34	8	35	18	36	9

A B D C

manière que le côté B C ou A D prenne la place du côté A B; on inscrit les 9 lettres suivantes de la dépêche dans les 9 fenêtres ouvertes. On applique successivement les deux autres côtés de la grille sur le côté A' B' du papier, toujours dans le même sens. L'instrument occupe ainsi quatre positions différentes, qui

permettent d'écrire les 36 premières lettres, en les répartissant de la manière indiquée dans la figure II ci-contre.

Si la dépêche a plus de 36 lettres, on peut appliquer un des artifices ci-après :

1°. Retourner la grille et recommencer les opérations comme pour le chiffrement des 36 premières lettres. En fait, on use ainsi d'une grille nouvelle, mais où l'ordre des lettres dans les lignes horizontales seul a été interverti ; résultat : chiffrement de $2 \times 36 = 72$ lettres.

2°. Dans chacun des deux cas précédents, si l'on fait tourner la grille en sens inverse du mouvement primitif, on obtient un nouvel ordre de lettres, où les positions 2 et 4 seules fournissent des figures nouvelles, mais symétriques des groupes de lettres provenant des positions 1 et 3 ; résultat : chiffrement de $2 \times 72 = 144$ lettres.

3°. Dans chacun des cas qui précèdent, il est permis de commencer le mouvement de la grille, de façon que la première coïncidence des deux carrés ait lieu sur des côtés qui ne sont pas homologues ; il est possible de commencer le chiffrement par chacun des quatre côtés, dans un ordre convenu : il en résulte que ce procédé permet de chiffrer un texte de $72 \times 4 = 288$ lettres.

Ici encore les lettres restent groupées par 6 ; il y a simple transposition des groupes, ou interversion des lettres dans les groupes, avec le maintien caractéristique de la symétrie dans le relèvement des lettres et des groupes.

Les trois modes d'emploi réunis permettent le chiffrement varié de $2 \times 288 = 576$ lettres.

Lorsque le chiffrement est terminé, on n'a plus qu'à transcrire les signes par une des méthodes connues.

Appliquons cette grille au texte indiqué ci-après : « L'ennemi fait de grands efforts pour pénétrer dans la place par le front Nord-Ouest » ; en commençant par le côté A B, et en faisant tourner l'instrument de droite à gauche, dans le

sens de la flèche, nous aurons pour les 36 premières lettres, la disposition ci-dessous (figure III).

Et le cryptogramme total, complété par 4 nulles, serait :

Siote — dufff — eeorg — nprnr — teaes — nnpin — eftdr — alefr — adrco — laupo — nenas — srtlt — lnxes — aotrp — dv.

La *lecture* d'un semblable texte chiffré se fait en disposant les caractères en 6 colonnes et sur 6 rangées, dans un tableau ayant les dimensions de la grille ; on y applique celle-ci par le côté convenu, puis on transcrit les signes dans l'ordre d'appel.

A ☞ FIG. III. B

s	i	o	t	e	d
u	f	l	f	e	e
o	r	g	n	p	r
n	r	t	c	a	e
s	n	m	p	i	n
e	f	t	d	r	a

D C

La grille classique exige le secret, et malgré cela, elle est loin d'assurer l'indéchiffrabilité. Plusieurs auteurs ont tenté de remédier à ses inconvénients, mais aucune solution satisfaisante n'a été publiée.

Nous examinerons ces procédés, puis nous ferons connaître un système de grilles cubiques simples et doubles, que nous préconisons pour répondre aux exigences de la correspondance secrète militaire et diplomatique.

Déchiffrement. — Pour le chiffrement des textes par la grille, on fait tourner celle-ci autour de son centre. Il s'ensuit que les fenêtres sont toujours à égale distance de ce centre, et sont symétriquement placées par rapport à un diamètre. Les clefs du système sont par conséquent, la po-

sition des cases à jour, le point de départ et le sens de rotation de la grille.

Ce sont ces remarques, et celles faites plus haut à propos du chiffrement, qui forment la base de la méthode de déchiffrement.

En effet, disposons la grille A B C D dans les quatre positions types successives, nous aurons les figures ci-après :

FIG. 1.

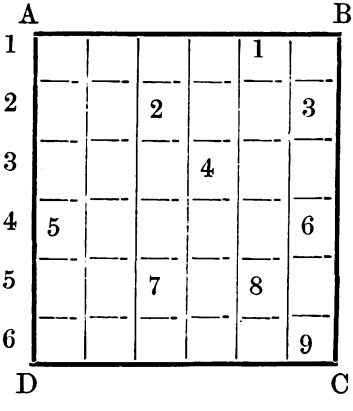


FIG. 2.

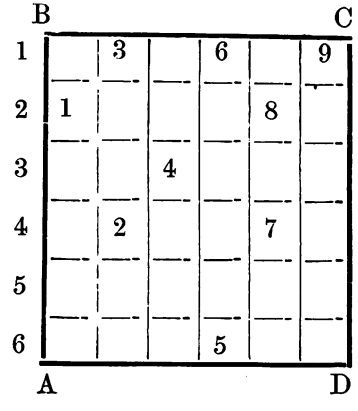


FIG. 3.

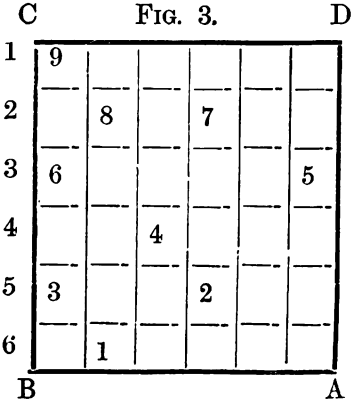
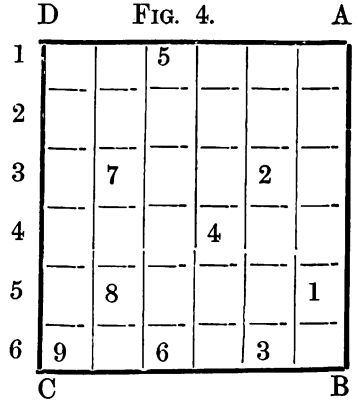


FIG. 4.



Si l'on condense ces quatre figures en une seule, où l'ordre naturel des cases serait marqué d'un indice signalant les chiffres symétriques, on reconnaîtra plus rapidement la structure générale des cryptogrammes « *grillés* » et des variations qu'ils peuvent subir. On y puisera en outre le moyen de chiffrer directement, sans instrument, en suivant le tableau de disposition des caractères ; nous aurons ainsi la figure 5.

FIG. 5.

1 9_3	2 3_2	3 5_1	4 6_2	5 1_1	6 9_2
7 1_2	8 8_3	9 2_1	10 7_3	11 8_2	12 3_1
13 6_3	14 7_1	15 4_2	16 4_1	17 2_1	18 5_3
19 5_1	20 2_2	21 4_3	22 4_1	23 7_2	24 6_1
25 3_3	26 8_1	27 7_1	28 2_3	29 8_1	30 1_1
31 9_1	32 1_3	33 6_1	34 5_2	35 3_1	36 9_1

Nous constatons que la connaissance d'une lettre suffit pour déterminer les lignes symétriques, dans les trois autres positions de la grille ; quel que soit l'ordre dans lequel les figures se succèdent, la règle des écarts moyens des nombres de voyelles indiquera au déchiffreur les côtés du carré parallèles à la direction du chiffrement.

