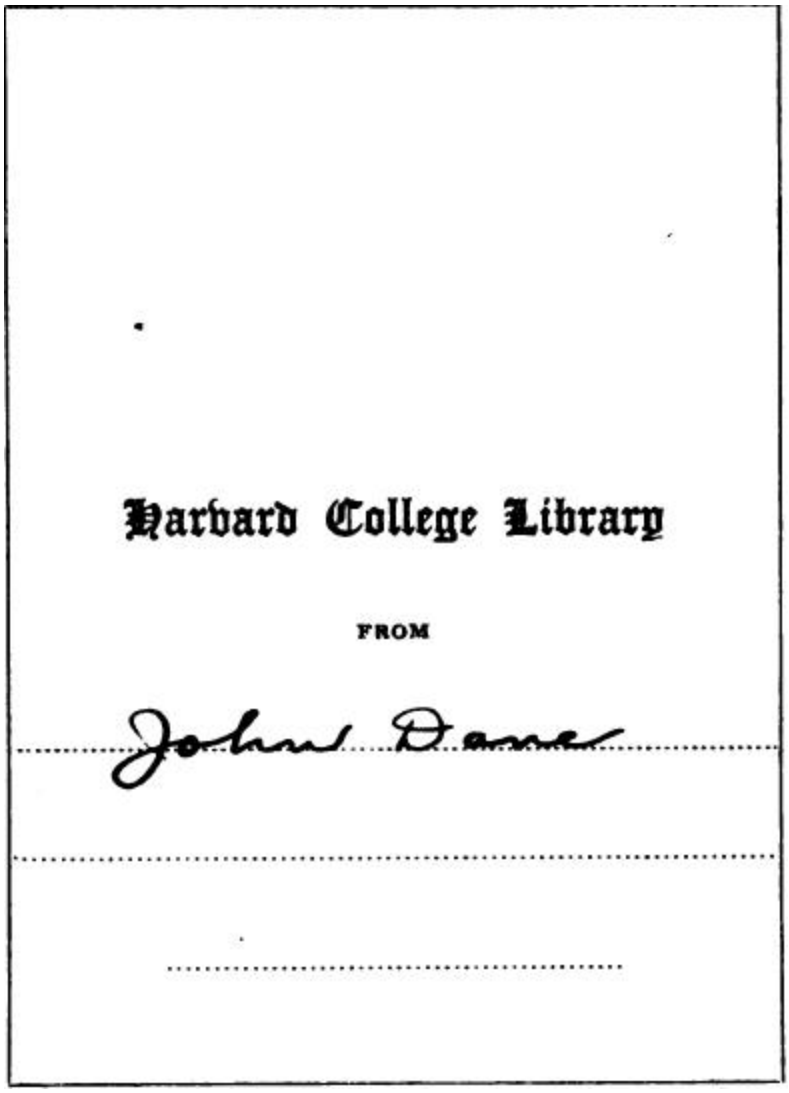

The text on this page is estimated to be only 3.00% accurate

t I

I t 1

The text on this page is estimated to be only 5.44% accurate

CRYPTOGRAPHIE MILITAIRE us iiitrais MiÉs iK nps di mm HoBTein pnww

The text on this page is estimated to be only 29.67% accurate

LA CRYPTOGRAPHIE MILITAIRE (Extrait du Journal des Sciences militaires.)

The text on this page is estimated to be only 9.22% accurate

CRYPTOGRAPHIE MILITAIRE DES mim mm m temps de enitEE Hontean procédé de décliiffrement applicable ani systèmes à donble cleC Ang. KKRCKHOFFS DucMnr es IsKrai Profeistnr h l'École des Hint«s ËlndeB canimerciilM et à l'École kriga Utmbn de la SocidM hioçniiui d'Archéologie et de Nunutmatiqae, de la SocléM d'Archéologie de Seina-et-Hanie , etc. Commuideiir de l'Ordre roilïlaire dn Chrisl, Officier d'académie. La cryfloj/ra^kie al un mailitàTe puùjonl PARIS LIBRAIRIE MILITAIRE DE L. BAUDOIN ET G* lIBRAIftlS-ÉDITEimS SUCCESSEUBS DB J. DUMAINE 80, Rne et PaasUBe D&nphine, 30 1883

The text on this page is estimated to be only 0.70% accurate

r^nà-y é c %7l^.. ^)«'^'. '"""^ •• • 'C

PRÉFACE Le goût des études cryptographiques semble se réveiller chez nous depuis quelques années : la Cryptographie est enseignée aujourd'hui dans nos écoles militaires, les revues populaires en exposent les éléments, et de nouveaux systèmes sont journellement proposés à l'examen du Ministre de la guerre. Si les efforts tentés de différents côtés pour doter notre armée d'un chiffre à la fois sûr et pratique sont dignes d'éloges et témoignent de préoccupations parfaitement justifiées, il n'en est pas moins vrai que, à une ou deux exceptions près, ils accusent chez leurs auteurs une connaissance très incomplète tant des travaux antérieurs que des différents procédés de déchiffrement. J'ai donc pensé que ce serait rendre service aux personnes qui s'intéressent à l'avenir de la Cryptographie militaire que de leur résumer les travaux déjà publiés sur la question, et de leur indiquer les principes qui doivent les guider dans la combinaison ou l'appréciation de tout chiffre destiné au service de la guerre. Le présent opuscule sera également utile aux officiers qui pourraient être appelés à appliquer, à un moment donné, une

VI PRÉFACE. méthode quelconque de correspondance cryptographique : car ce n'est qu'à la condition d'être initiés aux procédés des décbiffreurs qu'ils sauront éviter certaines imprudences qui compromettent la sûreté des meilleurs systèmes. AuG. Kkrckhoffs Paris, 1883.

■1 TABLE DES MATIÈRES I. La Cryptographie dans l*ariiéb 1 A. Notions historiques i B. État de la question 4 II. Desiderata de la Cryptographie uilitairb 8 III. Les différentes méthodes de Cryptographie 11 Â. Méthode par transposition 11 B. Méthode par interversion 16 i^ Systèmes à simple clef 16 2^ Déchiffrement des systèmes à simple clef 19 3« Systèmes à double clef 22 a. Système de Porta 23 6. Chiffre carré de Vigenère 25 c. Système de Saint-Cyr 27 d. Système de Bcaufort 30 e. Système de Gronsfeld 32 f. Système à clef variable 33 4® Déchiffrement des systi'^mes à double clef. 34 a. Nombre des alphabets 35 b. Ordonnance des alphabets • • . . 37 a\ Alphabets non intervertis 38 6'. Alphabets irrégulièrement intervertis.... 40 c'. Alphabets régulièrement intervertis. — Symétrie de position 46 d\ Alphabets indéterminés 48 c. Système à clef variable 52 5^ Un chiffre à triple clef 5«) C. Dictionnaires chiffrés 54 IV. Les Cryptoghapdfs 59

LA CRYPTOGRAPHIE MILITAIRE « La cryptographie est un auxiliaire puissant de la tactique militaire. » (Général Lbwal, Études de guet^re.) I. LA CRYPTOGRAPHIE DANS L'ARMÉE. A, Notions historiques. La Cryptographie ou l'Arf de chiffrer est une science vieille comme le monde ; confondue à son origine avec la télégraphie militaire, elle a été cultivée, dès la plus haute antiquité, par les Chinois, les Perses, les Carthaginois; elle a été enseignée dans les écoles tactiques de la Grèce, et tenue en haute estime par les plus illustres généraux romains'. Depuis la modeste scytale des Lacédémoniens et les trucs inventés ou rapportés par iEnéas le Tacticien*, jusqu'au fameux ^ C*est sous la rubrique : Stèganographie, chiffres ou écritures secrètes, que certains dictionuaires encyelopédiques donnent les renseignements qui se rapportent à la cryptographie. Les anciens auteurs rappellent plus ou moins Correctement : ars notarum, ars zypherarumy polygraphia, scotographia, cryplolO' ffia, steganologia, eryptomenylicesy etc. ; les Allemands disent aujourd'hui : Geheimschrift ou Chiffreschrift, et les Anglais : eryptography. * Lettres mises entre les semelles du messager, communications cachées dans un ulcère du porteur ou dans les pendants d'oreilles des femmes, dés percés de 24 trous à travers lesquels passe un fil, pigeons voyageurs, etc. iËneas (iv'^ siècle avant J. G.) est le plus ancien des auteurs militaires dont nous ayons des écrits ; le chap. xxxi de ses Commentaires sur la défense des places (traduits par le maréchal de camp Beausobre, 1757) est consacré aux lettres chiffrées et à la manière de les faire parvenir secrètement, Kerckhoffs. 1

? -, 2 — tonneau de Kessler *, les hommes de guerre ont imaginé bien des procédés pour transmettre au loin des ordres secrets, ou pour mettre leur instructions à Pabri des investigations et des surprises de l'ennemi. Nous ne possédons cependant que des renseignements fort incomplets sur les procédés cryptographiques proprement dits en usage chez les anciens ; en dehors des commentaires d'^Enéas, on ne rencontre, au sujet de la question qui nous occupe, que des passages isolés dans Polybe", Plutarque', Dion Cassius*, Suétone *, Aulu-Gelle *, Isidore '^ et Jules l'Africain \ Pendant le moyen âge, la cryptographie n'a guère été cultivée que par les moines et les cabalistes, et encore, là où elle a servi à un but pratique quelconque, les inventeurs ont-ils plutôt cherché à donner le change sur le sens des communications transmises, qu'à imaginer des méthodes de correspondance plus ou moins indéchiffrables; c'est qu'en ces temps d'ignorance ombrageuse, il était tout aussi dangereux de correspondre dans un langage mystérieux ou indéchiffrable, que d'écrire en clair les secrets les plus compromettants. Même au xvii® siècle, le simple fait d'avoir correspondu. en caractères secrets était encore considéré comme circonstance aggravante par les tribunaux anglais ;, ainsi dans le fameux procès intenté au comte de Sommerset, pour crime d'empoisonnement, le chancelier Bacon releva, comme une charge grave contre le noble accusé, son habitude d'écrire en chiffres à ses amis. i L'invention de Kessler, que le colonel Laussedat a rappelée dans une de ses conférences, se trouve exposée dans un petit livre devenu très rare, publié en 1616 à Oppenheim, et intitulé : Unterschiedene bisihero mehrem Theiîs iecreta oder Verborgene gefiehne Kûntle, ^ Histoire romaine, livre x, chap. 44-48. .8 Lys ANDRE, chap. i9. ^ Chap. XL, 9 ; chap. xli, 3. ^ César, chap. 56 ; Octave, chap. 88^. ^ Nuits at tiques f livre xviii, chap. 9. ^ Origines, i, 24. ^ Ge que Ton trouve dans le Cestes, ouvrage sur l'art militaire attribué à Jules l'Africain, et dont une traduction française a été donnée dans les Mé'=moires critiques et historiques de Guiscftardt, n'est guère autre chose qu^ane copie des Commentaires d'iEneas. — Philonde Bysance, l'auteur de la Polior-eétique, qui vécut au ii° siècle avant J. C, avait composé tout un traité sur V Envoi des lettres secrètes^ msiis cet OMvraige-^ été ^^erdu.

— 3 — C'était donc de Ibl siéganograpAie que pratiquaient nos pères, artificium sine secreli latentis suspidone scribendif plulôt que de la cryptographie^ dans le sens que nous attachons aujourd'hui à ce mot. On peut lire dans les œuvres du jésuite Schott * et dans un vieux traité de cryptographie du duc de Brunswick', les mille artifices qu'ils ont successive^ment inventés* Ce n'est qu'à partir de la Renaissance que la cryptographie devient un art véritable, ars occulte scribendt, comme on disait, et qu'elle acquiert une certaine importance dans les correspondances des princes avec leurs ambassadeurs, et dans les relations des grands seigneurs avec leurs affidés. On a vu, par ses lettres adressées au landgrave de Hesse, publiées il y a quelques années par de Rommal, que Henri IV aimait à se servir d'un chiffre pour sa correspondance intime. On sait également que Henri lY ayant fait intercepter quelques lettres chiffrées adressées par des membres de la Ligue au gouvernement espagnol, chargea le mathématicien Viète d'en trouver la clef. Celui-ci y réussit, et le roi put ainsi, pendant près de deux ans, surveiller les intrigues de ses ennemis. Sous Richelieu, Varl de déchiffrer les écritures sécrètes s'éleva presque à la hauteur d'une science d'Etat; au dire du maréchal de camp Beausobre% le ministre des affaires étrangères avait même une acaidémie où elle était enseignée ^ Soutenu par les largesses des gouvernants, encouragé par l'absence de probité politique qui caractérise les règnes suivants, l'art de déchiffrer a continué, jusqu'à la révolution de Juillet, d'être cultivé avec un égal succès par les espions de la cour et les hommes du cabinet noir. Je n'ai pu cependant trouver des traces bien nettes de l'emploi de. la correspondance cryptographique dans l'armée, au XVI® siècle ; mais on sait positivement que, dès le xvii® siècle, les ordres ne se transmettaient aux généraux commandant sur les frontières ou en pays ennemi j que par des chiffres \ 1 Gasparis ScHOTTi, Sckoltt steganographica^ 1665 ; classis viii. ' < GusTAVi Seleni^ Cryptomenyticet et eryptographiœ, iibri ix, 1624. ^ Voy. Commentaires sur là défense des places, p. 14S. Note du traducteuri * On trouve le précepte suivant dans le Breviarium Polilieorum du cî^rdinal Mazarin : Seribere tecreta manu tua ne graveriSy nisi per zifras seriba», * Cf. Bardin, Dictionnaire de V Armée de terre, 184ÎJ.