Soit le cryptogramme : euuns — erimm — aauat — illnt — eiame — eoatq — uidue — n.

Disposons les lettres en colonnes ; nous aurons (fig. 6).

FIGURE 6.

	4	5	3	4	3	2	voyelles
1	e	u	u	n	s	e	4
2	r	i	m	m	a	a	3
3	u	a	t	i	l	l	3
4	n	t	e	i	a	m	3
5	e	e	a	a	t	q	4
6	u	i	d	u	e	n	4

Sur 36 lettres, il y a 22 voyelles, soit 3.66 voyelles par ligne. Cette moyenne est satisfaite dans les lignes horizontales ; les écarts sont plus grands pour les colonnes verticales ; il est donc probable que le chiffrement a commencé horizontalement. Cette connaissance de l'origine du chiffrement n'a cependant pas grande importance.

En effet, si nous extrayons du tableau cryptogrammique les lettres symétriques, suivant les figures 1, 2, 3, 4, nous aurons, en commençant l'extraction par la première lettre de la fig. 1, la suite naturelle des signes de chaque tranche de neuf caractères (fig. 7).

FIGURE 7.

	1	2	3	4
1	u	u	e	m
2	n	r	s	a
3	e	a	i	i
4	a	l	m	n
5	t	i	u	m
6	t	e	l	a
7	a	u	e	t
8	q	d	e	i
9	u	e	a	n

Il ne nous reste plus qu'à juxtaposer ces diverses tranches, en nous aidant du sens, des fréquences des voyelles et des séquences probables.

En disposant horizontalement ces 4 colonnes verticales, nous aurons (fig. 8).

FIGURE 8.

1	2	3	4	5	6	7	8	9
u	n	e	a	t	t	a	q	u
u	r	a	l	i	e	u	d	e
e	s	i	m	u	l	e	e	a
m	a	i	n	m	a	t	i	n

et le sens véritable s'en déduit aisément, nous fournissant enfin le texte clair : « Une attaque simulée aura lieu demain matin. »

On a tenté de compliquer cette méthode de grilles :

1° Par le relèvement horizontal, vertical ou diagonal, direct ou en boustrophédon ;

2° En intervertissant le rang des lignes ou des colonnes de lettres, dans un ordre déterminé par une clef littérale.

Nous avons vu que le premier artifice n'augmente pas de beaucoup la sécurité des cryptogrammes obtenus de cette manière ; quant au second, on peut faire la remarque suivante : deux lettres successives du texte clair dispersées dans une grille donnée, ont entre elles un intervalle fixe. Si l'on dérange l'ordre des lignes ou des colonnes pour le relèvement, ce nombre-intervalle ne peut être influencé en plus ou en moins, que par un nombre multiple de la racine carrée du nombre de cases (36).

Ainsi (fig. I) entre 2 et 3, il y a un intervalle de 4 cases ; si la troisième ligne devient successivement quatrième, cinquième, sixième ou première ligne, l'intervalle devient

respectivement $4 + (6 \times 1)$, $4 + (6 \times 2)$, $4 + (6 \times 3)$ et $4 + (6 \times 4)$; lorsque ces intervalles sont comptés inversement, entre 5 et 4, ils deviennent respectivement : $6^2 = 36 - (4 + 6 \times 4) - 4 + 6 \times 3)$ etc.

Dans une même ligne, ou dans une même colonne, si l'on rapproche ou éloigne les caractères, c'est-à-dire si on les intervertit, le chiffre intervalle 4 varie simplement entre 1 et 5. Il y a donc entre deux lettres consécutives du texte clair un intervalle maximum égal ici à $6 + (6 \times 5) = 36$ ou $n + n (n - 1) = n^2$.

On en conclut qu'il suffit de rechercher dans le texte chiffré les lettres indicatrices : Q, X, H, J, E, Y, qui exigent immédiatement avant ou après elles certaines autres lettres. Dès lors, l'intervalle entre deux lettres peut être connu, et l'on en déduira le genre de permutation employée pour le relèvement, s'il y a lieu.

Pour faciliter son travail, le déchiffreur fera usage d'une série de tableaux, analogues aux figures 1 à 4 qui précèdent, pour les principales espèces de grilles.

Dès que les relations de 2 ou 3 lettres sont connues, la symétrie de position permettra de connaître les quatre séries semblables. A partir de ce moment, les lois des séquences et des fréquences permettront d'achever rapidement le déchiffrement.

A titre d'exemple, voici un modèle (fig. 9) de grille à 64 cases, pourvue de 16 lucarnes pour le chiffrement successif par rotation. Elle permet l'interversion composée de $64 \times 4 \times 4 = 1024$ lettres.

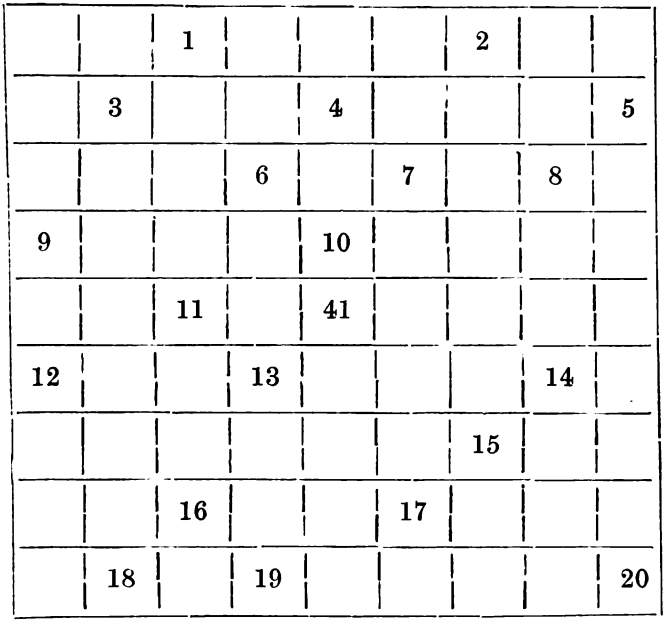
FIG. 9.

1				2		3	
	(4)				5	(15)	
		6					
		7			8		9
				10		11	
		12					
13	(50)			14		(55)	
		15			16		

NOTE. — Les chiffres entre parenthèses indiquent l'ouverture des 4 cases correspondant à la 4e fenêtre, c'est-à-dire à la 10e case de l'ordre naturel. Le nombre d'ouvertures de la grille $= \frac{64}{4} = 16$.

Enfin la figure 10 ci-après, indique une grille de 81 cases, c'est-à-dire d'un nombre carré impair de cases, et comprenant 20 fenêtres pour le chiffrement, plus une vingt-et-unième, pour la rotation. Cette case qui occupe le rang $\frac{80}{2} + 1 = 41$ ne reçoit point les lettres du texte à chiffrer.

Fig. 10.



Génération des grilles carrées. Examinons actuellement le mode de formation des grilles carrées.

Une observation des grilles décrites ci-dessus, montre que l'ouverture d'une fenêtre ou case, dans une grille, n'est pas arbitraire ; elle se fait en vertu d'une loi qui exige que, dans le mouvement de rotation de l'instrument, jamais une ouverture ne puisse coïncider avec une lettre déjà inscrite.

Si nous ouvrons une case quelconque dans la grille, elle recevra successivement quatre lettres du texte à chiffrer, par l'occupation de ses quatre positions différentes. Le nombre de fenêtres à ouvrir dans une grille est donc

égal au nombre total de cases, divisé par 4, nombre de rotations possibles.

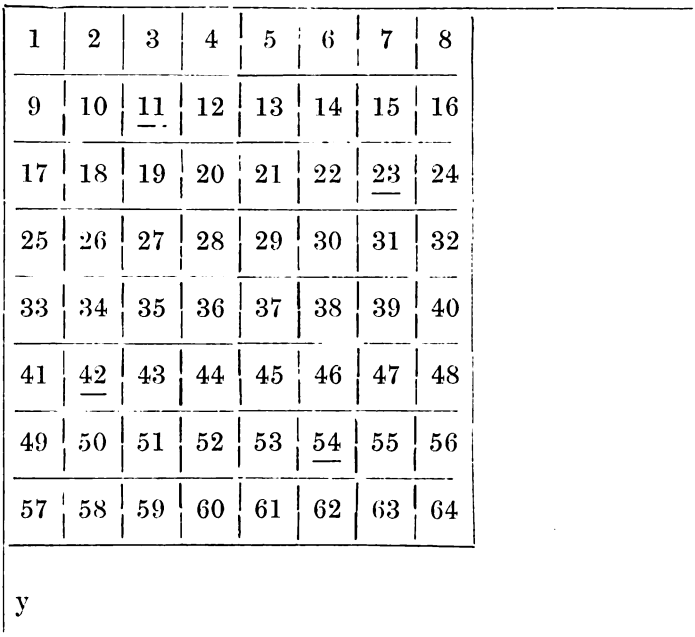
Voyons maintenant l'ordre dans lequel les cases doivent s'ouvrir.

Nous avons déjà vu précédemment, que pendant la rotation de la grille, les fenêtres occupent des positions symétriques par rapport au centre de l'instrument : l'ouverture d'une case (que nous indiquerons par un chiffre), indique par cela même l'emploi de trois autres cases invariablement liées à la première.

Leur recherche partielle offrant des tâtonnements d'autant plus longs que l'instrument comporte plus de cases, il y a avantage à procéder analytiquement.

Pour cela, prenons deux axes de coordonnées. et rappor-

FIG. 11.



tons-y la grille de la figure 9, dans laquelle chaque case sera numérotée suivant l'ordre naturel (fig. 11).

L'ouverture de la case 11 par exemple, s'écartant de deux unités à partir de l'axe des x, et de trois unités à partir de l'axe des y, amène dans les trois autres positions de l'instrument, l'ouverture des cases 23, 54 et 42, indiquées par un trait.

En vertu de cette loi analytique, remarquons que les nombres sont liés entre eux par des équations que nous allons mettre en évidence :

La case 11, d'une part, correspondra à la case
$64 + 1 - 11 = 54$;

La case 23, d'autre part, correspond à la case
$64 + 1 - 23 = 42$;

La case 23 répond aussi à la case 11, par la relation :
$(11 - 8)\ 8 - 1 = 23$;

La case 23 répond encore à la case 54, par la relation :
$(23 - 2 \times 8)\ 8 - 2 = 54$;

Constatons de plus que $54 + 11 = 23 + 42$, c'est-à-dire que la somme des extrêmes est égale à la somme des moyens.

Généralisons la méthode ; appelons n^2 le nombre total de cases, $\sqrt{n^2} = n$ sera le chiffre de cases du côté du carré.

Soient M, N, P, Q les numéros d'ordre croissants des cases amenées par les quatre rotations effectuées dans un sens. Nous aurons :

1° $M + Q = N + P$

2° $n^2 + 1 - M = Q$

$n^2 + 1 - N = P$

3° Pour les relations entre M et N, les différents cas ci-après peuvent se présenter :

$$\begin{matrix} M \\ ou \\ N \end{matrix} \leq n, \quad n < \begin{matrix} M \\ ou \\ N \end{matrix} \leq 2n, \quad 2n < \begin{matrix} M \\ ou \\ N \end{matrix} \leq 3n, \quad 3n < \begin{matrix} M \\ ou \\ N \end{matrix} \leq \frac{n^2}{2} \ (1)$$

Dans le premier cas, $\left(n - \begin{matrix} M \\ ou \\ N \end{matrix} \right) n + 1 = \begin{matrix} P \\ ou \\ M \end{matrix}$;

Dans les trois autres cas, la relation entre les deux premiers termes, M et N, s'établit par la formule (*a*)

$$\left[M - \begin{pmatrix} n \\ 2n \\ 3n \end{pmatrix} \right] n - \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = N \quad (a)$$

La relation entre le deuxième et le quatrième terme, N et Q, s'obtient par la formule (*b*)

$$\left[N - \begin{pmatrix} n \\ 2n \\ 3n \end{pmatrix} \right] - \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = Q \quad (b)$$

La synthèse de la construction des grilles carrées peut être exposée de la manière ci-après :

1° Le nombre de cases du côté de la grille étant n, le nombre total de cases de la grille carrée est évidemment n^2,

2° Le nombre maximum de fenêtres à ouvrir dans une grille carrée est $\frac{n^2}{4}$, si n est pair; et $\frac{n^2 - 1}{4}$, si n est impair;

3° Dans la grille où le côté est pair, la rotation se fait autour de l'intersection des diagonales, ou des diamètres du carré.

Lorsque le côté comprend un nombre impair de cases, cette rotation se fait autour de la case centrale elle-même qui occupe le rang $\frac{n^2}{4} + 1$, et qui ne reçoit pas de lettres.

---

(1) $\frac{n^2 + 1}{2}$, si n^2 est impair.

4° L'ouverture du nombre requis de cases se fait à volonté, tout en tenant compte des lois de relation entre la situation des cases qui, comme nous l'avons exposé, ne peuvent amener de double emploi.

5° L'examen de la structure générale des grilles carrées nous a fait découvrir les lois qui régissent l'ordre de succession des séries de cases. Ces relations permettent la construction immédiate d'une grille, par l'établissement des progressions arithmétiques, indiquées dans le tableau ci-contre :

Formules générales pour la construction des grilles carrées.

Première série de progressions (n — 1 termes).

M	N	P	Q
1	n	$n^2 - (n - 1)$	n^2
2	2 n	$n^2 - (2n - 1)$	$n^2 - 1$
3	3 n	$n^2 - (3n - 1)$	$n^2 - 2$
⋮	⋮	⋮	⋮
n—1	(n—1) n	$n^2 - [(n-1)n - 1]$	$n^2 - (n-2)$

Deuxième série de progresssions (n—3 termes).

1+(n+1)	n+(n—1)	$n^2 - 2(n-1)$	$n^2 - (n+1)$
2+(n+1)	2n+(n—1)	$n^2 - 2(n-1) - n$	$n^2 - (n+2)$
3+(n+1)	3n+(n—1)	$n^2 - 2(n-1) - 2n$	$n^2 - (n+3)$
⋮	⋮	⋮	⋮
(n—3)+(n+1)	(n—3)n+(n—1)	$n^2 - 2(n-1) - (n-4)n$	$n^2 - [(n+(n-3)]$

Troisième série de progressions (n—5 termes).