Dans les récits des guerres du premier Empire, il est souvent question de communications ci7ptographjques; les généraux avaient deux clefs pour correspondj:e avec eux et avec Tétatmajor général : le grand chiffre et le peiit ou chiffre banal. Le baron Fain, le secrétaire de Napoléon I«', rapporte que pendant la guerre de Russie TEmpereur entretenait des correspondances chiffrées ^ On sait également que, pendant la guerre d'Espagne, un Espagnol trouva moyen de dérober le chiffre de Suchet, et s'en servit pour faciliter à ses compatriotes là reprise de Mequi* nenza et de Lerida. Aujourd'hui la correspondance par chiffres secrets est adoptée dans toutes les armées de l'Europe; mais elle n'est encore appliquée d'une façon systématique que dans les bureaux des chancelleries. B. État de la question. Les Allemands posent en principe que la correspondance eryptographique doit être employée de la manière la plus étendue ; les programmes de leurs écoles militaires prescrivent non seulement d'exercer les officiers à la composition et à la lecture des dépêches secrètes, mais encore de les initier à la connaissance de tous les principes théoriques de l'art de déchiffrer. L'article 32 du règlement du 19 janvier 1874 porte également que les dépêches militaires doivent autant que possible être chiffrées. On pourrait donc s'étonner au premier abord que, à de rares exceptions près, l'usage de la correspondance chiffrée soit encore limité aujourd'hui, dans l'armée française, aux commandants en chef. Mais un système de cryptographie « d'un emploi facile et sûr est une lacune », dit le général Lewal, « qui a toujours existé dans notre armée' ». L'ancien commandant de l'Ecole supérieure de guerre ajoute, il est vrai, qu'il existe bien des pro^ Manuurit de 1812, contenant, le précis des événements de celte année, pour servir à Vhistoire de Napoléon, 1827. — Le colonel Fleissner (Handbueh der Kryptographie) lui attribue môme, mais à tort, l'invention d'un nouveau chiffre. • Tactique de marche, 1876.

— 8 — cédés à cet effet, et qu'il suffirait d'en adopter un « qui fût à la fois portatif et d*un usage à la portée de tous »; mais certaines déceptions, éprouvées par Tétat-major dans notre récente campagne de Tunisie, aussi bien que les méthodes enseignées et préconisées dans nos hautes écoles militaires, ne feraient-elles pas supposer qu'il existe une singulière analogie entre ce système facile et sûr et la pierre philosophale des anciens chimistes ? Nos meilleurs généraux sont bien d'avis, aujourd'hui, qu*il est indispensable que les différents commandants d'une armée aient à leur disposition un système de communications secrètes pour correspondre librement, non seulement entre eux et avec leur commandant en chef, mais encore avec leurs lieutenants; ainsi, le tacticien que je viens de citer pense qu'il faudrait pourvoir (Tun chiffre en temps de paix comme en temps de guerre^ les gêné" rauXy les chefs de régiment ou de service, tous les commandants de colonne et de poste. Il ajoute même, et avec raison, qu'il faudrait, durant la paix, exercer nos officiers au maniement de cette correspondance. « C'est une affaire à prévoir et à régler avant la guerre, dit-il; « une fois les opérations commencées il est trop tard pour y « songer. D'ailleurs, même en paix, on a besoin, et à chaque « instant, de correspondre secrètement. » On lit dans les Recherches historiques sur Vart militaire du général Bardin * 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 Feltreet Berthier expédièrent ses ordres; aussi, peu de dépêches parvinrent 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 de la cryplo« graphie! » Mais il ne sufiSt 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 Voy. Ta rticle GW/fre sléganographique.

: ~ 6 — imaginés jusqu'à ce jour, et là où ce défaut capital a été écarts, on se trouve en présence d'inconvénients pratiques tout aussi graves. Même au ministère de la guerre on ne s'est pas montré très beureux 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 èlre déchiffrée. Le Minisire, 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 crypto* gramme était traduit t Heureusement pour le secret de la corres* pondance, l'habile déchiffrenr était le fils du Ministre lui-même^ On a pu voir par les articles nécrologiques publiés en 1879 dans les journaux allemands, à l'occasion de la mort du capi*. taine 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 « auiiiliaire puissant de la tactique militaire », 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 déchiffrenr 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; il est également permis de croire que les affirmations peu mesurées de certains auteurs, non i Le capitaine Henri Berthaut, auquel je fais allusion, est certainement un des plus habiles déchiffreurs de Tétat-major.

 moins que Tabsence complète de tout travail sérieux sur Tari de déchiffrer les écritures secrètes, ont largement contribué 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 * que les chiffres à base variable sont ilUbibles y on du moins qu'on n'arrive h 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 Tépoque où l'art dç 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 * ». Dans la préface du Contr^espion, ^ où « le citoyen » Dlandol faisait connaître, en 1793, les clefs de quelques chiffres dont se servaient les royalistes dans leurs correspondances aveie les émigrés, il est dit que « ce n'était pas un des moindres services à « rendre à la patrie dans les circonstances d'alors qjie d'anéantir « par la publicité l'arme la plus dangereuse des ennemis secrets « de la République ». Je crois, à mon tour, ne pas faire acte de mauvais citoyen en mettant au grand jour un état de choses qui, pour relever d'un ordre d'idées différent, n'en est pas moins identique au fond, et dont nos ennemis du dehors ne pourraient ui^ jour que trop bien et trop aisément tirer parti. D^ns les pages qui suivent,.j'examinerai d'abord les desiderata de tout système de cryptographie militaire ; puis je dirai quel

 Il faut bien distinguer entre un système d^écriture chiffrée, imaginé pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux. Ceux-ci, en effet, ne peuvent, à leurgré et à un moment donné, modifier leurs conventions ; de plus, ils ne doivent jamais garder sur eux aucun objet ou écrit qui soitde nature à éclairer l'ennemi sur le sens des dépêches secrètes qui pourraient tomber entre ses mains. Un grand nombre de combinaisons ingénieuses peuvent répondre au but qu'on veut atteindre dans le premier cas; dans le second, il faut un système remplissant certaines conditions exceptionnelles, conditions que je résumerai sous les six chefs suivants : lo Le système doit être matériellement, sinon mathématiquement, indéchiffrable; 20 II faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ; 30 La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ; 40 II faut qu'il soit applicable à la correspondance télégraphique; 50 II faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes; 60 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. Tout le monde est d'accord pour admettre la raison d'être des sonnes qni voudraient approfondir la question ; ils leur seroQt d'autant plus utiles que, à deux ou trois exceptions prés, les ouvrages cités se trouvent tous à la Bibliothèque nationale. 'jSB