1+2(n+1)	n+2(n—1)	$n^2 - 3(n-1)$	$n^2 - 2(n+1)$
2+2(n+1)	2n+2(n—1)	$n^2 - 3(n-1) - n$	$n^2 - (2n+3)$
⋮	⋮	⋮	⋮
(n—5)+2(n+1)	(n—5)n+2(n—1)	$n^2 - 3(n-1) - (n-6)n$	$n^2 - [(2n+(n-4)]$

Quatrième série de progressions (n—7 termes).

etc.	etc.	etc.	etc.

Remarques. — L'application des équations entre M, N, P et Q pour la détermination de ces valeurs, fournit les deux catégories d'identités ci-après :

$$1^\circ \qquad 1 + n^2 = n + [n^2 - (n - 1)] = n^2 + 1$$

$$2^\circ \qquad n^2 + 1 - 1 = n^2$$
$$n^2 + 1 - n = n^2 - (n - 1)$$

ce qui prouve la parfaite exactitude des formules qui leur ont donné naissance.

Les colonnes M et Q sont des progressions arithmétiques respectivement croissantes et décroissantes, dont la raison est l'unité; les colonnes N et P sont des progressions semblables dont la raison est n, le côté du carré.

Les progressions extrêmes commencent par les termes extrêmes 1 et n^2; les progressions moyennes, par les termes précédents augmentés et diminués respectivement de (n—1).

Le premier terme de chaque série, à partir de la deuxième, est égal au premier terme de la série précédente, augmenté ou diminué respectivement de (n + 1) pour les séries extrêmes; augmenté ou diminué respectivement de (n —1) pour les séries moyennes.

Le nombre des termes de chaque série successive, forme une progression arithmétique décroissante, dont le premier terme est n — 1, et dont la raison est 2.

La construction ci-après de la grille carrée de $9^2 = 81$ cases, sera une application de ces formules générales. Elle fera clairement comprendre le mode de construction concret d'une grille donnée.

Grille de 9².

1re série 8 termes	1 (1+8)=9	9 (1+81=9+73)	73 (81—8=73)	81
	2	18	64	80
	3	27	55	79
	4	36	46	78
	5	45	37	77
	6	54	28	76
	7	63	19	75
	8	72	10	74
	+10=(9+1)	+8=(9—1)	—8	—10
2e série 6 termes	11	17	65	71
	12	26	56	70
	13	35	47	69
	14	44	38	68
	15	53	29	67
	16	62	20	66
	+10	—8	—8	—10
3e série 4 termes	21	25	57	61
	22	34	48	60
	23	43	39	59
	24	52	30	58
	+10	+8	—8	—10
4e série 2 termes	31	33	49	51
	32	42	40	50
	+10	+8	—8	—10
5e série 1 terme	41	41 (case centrale)	41	41

Nombre de grilles. — Nous savons que n^2 est le nombre de cases d'une grille carrée, et que $\frac{n^2}{4}$ est celui des fenêtres.

Si nous faisons tourner le système des ouvertures de manière que chacune d'elles prenne la place (comme rang) de la suivante, nous obtiendrons une grille nouvelle.

Comme nous pouvons répéter cette opération $\frac{n^2}{4}$ fois, nous aurons $\frac{n^2}{4} = m$ grilles nouvelles, c'est-à-dire le nombre des combinaisons de m objets, un à un. De même, nous pouvons opérer cette substitution deux par deux, trois par trois, etc. ; le nombre de figures nouvelles sera respectivement celui des combinaisons de m objets, deux à deux, trois à trois, etc.

La somme de toutes les combinaisons possibles sera par conséquent la somme des coefficients du développement du binôme $(x + a)^m$.

On obtient cette somme en faisant dans le binôme $x = a = 1$

d'où $2^m = 1 + Cm_1 + Cm_2 + Cm_3 + \ldots + Cm_m$ (a)

d'où $2^m - 1 = Cm_1 + Cm_2 + Cm_3 + \ldots + Cm_m$ (b)

Exemples. — Pour la grille $n^2 = 36$ cases, $\frac{n^2}{4} = m = 9$; nous pouvons donc construire $2^9 - 1 = 511$ grilles différentes.

Dans la grille de 64 cases, m $\frac{64}{4} = 16$; nous pouvons alors construire $2^{16} - 1 = 65.525$ variétés de grilles.

Cette infinité d'instruments différents ne met cependant pas les cryptogrammes à l'abri du déchiffrement. Comme nous l'avons vu, la symétrie obligée de leur

construction, et la connaissance des fréquences et des séquences de la langue, ont bien vite mis le chercheur sur la voie qui sera toute tracée, dès que quelques lettres seulement du texte seront juxtaposées.

GRILLES SPÉCIALES.

GRILLE IRRÉGULIÈRE DU MARQUIS DE VIARIS (1).

Cet instrument devrait rationnellement être classé parmi les méthodes irrégulières à clef-convention. Nous l'analysons après les grilles proprement dites, parce que son auteur l'a compris sous ce nom

(1) Le Génie civil — tome 13-1888.

Grille irrégulière Viaris.

+	Sp.	119	120	121	122	123	124	125	126	127	128	+	+
+	+	S									J		
+	+	I	26	27	28	29	30	31	32	H			
+	+	U							F				
+	T	52	53	54	55	56	57	B					+
+	P						D						+
+	Q					G	97	98	99	100	101	102	+
X	78	79	80	81	C	86	87	88	89	90	91	+	+
Z				A								+	+
K			E	44	45	46	47	48	49	50	51	+	+
Y				R	64	65	66	67	68	69	70	+	+
V	1	2	3	4	O	109	110	111	112	113	114	+	+
+	B					L							+
+	D						N	92	93	94	95	96	+
+	G	38	39	40	41	42	43	M					+
+	+	O	58	59	60	61	62	63	V	82	83	84	85
+	+	R	13	14	15	16	17	18	19	Y			
+	+	E	5	6	7	8	9	10	11	12	K		
+	+	A								Z			
+	+	C	20	21	22	23	24	25	X	115	116	117	118
+	L							Q					+
+	N	33	34	35	36	37	P						+
+	M					T	103	104	105	106	107	108	+
F					U							+	+
H				I	71	72	73	74	75	76	77	+	+
J			S									+	+
+	+	Sp.	129	130	131	132	133	134	135	136	137	138	+

Leon. del.

La grille du marquis de Viaris est basée sur les principes suivants :

1° Les rangées horizontales d'un rectangle quadrillé sont marquées deux fois par les lettres successives de deux alphabets ; le premier alphabet occupe un certain nombre de cases dans les trois premières colonnes; le second est dispersé en zig-zag dans tout le rectangle, d'une manière arbitraire, ou d'après une convention.

2° Pour chiffrer un texte, on transcrit les caractères dans les cases des lignes horizontales correspondant aux lettres de la clef, en commençant par le premier ou par le deuxième alphabet, suivant que le mot-clef contient un nombre impair ou pair de lettres.

Soit à chiffrer un texte avec la clef : Vercingétorix. (1)

L'ordre dans lequel on a inscrit successivement les différentes tranches de lettres est: V, E, R, C, I, N, G, du premier alphabet, E du second, T, O du premier, R, I du second, X du premier, enfin V, C, N, G, T, O, X, du second alphabet ; soit un nombre de tranches double du nombre de lettres *différentes* du mot clef. Nous arrivons à chiffrer, dans le cas ci-dessus, 118 lettres. En y ajoutant celles provenant des deux lignes supplémentaires extrêmes, nous parvenons à 138.

Le relèvement des lettres se fait verticalement en commençant par la colonne de gauche, ou dans un ordre convenu, par exemple, le rang des lettres de la clef littérale, répétée au besoin.

Pour la *lecture*, le destinataire marquera au crayon les cases qui doivent recevoir les lettres de la dépêche ; puis il y inscrira le texte chiffré dans l'ordre des colonnes verticales.

---

(1) Les chiffres inscrits dans la grille représentent l'ordre de dispension des lettres du texte.

Remarques. — 1° La méthode exige absolument le secret pour offrir quelques garanties de sécurité.

2° Les alphabets provenant de la clef littérale doivent être écrits à l'avance dans le tableau, sinon les risques d'erreur seront fort grands.

3° La clef doit être adroitement choisie, si l'on veut éviter que le nombre de lettres du texte clair, à transcrire dans le tableau, se réduise considérablement.

4° Il faudra changer fréquemment le mot-clef pour ne pas donner prise aux comparaisons.

5° Si l'expéditeur a rempli les cases vides par des lettres quelconques, choisies ou non, il augmente de beaucoup le travail du chiffrement et de la lecture ; il aura presque doublé le nombre de caractères à transmettre.

6° La dispersion irrégulière des lettres du texte, but de la grille Viaris, peut être obtenu par la grille ordinaire, en y inscrivant les caractères, suivant un ordre déterminé par une convention quelconque; par exemple: 10,20,30,40,etc.; 1, 11, 21, 31, 41, etc.; 2, 12, 22, 32, 42, etc., etc.

Déchiffrement. — Dans l'hypothèse 5°, la réduction du cryptogramme s'opérera aisément, si l'on a en sa possession le tableau type; il suffit alors de transcrire le texte dans l'ordre des colonnes verticales. Si celles-ci ont été au préalable interverties, on formera les lettres du texte chiffré en autant de colonnes de lettres que le tableau en comporte, comme dans les méthodes régulières des diviseurs ou des grilles exposées précédemment : les règles linguistiques connues aideront puissamment le chercheur dans la juxtaposition des colonnes verticales.

Si le texte chiffré obtenu est transmis sans remplissage par des nulles, tel :

78, 1, 119, 52, 79, 2, 38, 33, 120, 26, 53, 80, 3, 39, 58, 13, 5, 20, 34, 129, 121, 27, 54, 81, 44, 4, 40, 59, 14, 6, 21, 35, 130, 122, etc., les essais de permutation, dictés par la

présence des lettres indicatrices Q, X, H, J, Y, B, E, amèneront bien vite la réunion de quelques bigrammes, trigrammes et quatrigrammes : 78. 79. 80. — 1. 2. 3. 4. 5. — 119. 120. — 38. 39., etc.

Si les colonnes ont été interverties, la réduction sera un peu plus difficile ; les premiers tâtonnements consisteront alors à reconstituer ces colonnes dans un ordre quelconque, mais avec leurs nombres respectifs de lettres. A partir de ce moment, les opérations marcheront plus facilement. Les lois des séquences et des fréquences indiqueront les essais les plus probables à tenter, pour remettre les lettres à leurs places respectives, dans les lignes successives.

En résumé, la répartition des lettres dans un ordre irrégulier, l'ouverture d'un plus grand nombre de cases, n'obligeant pas à inscrire dans la grille un nombre multiple de la racine carrée de la grille, l'interversion par la grille d'un texte déjà chiffré, sont des palliatifs insuffisants contre le déchiffrement ; d'autre part, ces artifices augmentent le travail des correspondants et les chances d'erreurs.

Conclusion : l'emploi des grilles étudiées jusqu'ici, n'offre une certaine sécurité qu'aussi longtemps que les correspondants usent de plusieurs instruments, et gardent le secret le plus absolu. Cette condition exige que les agents chiffrent et lisent eux-mêmes leurs cryptogrammes, dans l'isolement le plus complet.

On peut donc condamner, dans la plupart des cas, l'usage des grilles, et même des instruments quelconques, comme nous le verrons, si leur perte ou leur divulgation livrent aux intéressés le secret de la correspondance.

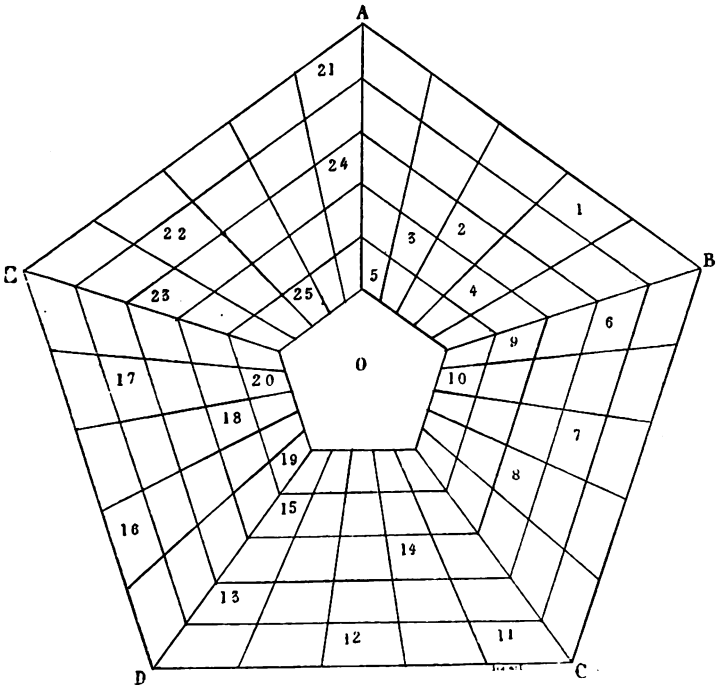
En imaginant son intéressante grille, la plus sérieuse de celles examinées jusqu'à présent, M[r] de Viaris lui a donné pour base une loi de génération qui restreint singulièrement la résistance au déchiffrement. La dispersion des

lettres, tout irrégulière qu'elle soit, est encore trop régulière, et c'est ce qui, outre l'exigence du secret de l'instrument, fait la faiblesse de cette méthode.

En cherchant à éviter ces inconvénients, nous avons été amené à construire des grilles ayant la forme pentagonale, hexagonale, heptagonale, etc., de manière à multiplier le nombre de cases de l'instrument, et à augmenter la dispersion des signes du texte à chiffrer, tout en donnant moins de prise aux essais du chercheur.

A titre d'exemple, nous décrivons ci-après (figure A) la *grille pentagonale régulière:*

Figure A.



Les côtés et les rayons des triangles-secteurs de ce pentagone sont subdivisés de manière à former 5 sous-grilles de 25 cases chacune.

Les cases-fenêtres y ont été ouvertes d'après les principes connus. On remarquera qu'il n'est point nécessaire que le nombre d'ouvertures soit de 5 dans chaque secteur. Ce nombre y varie au gré des correspondants, de 0 à 25, sans que le nombre total de fenêtres puisse être inférieur ou supérieur à 25.

L'instrument ainsi préparé jouit de la propriété de pouvoir chiffrer en cinq fois, $5^3 = 125$ lettres, par cinq rotations successives, dans le même sens. Le retournement double ce chiffre.

N étant le nombre de côtés du polygone régulier, toutes les grilles construites sur le mode de la figure A permettent le chiffrement direct de $2 \times n^3$ caractères. Le nombre de grilles de chaque espèce sera égal à la formule 2^m—1, trouvée précédemment, m étant égal ici à $\frac{n^3}{n}$.