 trois derniers desiderata ; on ne Test plus, lorsque! s'agit des (rois premiers. C'est ainsi que des personnes autorisées soutiennent que Tindéchiffrabilité absolue du chiffre ne saurait être considérée comme une condition sine quâ non de son admission dans le service de l'armée; que les instructions chiffrées transmises en temps de guerre n'ont qu'une importance momentanée, et n'exigent guère le secret au delà des trois ou quatre heures qui suivent le moment où elles ont été données ; qu'il importe donc peu que le sens d'une dépêche secrète soit connu de l'ennemi quelques heures après son interception ; qu'il suffit, en un mot, que le système soit combiné de telle façon que la traduction d'un cryptogramme exige au moins trois à quatre heures de travail. On ajoute que la possibilité de pouvoir changer de clef à volonté ôte d'ailleuris au défaut de non-indéchiffrabilité toute son importance. Cette argumentation peut, au premier abord, paraître assez juste; au fond, je la crois fausse. C'est en effet, selon moi, oublier que le secret des communications envoyées à distance conserve très souvent son importance au delà de la journée où elles ont été transmises ; sans énumérer toutes les éventualités qui peuvent se présenter, il me suffira de citer le cas où le commandant d'une ville assiégée envoie des renseignements à l'armée qui doit la secourir. De plus, une fois qu'un cryptogramme intercepté a pu être déchiffré, toute nouvelle dépêche, écrite avec la même clef et qui subit le même sort, peut être lue instantanément. Il arrivera par suite que, pendant un temps plus ou moins long» des dépêches seront expédiées dans toutes les directions, dont le déchiffrement se trouvera en quelque sorte fait d'avance : à moins d'admettre que dans un corps d'armée toutes les instructions chiffrées émanent d'un seul ou du moins passent par leâ mains d'un seul, ce qui serait réduire la correspondance secrète à un rôle singulièrement modeste. La faculté de pouvoir changer de clef à volonté est certainement une condition essentielle de tout système de cryptographie, mais c'est un avantage trompeur et sur la réalisation pratique duquel on aurait tort de compter, à travers les mille péripéties d'une longue campagne. Quant à la nécessité du secret, qui, à mes yeux, constitue le

T - 10 — principal défaut de tous nos systèmes de cryptographie, je ferai observer qu'elle restreint en quelque sorte l'emploi de la correspondance chiffrée aux seuls commandants en chef. Et ici j'entends par secret, non la clef proprement dite, mais ce qui constitue la partie matérielle du système; tableaux, dictionnaires ou appareils mécaniques quelconques qui doivent en permettre Tapplication. En effet, il n'est pas nécessaire de se créer des fan» tomes imaginaires et de mettre en suspicion l'incorruptibilité des employés ou agents subalternes, pour comprendre que, si un système exigeant le secret se trouvait entre les mains d'un trop grand nombre d'individus, il pourrait être compromis à chaque engagement auquel l'un ou l'autre d'entre eux prendrait part. Rien qu'à ce point de vue il y aurait lieu de condamner l'emploi du dictionnaire chiffré, qui est en usage aujourd'hui dans l'armée. On m'objectera peut-être qu'en admettant le deuxième desideratum, il n'est guère possible d'établir un système complètement indéchiffrable. Il faut s'entendre : je sais très bien que vouloir dans ces conditions trouver un système mathématiquement indéchiffrable est chose mathématiquement impossible, mais j'affirme, et non sans de bonnes raisons, que, tout en réalisant les différents desiderata que j'ai énumérés plus haut, on peut parfaitement combiner des systèmes, sinon mathématiquement, du moins matériellement indéchiffrables. ■ Il paraît qu'il est sérieusement question, au ministère de la guerre, de remplacer le dictionnaire chiffré par quelque autre système plus pratique. Eh bien I si l'Administration veut mettre à profit tous les services que peut rendre un système de correspondance cryptographique bien combiné, elle doit absolument renoncer aux méthodes secrètes et établir en principe qu'elle n'acceptera qu'un procédé qui puisse être enseigné au grand jour dans nos écoles militaires, que nos élèves seront libres de communiquer à qui leur plaira, et que nos voisins pourront même copier et adopter, si cela leur convient. Je dirai plus : ce ne sera que lorsque nos officiers auront étudié les principes de la cryptographie et appris Part de déchiffrer, qu'ils seront en état d'éviter les nombreuses bévues qui compromettent la clef des meilleurs chiffres, et auxquelles sont nécessairement exposés tous les profanes; alors seulement cet article du règlement du

— n — ^ 19 novembre 1874, que j'ai mentionné plus haut, pourra rexîevoir une application pratique et réellement satisfaisante, m. LES DIFFÉRENTES MÉTHODES DE CRYPTOGRAPHIE. On peut rapporter les différents systèmes d'écriture secrète à trois méthodes principales : 1<> La méthode qui se borne à une simple transposition des lettres du texte en clair ; 2o Celle qui fait reposer la combinaison du chiffre sur une interversion de Tordre alphabétique des lettres ; 30 Celle qui représente les syllabes, les mots, ou même des phrases entières par des nombres ou des groupes de lettres*. A. Méthode par transposition. Les systèmes qui reposent sur une transposition des lettres : sont très anciens; ils permettent des variations nombreuses et ont servi de base à quelques appareils mécaniques, tels que les grilles^ qui jouissent encore aujourd'hui de la faveur du public*. Voici un exemple de transposition. élémentaire : les lettres de la dépêche ont d'abord été transcrites dans leur ordre naturel sur un certain nombre de lignes d'un nombre déterminé de camctères, puis on les a recopiées dans un ordre convenu ' ; c'est 1q nombre représentant la seconde disposition qui constitue 1^ clef du chiffre*. 1 Je me propose de publier bieQt6t un trarail complet sur les différents systèmes de cryptographie ; j'y rendrai volontiers compte de toute nouvelle combinaison qu'on voudra bien me communiquer, pourvu qu'elle ait quelque valeur au point de vue pratique. ^ Voy. Kluber^ Kryptographik, chap. xiu. Du Moncel, Exposé des appHca' lions de Vélectrieité, III, p. 530. 9 Gomme la somme des lettres du texte en clair doit former un multiple da nombre des colonnes horizontales, on ajoute, s'U y a lien, le nombrf de nullet nécessaire pour remplir la colonne finale ; il en faudra cinq ici. * Un appareil imaginé par un architecte de Paris, M. Rondepierre, et auquel eéluirci a donné ie nom de Phyrographe, est construit sur ce principe.

The text on this page is estimated to be only 27.45% accurate

- 12 — Une attaque simulée aura lieu demain matin à quatre hewret. A 1 2 3 k 5 6 1 8 9 10 11 1 u "n e a 1 t a 9 ti e s 2 • 1 TTl n 1 e e a u r a 1 3 • 1 "e u d e m a • 1 ■n m a \ l « 1 n a q XI a l r e 11 5 e u p e d a 1> c d e f B 2 n 9 8 5 3 10 1 3 6 ^ 1 n s u q t e e ti a l a 2 m 1 r u e XL a • 1 a e 1 3 e a n 1 e u m • 1 a m d !> • 1 h r t q Tl e . t a u a b 11 f d e a r e e h a e = nsuqteeuatamlrueuaiaeleanieumiaindihrt qnetauaufdcsreebae Une fois que le déchiffreur se doute du procédé qui a été adopté, et c'est ce qu'il voit tout de suite à la lettre E, qui en ce cas revient le plus souvent, le déchiffrement n'est plus qu'une affaire de tâtonnement. Il suffit de compter au préalable le nombre des lettres du cryptogramme et de les décomposer en deux facteurs (55 = 5x11); l'un représentera le nombre des lignes horizontales et l'autre celui des colonnes verticales. Rien que la présence d'un q ou d'un x, le premier étant toujours suivi et Tautre étant généralement précédé d'un u, trahit le secret de la clef. A l'occasion des derniers procès intentés aux nihilistes, les journaux russes ont fait connaître le chiffre secret adopté parles accusés : c'est un système de transposition double ; les lettres^ après avoir été une première fois transposées par colonnes verticales, le sont une seconde fois dans le sens des colonnes hori,,j