Le relevé des lettres peut se faire par un angle quelconque du polygone A B C D E, suivant convention.

Le relèvement par secteur successif amène trop de régularité dans les séries de lettres du texte, et fournit ainsi des points de repère aux recherches.

La transcription concentrique procure une dispersion des lettres suffisamment irrégulière pour augmenter sensiblement les tâtonnements.

Ces propriétés renforcent sérieusement la sécurité des textes chiffrés par ces instruments. Toutefois, elles n'assurent pas encore l'indéchiffrabilité, précisément parce que la connaissance de la position d'une seule lettre, amène symétriquement, celle de 5, 6..... n autres lettres, suivant le nombre de côtés du polygone régulier.

GRILLE CUBIQUE SIMPLE.

Figure B.

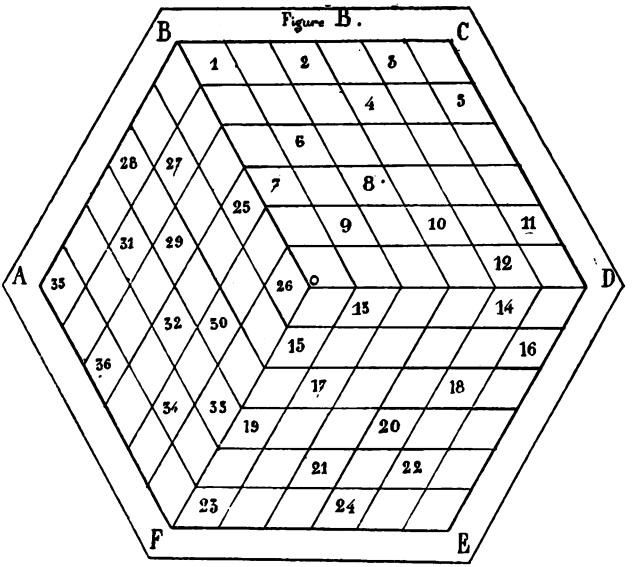
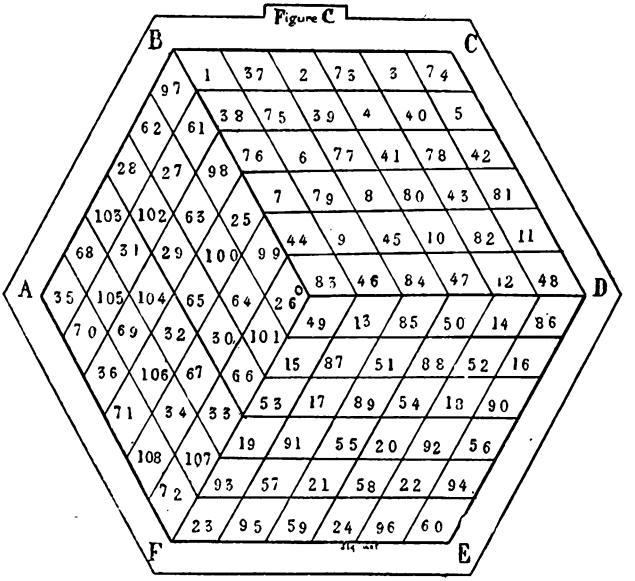


Figure C



Parmi les grilles provenant de cette catégorie de figures, deux types méritent une mention particulière, parce que leur emploi présente une sécurité réelle, une quasi indéchiffrabilité matérielle, sans être obligé de cacher l'instrument servant aux opérations: Ce sont les *grilles cubiques, simple,* (figures B et C) et *double* (fig. D), que nous allons examiner.

La *grille hexagonale régulière,* analogue à la grille pentagonale régulière, sera formée de six secteurs de 36 cases (ou 6^3=216 cases), venant se placer dans six positions différentes, par six rotations successives autour du centre de figure.

Par contre, la *grille cubique simple* ne comprend que trois secteurs de 6^2, ou 108 cases réparties dans trois losanges égaux, tournant autour du centre, de manière à venir occuper successivement la position des trois faces visibles d'un cube ; d'où le nom de *grille cubique.*

Le nombre de fenêtres percées dans l'ensemble de la grille est égal au nombre total de cases divisé par 3. Leur répartition dans les losanges varie au gré des correspondants d'après une loi de génération analogue à celle que nous avons trouvée pour les grilles carrées, (dans la figure B, elle a été faite par tiers égaux, à titre de curiosité).

Dans la figure C, la dispersion des 108 lettres d'un texte a été obtenue par la rotation de droite à gauche, de B O en O F, puis de O F en O D. Le relèvement direct suivant les tranches parallèles à E D C, produira le cryptogramme : (1).

60. 94. 56. 90. 16. 86. 48. 11. 81. 42. 5. 74. — 96. 58. 20. 54. 89. 50. 47. 10, etc., etc. Le retournement de la grille produit le chiffrement de 108 autres caractères.

Il est avantageux de chiffrer des parties de texte, alternativement par la face supérieure (recto), et par la face inférieure (verso) de la grille, afin de brouiller davantage les chiffres.

(1) En remplaçant les lettres de la dépêche par leurs rangs dans le texte.

La disposition, comme le relèvement, peuvent s'opérer de nombreuses manières : par un des angles, par le centre vers un des angles du polygone, concentriquement ou par bandes parallèles à deux côtés, ou aux axes de la figure.

Toutes ces indications peuvent être faites oralement d'avance ; mais il vaut mieux user d'un moyen qui supprime ces conventions préalables et évite les erreurs.

A cet effet, le centre et les angles du polygone sont sept points remarquables ; on peut les désigner cryptographiquement par sept lettres d'un mot-clef, Louvain par exemple.

Si l'on numérote ce mot de la façon habituelle, nous aurons un des groupes de concordances ci-après :

L	O	U	V	A	I	N			A	I	L	N	O	U	V	
O	A	B	C	D	E	F		ou	O	A	B	C	D	E	F	
1	2	3	4	5	6	7			1	2	3	4	5	6	7	

Afin d'annoncer au destinataire les modes de chiffrement et de relèvement, employés par l'expéditeur pour composer la dépêche chiffrée, celle-ci est précédée des lettres de la clef qui marquent l'origine et le sens des opérations.

Ainsi, pour faire connaître que le chiffrement a été fait comme dans la figure C, on commencera le cryptogramme par les lettres U A L I U N, équivalentes des lettres B D O E B F, représentant les angles extrêmes des losanges et le sens du travail.

Le relèvement opéré plus haut sera figuré par les lettres I A V, équivalentes des lettres E D C, désignant cette ligne brisée.

La face opposée de la grille peut être distinguée par les lettres : P, pour le centre ; G, H, I, J, K, L, pour le périmètre de l'hexagone.

Si l'on fait usage du retournement, on emploiera un mot-clef plus long, ou mieux, on choisira un membre de phrase ordonné en clef littérale et numérale comme suit :

Par exemple. « La cryptographie est un art et une science », donnera :

L A C R Y P T — O G P H I E S U N
O A B C D E F — P G H I J K L
1 2 3 4 5 6 7 — 1 2 3 4 5 6 7

1° Pour désigner le retournement simple, on écrira :

B D O E B F H J P K H L
ou C Y L P C T P I O E P S

2° Pour indiquer le retournement alternatif, par losange nous écrirons :

B D H J O E P K B F H L
ou C Y P I L P O E C T P S

Afin de rendre complète la sécurité des cryptogrammes, il convient de permettre *ad libitum* le chiffrement et le relèvement direct ou en boustrophédon, et l'usage facultatif d'un jeu de plusieurs grilles (une demi-douzaine, par exemple), de manière que la grille employée et le changement d'instrument puissent être, le cas échéant, annoncés dans le corps d'un cryptogramme.

Il faut encore que toutes ces variantes soient comprises aisément du destinataire, avec la garantie du secret, par les seules ressources qu'offre la connaissance de la clef littérale.

Pour réaliser ces desiderata, il suffit de faire usage d'une clef de 24 lettres (1) qu'on obtient aisément :

1° En complétant une clef littérale assez longue par l'addition des lettres restantes de l'alphabet :

L A C R Y P T — O G P H I E S — U N B D F J K, etc
1 2 3 4 5 6 7 1 2 3 4 5 6 7 1 2 3 4 5 6 7

2° En transformant la clef provenant du mot Louvain par un dispositif convenu (2) :

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

(1) Suppression du K et du W. — (2) Nous verrons plus tard les différents modes de formation des clefs littérales et numérales, et la manière de ne donner aucune prise au chercheur.

Ce qui donne :

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

L'ensemble du système comportera donc l'usage d'une clef littérale provenant d'un mot d'ordre. La possession de celui-ci permettra de composer instantanément, si c'est nécessaire, les séries représentant les diverses conventions, vis-à-vis de leurs équivalents en clair :

1° Les différentes grilles :

L U F, B D R, J P I, X Z G, O V S, C E N
1 1 1 2 2 2 3 3 3 4 4 4 5 5 5 6 6 6

2° La face recto des grilles :

L B J X O C M ou F R I G S N H
O A B C D E F O A B C D E F

3° La face verso des grilles :

U D P Z V E G
P Q R S T U V

Dans le but de dépister les recherches, les faces seront désignées à volonté par les 5 ou 6 premières, ou dernières, ou encore par les 8 lettres du groupe.

4° Le mode de disposition ou le relèvement en boustrophédon :

M Q H
7 7 7

5° La rotation en sens inverse (1) :

Y A T
8 8 8

En transmettant, comme en recevant un cryptogramme, le destinataire, comme l'expéditeur, noteront avec le plus grand soin les séries de lettres figurant les conventions générales et particulières.

Pour chiffrer un texte, on trace ou l'on calque sur une

(1) La rotation directe a lieu dans le sens des aiguilles d'une montre.

feuille de papier, une grille semblable au format de celles qu'on possède. (En pratique, on usera de feuilles préparées sur leurs deux faces). On transpose le texte suivant les cases ouvertes dans l'ordre convenu, ou indiqué par la clef. On procède ensuite à la rotation de la grille ou à son retournement, et l'on continue la transposition.

Lorsque celle-ci est achevée, on fait le relèvement des lettres, d'après la disposition marquée par la clef, et l'on transcrit la dépêche dans la forme voulue par la transmission.

On inscrit en tête du texte chiffré, et l'on intercale dans le corps de la dépêche, les lettres qui signifient au destinataire les artifices ayant servi au chiffrement.

Les fragments de texte d'un nombre de signes inférieur à la contenance d'une face de grille (1) sont cryptographiés comme les tronçons parfaits.

Exemple. — Soit à chiffrer le texte :

« Trouvez-vous demain à dix-huit heures à la station de Vielsalm. Vous y recevrez de nouvelles instructions et vous ferez connaître les renseignements recueillis sur l'esprit des populations. »

Supposons que le chiffreur suive les conventions suivantes:

1° Grille n° 5 ;

2° Disposition successive de haut en bas et de gauche à droite ;

3° Rotation de la grille en sens inverse ;

4° Relèvement parallèle aux côtés C D E (de haut en bas), en boustrophédon ;

6° Retournement de la grille: disposition suivant V Q R S T ; relèvement suivant T U V.

Clef littérale: Louvain (24 lettres) (voir précédemment).

(1) 108 lettres pour la grille cubique simple.

« Le chiffreur transmettra le chiffre ci-après : (1)

o v s jolcjm y a t xoc mqh *(udpzveg gdpzv veg)*

(5 5 5) (8 8 8) (7 7 7)

evdus — snivy — ferhu — avmdc — esool — unrul — leuic — icxst — moiiv — niras — etoee — snore — usdoa — atvzi — ttevz — tchne — lella — nezoe — erunr — daret — uisao — tvs — *(udpzv — eggdp — zvveg)* — iessa — eigdl — tstpr — tesul — snenr — eueiu — esslm — ncrei — snlpp — coero --»

Pour la *lecture*, on procède aux mêmes opérations, d'après les indications des signes de la clef, *si les tronçons sont parfaits*, sauf qu'on commence par répartir les lettres dans les cases de la figure tracée sur le papier. On y applique ensuite la grille, et l'on appelle les lettres dans l'ordre désigné par la clef : *c'est le texte clair*.

Lorsque le lecteur arrive au fragment final de la dépêche, il se sert de sa grille comme pour le chiffrement d'un pareil nombre de signes, mais au lieu d'inscrire les lettres, il marque simplement les cases d'une croix au crayon. Il enlève ensuite l'instrument et dispose la fraction de cryptogramme dans le sens voulu en inscrivant une lettre dans chacune des cases marquées.

Cette répartition effectuée, l'application de la grille sur la figure et sa rotation éventuelle permettent d'obtenir la traduction du texte.

L'ensemble de la méthode qui vient d'être décrite nous amène à conclure :

1° La grille cubique simple garantit le secret des cryptogrammes, même si les grilles venaient à tomber en des mains ennemies.

2° Outre la possession des grilles, le système n'exige des correspondants que l'usage de papier et de crayon.

(1) Dans une transmission réelle toutes les lettres se suivent naturellement, sans les distinctions que nous avons faites ici dans le simple but de faciliter la compréhension.

3° Le travail du chiffrement ou de la lecture est minime.

4° La perte d'une ou de toutes les grilles n'interdit pas la correspondance cryptographique. Si l'agent possède la formule de génération des grilles et la convention qui a présidé à la confection de celles-ci, il est aisé de reconstituer ces instruments en peu de temps : un bon canif apte à couper du carton mince suffit (1). A la rigueur, on peut découper les cases dans une simple feuille de papier.

5° Le système que nous proposons réalise au plus haut point les qualités pratiques requises pour l'emploi de la cryptographie en campagne, pour les relations réciproques entre les états-majors et entre ceux-ci et les officiers envoyés en mission.

6° L'indéchiffrabilité « *mathématique* » n'est pas obtenue par ce procédé, puisque, en supposant un jeu de grilles tombé aux mains de l'ennemi, celui-ci, par l'essai successif des différents genres de combinaisons, pourra par un heureux hasard, obtenir le déchiffrement d'une des dépêches interceptées. Nous pouvons assurer que ces tâtonnements seront, la plupart du temps, extrêmement longs. Dans tous les cas, le déchiffrement d'une dépêche ne simplifie en rien le travail du déchiffreur, pour la réduction d'autres dépêches, puisque, même sans changer le mot-clef, les correspondants *chiffrent chaque texte à volonté*, au gré de leur imagination pour ainsi dire, avec l'unique devoir de faire connaître en chiffres au destinataire la ou les grilles employées, le ou les modes de disposition et de relèvement.