The text on this page is estimated to be only 28.71% accurate

— 13 — zontales. Le même mol sert de clef pour les deux transpositions*; à cet effet, on le transforme en formule numérique, en mettant à la place de chaque lettre un chififre arabe, et en s'y prenant de telle façon que la valeur des chiffres corresponde au rang des lettres dans le classement alphabétique *. Voici le procédé appliqué au mot Schuvalow : achlosuvw_ schuvalow 12 3 4 56 7 8 9"" 623 781459 S'il s'agissait maintenant de transposer une phrase, comme celle-ci : Vous êtes invité à vous trouver ce soir, à onze heures précises^ au local habituel de nos réunions, on procéderait d'abord comme dans le cas précédent, puis on reprendrait la même opération pour les lignes horizontales. A 1 2 3 5 6 7 8 9 1234»S6789 V o u s e i e s * 1 n V • 1 t e a V o u s t V 0 •Q V e p c e • s 0 • 1 r a o n z e h e u V e. s P V e c • 1 s e s a u l o c a 1 h a h • 1 t u e 1 d e n o s p exinaonsxx * c'est une faute 1res grave de la part de celai qai a imaginé le système, ' Je suppose que si la même lettre se trouve répétée, on compte les répëtitions comme autant de lettres se suivant alphabétiquement. Par exemple : Ta g an rog = aaggnort s 81325 76 4. 12345678

The text on this page is estimated to be only 27.19% accurate

- 1* — B 6 2 3tJ814 6 9 6 .9 c • Q u e s e 1 2 Û V m 1 V o n t e 11 3 V t V e V s o u c 5 a c a h * 1 o 1 h t d n 0 1 o s XI d e 1» 1 i 0 XI e s V s e • 1 ^ a S o o n e • p z b e h e s P e 11 V r 9 n M n s X e i o X = sciaueselavivonteuvtrersoucacabiolhtnelosuder^ etc. Quelque compliquée que celle transposition puisse nous paraître, le déchiffrement d'un cryptogramme, écrit d'après ce système, ne saurait jamais présenter de difficultés insurmontables dans les langues où certaines lettres ne peuvent se présenter que dans dès combinaisons déterminées, telles que le q ou le 07 français. Aussi les déchiffreurs russes paraissent-ils avoir mené leur besogne à bonne fin dans un temps relativement court. Si l'on adopte un système plus compliqué, il cesse d'être pratique sans devenir pour cela beaucoup plus difficile à déchiffrer. J'ai dit que la grille * repose sur le principe de la transposition ' des lettres; c'est un procédé ingénieux, fort usité au siècle dernier, et que les perfectionnements récents introduits par le colonel autrichien Fleissner paraissent avoir rendu indéchiffrable *. La figure ci-après représente un ancien modèle : c'est une plaque métallique carrée, h 36 divisions, dont les 9 cases numérotées sont découpées à jour. ^ ^ Ce procédé parait avoir été inyenié, au xvi^ siècle, parle mathématicien italien Jérôme Cardan. Voir son livre De tubiUilaU, traduit en français pat Richard Leblanc, De la tubtitité et tubtiles inventions» Par^, 15^6. : — Voir également de Prasse. De Retieults cryptographicii, Leipzig, 1799. * Handbueh der Krypiographie, von Fleissner von Wostrowitz ; Wien, 1 88 1 . 'M

The text on this page is estimated to be only 28.52% accurate

-^ 15 -^ Supposons qu'on veuille écrire la phrase citée en premier lieu, moins les trois derniers mots : on place la plaque sur une feuille de papier, après y avoir préalablement tracé un carré de même dimension, et Ton écrit, aux endroits laissés ouverts, les 9 pre^ A B 0 1 2 3 C ti^ 5 6 7 8 ■ 9 mières lettres de la dépêche ; on fait tournei* ensuite Tinstrument de droite à gauche, de manière que le côté BG prentie la placé du côté AB ; on inscrit les 9 lettres qui suivent, et l'on retourne de nouveau la plaque pour continuer la même opération jusqu'à la 36

— 16 B, Méthode par interversion. Dans les systèmes qui se rapportent à la méthode par inierversion^ il faut distinguer ceux h base invariable, c'est-à-dire où chaque lettre de Talphabet est, dans le courant du même cryptogramme, représenté par le même caractère ou le même signe, et ceux à base variable, où Ton change d'alphabet à chaque mot ou à chaque lettre. On appelle communément les premiers systèmes à simple clef, et les seconds systèmes à double clef. Les systèmes à simple clef ne présentent aucune sécurité ; les systèmes à double clef comportent seuls des combinaisons plus ou moins indéchiffrables. 1« Systèmes à simple clef. Au point de vue de la forme, les systèmes à simple clef peuvent être variés à TinlSni; on peut non seulement combiner Talphabel normal d'un nombre en quelque sorte incalculable de manières différentes, mais on peut encore remplacer les caractères alphabétiques par des nombres, des signes algébriques, astronomiques ou de fantaisie, ou encore par des groupes de lettres ou de chiffres, et même par des mots ou des phrases entières. Au fond cependant, et pour le déchiffreur, toutes ces combinaisons ne constituent qu'un seul et même système tombant sous l'application d*un même procédé de déchiffrement. Le système à la fois le plus simple et le plus pratique est celui qui consiste à changer la valeur des lettres de l'alphabet d'après une clef convenue. Nous avons vu, plus haut, comment on transforme un mot de clef en un nombre de clef ; on peut adopter le même procédé pour établir l'ordre de succession des lettres du nouvel alphabet. Soit Champigny la clef; la formule numérique y correspondant est 241685379. Si nous voulions ordonner l'alphabet cryplographique d'après ce nombre, nous obtiendrions : 24i 1685329 l)dafliecg*i Timjoqnlpr t V SX. z\vuv

— n — AB CD ET OH IJKLMTJ 0 P 0 R S TUVWXY Z bdafliec g*il£:injo

The text on this page is estimated to be only 20.82% accurate

— 18 — 89995S450 44520 4556^3652 llâSO si ce n'est la 31S2891499 14 254452 44520 2311094259467524594995645 44118934 5294. 445234114544520. 89 99 S2 ikS 0 4 ^-^ 52 3 4* 11 4>5 4^ 52 0 ension darmes demande = Rien de nouveau, si ce rCest la certitude de la suspension alarmes demandée. Je ne puis énumérer ici tous les systèmes à simple clef; je dois me 'borner à citer parmi les anciens auteurs les noms de Ti'ilheim*, Porta», Biaise de Vigenère', Bacon*, Hermann^et Wirabeau*, qui ont imaginé des alphabets plus ou moins ingéi Polygraphiœ Hbri VI; composés, d'après la préface, en 1508. Il «n a été fait une traduction par Gabriel de CuUange : La Pulygraphie et mUoentUe ticriture eabolitlique de Jean Triihème; Paris, 1561. Plusieurs ouvrages de cryptographie ou de st(^ganographîe ont été publiés sous le nom de l'abbé Tritheim (1462-1516), sans qu*on puisse savoir au juste ce qui s'y trouve de lui (Gf Schott, Schola tteganographiea, vu). Je ne crois pas qu'on doive lui attribuer autre chose que l'invention d'un système d'écriture secrète, où les lettres sont remplacées par des mots choisis de mani