7° Le changement de mot-clef se fait de la manière la plus aisée; il suffit d'insérer le nouveau mot dans le texte à transmettre, et de le cryptographier avec les autres parties du cryptogramme.

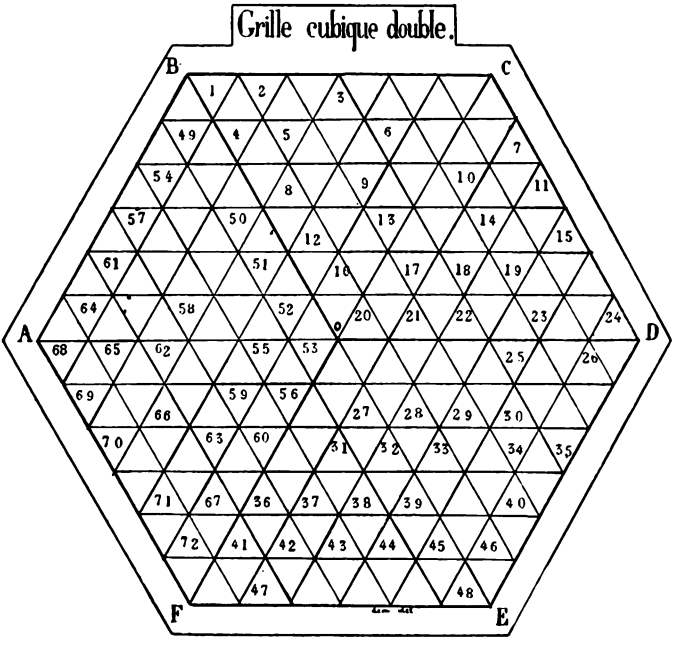
8° La faculté de chiffrer un nombre quelconque de signes,

(1) Le lecteur voudra bien se rappeler à cet effet que le côté de l'hexagone régulier est égal au rayon de la circonférence circonscrite.

d'employer des lettres nulles ou non, d'intercaler dans le texte toute espèce de convention, sans permettre au déchiffreur d'y trouver une base pour ses investigations, sont les propriétés les plus caractéristiques de notre méthode.

Remarque. Si au lieu de lettres, on se sert de nombres pour désigner les caractères d'un texte secret, les chiffres se prêtent à toutes les combinaisons qui ont été énumérées précédemment; mais le travail est plus long, les chances d'erreur dans les opérations augmentent, et les cryptogrammes obtenus donnent plus de prise au déchiffrement par l'obligation d'indiquer aussi en chiffres les conventions entre les correspondants. Il faut noter encore que la représentation des lettres par des nombres nécessite deux chiffres pour chaque lettre.

Figure D.



Grille cubique double. — Lorsque les communications consistent en des textes de grande étendue, il y a avantage, au triple point de vue de la simplicité, de la rapidité et de la dispersion, à faire usage de la grille représentée figure D ci-contre.

La *grille cubique double* est analogue à la cubique simple, mais les trois losanges comprennent chacun $12^2 = 144$ cases. Un seul de ces instruments permet, par conséquent, le chiffrement total de $2 \times 3 \times 12^2 = 864$ lettres.

Les règles d'emploi, les conventions à faire entre correspondants, sont en tous points semblables à celles décrites pour la grille congénère simple. La grille double se prête de plus à la disposition et au relèvement suivant les parallèles aux diagonales de l'hexagone, c'est-à-dire par bandes d'étendue variable.

On remarquera que les grilles pentagonales, hexagonales, heptagonales régulières, sont de vraies grilles cubiques, en ce que le nombre de cases de leurs faces, est toujours égal au cube (n^3) du chiffre figurant le nombre de côtés du polygone régulier qui leur sert de base; les grilles cubiques n'ont que la moitié du nombre de cases des grilles hexagonales régulières.

Les grilles polygonales régulières jouissent d'une grande partie des propriétés des grilles cubiques; mais le défaut de leurs cuirasses réside dans la trop grande régularité de répartition des ouvertures que crée le genre de rotation des secteurs autour du centre de figure.

Dispersion irrégulière.

Avant de terminer ce chapitre il nous reste à signaler deux règles de dispersion irrégulière des lettres par les jeux de cartes, qui tiennent beaucoup des stratagèmes antiques. L'idée en est empruntée à l'ouvrage (1) du Colonel Autrichien Fleissner von Wostrowitz.

(1) Handbuch der Kryptographie Wien 1881.

1° On range les cartes dans un ordre convenu; par exemple suivant le rang des lettres d'un membre de phrase. On inscrit une des lettres sur chacune des différentes cartes du jeu. On transpose ensuite le texte clair en dispersant ses lettres une à une ou par groupe, sur chacune des cartes correspondantes, dans l'ordre déterminé. On dérange le jeu et l'on expédie le paquet de cartes à son adresse.

Le maximum de précaution aura été pris, si les inscriptions ont été faites avec une encre sympathique. Si la dépêche doit être transmise par le télégraphe, on recueille les lettres par groupes de cinq, suivant l'ordre des cartes.

A la réception du cryptogramme, le correspondant, qui devra posséder un jeu de cartes analogue à celui de l'expéditeur, répartira les lettres d'après la convention, et procédera à la lecture.

Ce stratagème peut fournir de bons résultats si le secret des cartes est bien gardé.

2° Un artifice, qui rappelle celui de la scytale grecque, consiste à écrire un texte sur les faces latérales du parallélipipède rectangle, formé par un ou plusieurs jeux de cartes comprimés par une presse; l'ordre convenu des cartes est ensuite dérangé et le paquet est expédié au destinataire.

Ce dernier procédera aux opérations inverses et verra apparaître le texte sous la presse.

L'emploi de ce stratagème exige que la position des cartes soit déterminée clairement par les correspondants.

On peut conclure de ce qui précède que, saufles grilles cubiquepréconisées par nous, aucune méthode par transposition ou interversion des *caractères du texte clair*, ne peut offrir de sécurité vraie, puisque les lettres conservent leurs noms; le rétablissement des signes dans l'ordre clair pourra

toujours se faire, même sans la connaissance de la clef ou du système employé, rien que par la règle des fréquences et des séquences des lettres.

Ne perdons pas de vue, dans l'invention des méthodes de chiffrement, que la réduction des cryptogrammes se fait directement, sans que la connaissance de la clef soit nécessaire, sans que les déchiffreurs essaient même de la connaître *à priori*.

D'autre part, le nombre des combinaisons auxquelles peut se prêter un système, n'est pas un facteur de la résistance au déchiffrement; au contraire, presque toujours la découverte d'un de ces facteurs équivaut à celle de toute la série correspondante de signes qui en procèdent.

La difficulté, dès ce moment, est divisée par ce facteur, le nombre de combinaisons se réduisant aussi rapidement qu'il augmente. Au surplus, si exceptionnellement un cryptogramme très court, ne comprenant que quelques mots peut être facilement réduit, à cause du petit nombre de combinaisons qu'il comporte, un texte chiffré offre, en principe d'*autant moins* de résistance à la traduction qu'il est *plus long*. Ce principe se vérifiera d'une manière plus générale encore, pour les systèmes par *substitution* dont nous nous occuperons bientôt.

(A suivre.)

Le Lieutenant d'artillerie
adjoint d'état-major,
A. COLLON.

FIN DU TOME I.

Etude sur la Cryptographie

SON EMPLOI A LA GUERRE ET DANS LA DIPLOMATIE.

TABLE DES MATIÈRES

du tome I.