The text on this page is estimated to be only 28.26% accurate

— 19 — fiieuK, dont on peut trouver la descriptibû dâiis les traités spé* ciaux^ D'ailleurs, ces inventions ne peuvent avoir pour nous qu'ua intérêt purement archéologique ; elles ne sont pas pratiques, et se déchiffrent toutes, celle de Hermann exceptée, avec aine égale facilité. 2® Déchiffrement des systèmes à simple clef. Quel que soit le système adopté, qu'il soit à base invariable ou à base variable, le déchiffrement d'un cryptogramme dont on n*a pas la clef comporte deux Opérations bien distinctes : un calcul de probabilité et un travail de tâtonnement. Le calcul de probabilité repose sur une particularité propre à toutes les langues^ à savoir que certaines lettres reviennent plus souvent que d'autres, et que le rapport de ces répétitions est •exprimé par une moyenne assez constante pour les 9 à 12 principales lettres de Talphabet. Ainsi dans les langues française, anglaise et allemande, c'est la lettre E qui est le plus fréquemment répétée; en espagnol c'est l'O, en russe TA et en italien E et I; en français, il y a en moyenne un E sur cinq lettres. Ainsi, si on avait à cryptographier * une dépèche avec l'alphabet ci-dessous établi sur la clef Orléans, on saurait d'avance que c'est le chiffre A qui doit revenir le plus souvent. AECDEFGHI JKLIVINOP pRS TUVWXTZ e fc*b a dg'lmj iLlcD s tg^porxizxwvy Votre dépèche a été déchiffrée donnera, en effet, nn cryptogramme où, sur 26 chiffres, le A est répété 9 fois : ZSRPA BATACLA E ARA 3AGLMDDPAA i Outre les auteurs déjà cités, on peut encore consulter : Hanbdi, Stêganologiaettlenographianom (texte allemand) ; Nuremberg, i6i^. Seleni, Cryptomeny lices et cryptograghiœ iibri ik; 1624. Frbdbrici, Cryplogtaphia otierGeheime eorrêtpondentz 'y Leipzig, *1685. L'article Cypher, dans VEneyelopœdii de Rees, 1819, et l'article Cryph^. ^raphy dans VEneychpœdia Britannica, 1877. Lacroix, La Cryptographie, ou VAri d'écrire en chiffrée, Paris, 18S8. s Comme nous avons déjà les termes cryptographie, cryptographique^ cryp^ iogramme eteryptographe^ il doit être permis de compléter la série des compo^s par Tadpption du verbe cryptographier.

— ÎO — Un calcul que j'ai fait sur quelques circulaires du Ministre cl

— 21 — Comme mon but n'est pas tant d'apprendre au lecteur à déchiffrer que de lui indiquer la marche suivie par les déchiffreurs, je me contenterai de lui montrer par un exemple des plus élémentaires comment on procède pour le déchiffrement d'un texte dont on n'a pas la clef. Soit le cryptogramme : SP Z BOB CSRRSQSPB CB PSXB JBJ PBOOXBJ. J_^ 2^_3 4 ^ 6 J7_ 8 SP Z BOB CSRRSQSPB CB PSXB JBJ PBOOXBJ Le caractère qui se rencontre le plus souvent est b; je dis qu'il doit correspondre à la lettre E, et je fais le raisonnement suivant : N<> 3. BOB : en fait de trigrammes commençant et finissant par un e, il n'y a que été. N® 2. Z : la langue française n'a que deux monogrammes, a et y; été ne peut être précédé de y, donc Z = û. No 7. JBJ : ce groupe ne peut être que ses; c'est le seul trigramme ayant un e au milieu, précédé et suivi de la même lettre. N** 8. PBOOXBJ : nous connaissons déjà cinq lettres de ce groupe, .ett.es; le seul mot qui réponde à cette disposition est lettres, N<> 1. SP : les seuls bigrammes qui peuvent aller avec a été sont ça, il, on; or P est un /, donc SP = î7. No6. PSXB = /îre. Gravezande, Introduction à la philosophie \ Loyde, 1737, chap. xxxv. Ce chapitre a été souvent reproduit, et se trouve, entre autres, dans le Dictionnaire encyclopédiqite de Diderot et dans la Cryptographie de Lacroix. Breithàupt, Ars deeifratoria sive occultas scripiuras solvendi et legendi feient%a\ Helmstadt, 1737. John Davys, AnEssay on theart of decyphering ; 1737. Conrad, Cryptographia denudata, sive ars deciferandi ; Leyde, 1739. Thigkenesse, a treatise on Ihe art of decyphering ; 1772. KhVBEti f Kryptographik; Tubingue, 1809. Vesin de Romanini, La Cryptographie dévoilée ; Paris, 1857. # Kasiski, Die Geheimsehriften und die Deehiffrirkunst ; Berlin, 1863. Fleissner von Wostrowitz, Handbuch der Kryptographie; Vienne, 1881. On peut aussi lire avec fruit le chap. xv du Scarabée d*or, les Ecritures se» crêtes dévoilées, de Charles Joliet, ainsi qu'un excellent article de Prodhomme, dans le Dictionnaire des connaissances humaines de Lunel. -'^^ ^- ^ - - * '

— 23- — Bien des combinaisons à base variable ont été imagiaéesymàis il n'y en a guère que trois ou quatre qm soient réellement prar tiques et qui soient encore eu honneur de nos jours; quoique différentes pour la forme, elles sont identiques au fond, et reviennent au système exposé à la Sn dn xyi* siècle par Biaise de Vigenère. Pendant près de trois siècles elles ont servi de chiffre secret à la plupart des petites cours d'Allemagne et d'Italie, et aujourd'hui encore elles passent pour indéchiffrables aux yeux des personnes qui ne sont pas au courant des procédés de déchiffrement. Comme toute méthode d'écriture cryptographique destinée aux besoins de Tarmée doit pouvoir être appliquée à la télégraphie, nous n'avons à nous préoccuper que des systèmes qui sont uniquement basés sur l'emploi des lettres ou des chiffres arabes et cela avec exclusion de toute combinaison exigeant l'emploi simultané des deux ^ a. Syatèxxie de PortaL'invention du premier système littéral^ à double clef remonte, comme je l'ai dit plus haut, au physicien Porta •; quoique luimême ait été bi&n loin de sentir toute l'importance de l'introduction d'une clef proprement dite dans la méthode des écritures chiffrées, nous n'en devons pas moins le considérer comme le fondateur de la cryptographie. Porta emploie onze alphabets différents, qu'il désigne, comme on le voit dans la figure ci-après, par lesi lettres. AB,, CC,, etc., ou tout simplement par A, C, ou B,. D. * U y a toute probabililé que le Jlioistre des postes et télégraphes ne tardera pas à appUquer au service intérieur les principes de la convention internationale de Londres, aux termes de laquelle Temploi simultané des lettres et des chiffres est exdu du langage secret. Une considération plus importante, c'est qu'il est presque impo sible d'éviter les erreurs dans la transmission par voie télégraphique des dépêches chiffrées, si on n'a pas soin de les découper par petits groupes fixes de 3 à 5 lettres ; or, le fonctionnement de l'appareil Hughes s'oppose au fraclionnement régulier des dépêches, dans le cas de l'emploi simultané des chifi^es arabes et des lettres. « Je dis lUléral, c'est-à-dire basé sur l'emploi des lettres, parce que Tritheim avait déjà songé, cinquante ans auparavant, à employer des série» de mots et de phrases pour correspondre aux lettres du texte en clair. 9 De furliois HUerai-um notis, lib. ii, cap. 16.

The text on this page is estimated to be only 19.05% accurate

Veul-OD écrire avec l'un oit l'autre de ces alphabets, on choisîl, pour représenter les lettres du leste en clair, celles qui, dans le tableau, leor font face. Ainsi, si l'on cryptographie avec l'alphabet D ou G, on représente a par z, et vice verad i par a; b par n et n par b, et ainsi de suite. Mais pour dérouter les calculs des investigateurs. Porta, en homme qui sait déiihiffrer, recommande d'écrire chaque lettre avec un alphabet différent; de plus, pour ne pas obliger les correspondants à prendre les onze alphabets \ la suite, ce qui aurait bien vite trahi le secret, il propose de n'en adopter que quatre, cinq ou six, et de convenir d'un mot dont les différentes lettres indiqueront le^; alphabets qu'il faudra successivement choisir'. Ce mot constitue la clef du cryptogramme; on l'écrit sous le leile k chiffrer, et on le répète le nombre de fois nécessaire. Voici un exemple avec la clef roi : 1 U, Fleissner altribne l'iavealion de c« syslèmo à Nipolëon 1"; ce n'est pas la seule erreur historique ou b bliograpbiqne qu'il y ait à reprocher à l'ëcriTBÎD autrichien.

2o — vol r e d e p e c 11 e est d e c Il if £ V € e no I ROI RO I R 0 I R 0 I RO I ROI ROI R d hm ay z X i n ton X am V J ^ n p o JTOB X = dhmayzxintonxamvyynpoymnx L'invention de Porta, avons-nous vu, ouvre, en quelque sorte, une nouvelle ère dans Thistoire de la cryptographie, mais elle présente deux grands inconvénients, qui l'ont fait abandonner depuis longtemps : d'abord le petit nombre de ses alphabets et ensuite la nécessité de représenter le même alphabet par deux lettres différentes. Par suite de cette dernière circonstance, un mot de quatre leltres, comme poli, donne une clef qui ne comporte en réalité que deux alphabets. 6. Cb.ifi*re carré ou tableau, de Visenère. Le chiffre carré, aussi nommé le chiffre indéchiffrable ou chiffre par excellence, n'est autre chose que le syslème de Porta, simplifié par Biaise de Vigenère, qui l'a exposé, tel qu'il est encore en usage aujourd'hui, dans son Traité des Chiffres *. Le chiffre carré a joui d'un crédit extraordinaire auprès des chancelleries du xviii« siècle, et, ce qui pourrait porter à croire qu'on n'a guère trouvé mieux depuis, c'est qu'on s'en est encore servi, après 1870, au ministère de la guerre. Dlandol l'a fait connaître au public, à l'époque de la Révolution, dans un opuscule que j'ai déjà cité. Au chap. vi, il dit que « ce « chiffre a été nommé le chiffre par excellence» parce qu'il réunit « le plus grand nombre d'avantages que l'on puisse désirer pour « une correspondance secrète, il les réuniroit tous sans aucune « exception », ajoule-t-il, « s'il n'étoit pas d'une exécution un c(peu lente; mais il rachète bien cet inconvénient par la sûreté « incroyable dont il est. Cette sûreté est telle que l'univers entier « ne le connoitroit, si on ne savoit pas le mot de clef convenu a entre les correspondants, on pourroit montrer sa lettre à tout « le monde, sans que personne pût la lire. » Certes le citoyen Dlandol était meilleur patriote qu'habile déchiffreur 1 ^ Voy. p. 50, b.

The text on this page is estimated to be only 12.06% accurate

- 26La disposilion du tableau de Vigenëre diffère de celle du tableau de Porta, en ce que l'alphabet y est mis ea wniVe carré, et qu'où obtient ainsi autant d'alphabets différeaLi qu'il y a de lettres dans l'alphabet t. Quant au maniement de ce tableau, on procède comme pour le système de Porta; il faut seulement remarquer que l'alphabet horizontal supérieur représente l'alphabet normal, et que les 26 autres qui suivent sont les alphabets cryptographiques. i Lt P-^re Kîrr.her (Polygraphia nova tt unttunalli; Rome, 14S3} a remplacé les Ictlrea du lableBu de Vigeoàre par des nombreJ, d'où le nom d'Abaau numeraiii d >iuië à soD ijsifme. Sealement. au liea d'écrire Le texte cryptograpliique de la façon ordinaire, Kircher prend une page d'écrilure quelconque, et indique les Dombnts du cryptogramme par des points placéi sous les leltres. & des inlervatled correspondaDt à la valeur des nombres obt 'Dos. Schatt a cominentË le système du Père Kircberdans sa Sckola ilenograiihîea; de li que beaucoup d'aotears, Larousse entre autres, lui en ont attribué la paternité.

The text on this page is estimated to be only 27.03% accurate

— 27 — Soil h cryptographier Détruisez le tunnel avec les Irais alphabets correspondant au mot BAC; on au^a : d e t BAC e e V r n 1 BAC s ^x'k s e z BAC t el) 1 e t BA C tm e V Ti n Ti BAC V n p c 1 B A f 1 = eevsuktebmevvnpfl. Rien n'est plus facile que de lire un cryptogramme écrit dans ces conditions, lorsqu'on en connaît la clef: on transcrit le texte chiffré par tranches égales au nombre des alphabets choisis, on écrit en-dessous la clef, et Ton fait l'inverse de la première opération. Soit donné à déchiffrer eyfdaolrakhhgmhncfmk. Tunis étant la clef, on trouvera : ey f da o 1 r a 11 h 11 ^mli n c f mk TUW 1 S TUN 1 S TUlï I S TTJar I S 1 e s V i V r « a s o B 1 e p XL i s e s = Les mures sont épuisés. Ainsi que nous le verrons plus loin, les dépêches écrites avec le tableau de Vigenère se déchiffrent très facilement; ce n'est que dans des cas exceptionnels que le système peut présenter quelque sécurité. c. Système de Saint-Cyr. Ce système, qui est en usage depuis longtemps, n'est autre chose qu'une forme déguisée du tableau de Vigenère; faute d'une dénomination propre, je Tai désigné sous le nom de l'école où il est enseigné et préconisé aujourd'hui. En voici la description; elle est prise dans le Cours d'Art militaire de l'année 1880-1881, tel qu'il a été autographié pour les élèves de la 1'® division * ; « L'instrument, y est-il dit, se compose d'un alphabet fixe, i On trouve également une description de ce système dans Bartels, M'faden fur den Unierricht auf denkôniglichen Krieguchulen; Berlin, 1881.

— 28 — sous lequel glisse un double alphabet mobile; deuK bandes de papier quadrillé y suffisent *• E T^ B J) £ H RL TK M n Tî 0 m 3L 8 XI u vlw[x w|x|y YfZ z a etc. « On prend un mol quelconque de 3 à 5 lettres, pour former la clef*. Adoptons le mot BAC et prenons la dépêche suivante * Détruisez le tunnel, « La clef ayant 3 lettres, on partage également la phrase à chiffrer en groupes de 3 lettres, comme il suit : dét — rui — sez — let — unn — el; on chiffre d'abord les premières lettres de chaque groupe, puis les secondes, et enfin les troisièmes. « Pour chiffrer les premières, on place la première lettre de la clef, B, prise sur Talphabet mobile, sous la lettre A de l'alphabe^ fixe (voy. la fig. ci-dessus); et, prenant la première lettre de chacun des groupes de la dépêche sur Talphabet supérieur» on écrit la lettre qui lui correspond sur l'alphabet inférieur. « On passe ensuite aux deuxièmes lettres des groupes. Pour les chiffrer on place la deuxième lettre de la clef A sous la lettre A de l'alphabet fixe, et on opère comme nous venons de voir. On fait de même pour les troisièmes lettres. La dépêche se trouvera donc écrite comme suit : d e t rai sez 1 e t unn c 1 B AC BAC BAC BAC BAC B A e e V s XI It t el) m e V V n p f 1 = eevsuktebmevvnpfl « En admettant, ajoute le texte, que l'instrument soit perdu ou pris, il ne dit rien ; il faut connaître la clef » Il est facile de s'assurer que ce procédé n'est qu'un raccourci du précédent, en comparant dans les deux systèmes les trois alphabets qui correspondent à la clef BAC. i Une maison de Berlin (Egert, 6S, Kochs(rasse) a fabriqué un appareil mécanique pour cryptograbier avec ce système. s Nous verrons plus loin que si les correspondants prenaient cette recommandation à la lettre, il faudrait à peine une demi-beure pour décbiffrer tans eief toute dipêcjie cryptograpbiée d'après ce système.

The text on this page is estimated to be only 24.73% accurate

— 29 — Chiffre carré. A B c D E Y G H I J X L M IS 0 P 2. R S T| £ VWH Yi Z A a "F c T e 7 gîi" 1 J X T m n o £. q r s t "U ■vw X Z z B ¥ c d e f l £ 1 J Tç 1 m TL o P. a r s T XL vw X z z a C c a e T bd h a LlJ "k 1 m n o [£. a r s i TX V w X Z z a h Système de Saint-Cyr. |A|B|C|I)|E|F|GrH|I|J|lL|L|M|NlO|P|Q|R|S|T[TJ|V[W|X|Y|Z| a b c "a: e f ? Tï 1 2 ¥] T] m n o P <1 -p s 1 1 XL vw X z z a ¥ c ■a: etc. a V c a e f ff ¥ 1 • it 1 m n o P. q r s t M V w X .Y z a ¥ c d e etc. a h c d e f i h 1 A It 1 m n o P. 3. T» s t u V WX z z a ■5" c T e f etc. Comme on obtient le môme texte cryptographique avec les deux systèmes, le correspondant ou le déchitfreur n'ont môme pas à se demander avec lequel des deux la dépêche a été écrite *. Le seul avantage que ce procédé présente sur le précédent, c'est que, en cas de perle, l'instrument peut ôtre refait en deux ou trois minutes de temps. Au point de vue cryptographique, il n'acquiert une valeur réelle qu'à la condition d'intervertir l'ordre des lettres dans l'alphabet mobile. 11 est dit dans le Cours d'Art militaire qu'on pourrait établir l'instrument dans des conditions qui le rendraient plus portatif^ en le formant au moyen de deux cercles concentriques, dont l'un serait mobile et tournecait autour de son axe; ce serait ce dernier qui correspondrait au double alphabet. y. 1 Lorsque Talphabet est • ioteryerti ■ (voir plus loin), le système de Saint-Cyr donne un texte différent»

The text on this page is estimated to be only 12.86% accurate

- 30 — Cette disposition, qui est représentée dans la figure précédente, a été imaginée, dès 1563, par Porta >, et a reçu depuis de nombreuses applications, telles que le cryptographe de Wheatstone «t les boites à cadrans mobiles qu'on a vendues à l'époque de la guerre d'Italie. Tous ces appareils, dont quelques-uns sont représentés dans des ouvrages récents de télégraphie comme des inventions merveilleuses, ne sont en réalité autre chose qu'un «impie tableau de Yigenère. d. Système de Seaufort. Une modification assez ingénieuse a été apportée au chiffre carré par Tamiral anglais Francis Beaufort (1857). Quoiqu'elle paraisse au premier abord n'affecter que le maniement du tableau, elle altère assez sensiblement le texte cryptograpbique pour lui donner aux yeux des non-initiés un véritable air d'indéchiffrabilité. Voici d'abord le tableau de Beaufort: la b c Re t ^W jl^l m n 0 p qp s i u vw X y * a i> c a e f ? * t j Ttlm n 0 p q p 9 t u V wx y z a b c d e t ih. Ul^ 1 m n opq pat ■a vw :x.Y * abc d e f ft i J^^ m n 0 p q p s t TL viv i y z a b c a e f ff ? \î i 1 m n 0 p q P 8 t u V wx y z a 1) c d e ^f ° I4 f 1 m XI opq P S t u VVPI xy 2 a t c d e f f ° 1 j le l m n 0 pq p s t u V ^vx y a a b c a « f f % i j X Im n 0 p qp s l U V wx y z 0 "b ode f g^Ê i jk 1 m n op q p s t "G VW xy z a 1) 0 a e f fv. JT^l m n 0 p q r s t u v-vvx y z a b c à lU ^W lï Im -n 0 p q p s t u V wx y z al) c d e îgt K^t Im n op q ^ s t ■Q V"W^ xy z a 1) c d e f n jki mu o p qp s t u vwx y z a boa ^ ^ ? ^ ! J kl m n o p q P s t uv wxy z a 1> c d e îgt i J k Im n op q p s t 11 vw xy z abc de f rv ^ï^ m n 0 P qjc» s t u V wx y z a b c a e ts fi i j Klm nop qr s t U V vv^xy z a T> c d e ^A i j k l m n opq ^8 t n vw xy z a "b 0 d e f ?9Î jkl mn 0 p qp s t XL VW JL y z a ^c a ^J f ^1 .i klm 31 0 p q p s t nv wxy z a b c d e ^/^ ^^ï Imn opq p s t wv^vsr xyz a "b c a e f f^ i A^ mn 0 P qp s t XL V w_x y z a b c d « ^J? fii j klm nop q r s t nv wxy 2 a b c d e f g-fi i jk l*m.-D op C| p s t U.V w x.yz abc a e f jriii î^^ mu 0 P qr s txi vvirx y z a boa e f jr ^}l klm nop q r s t u V wxy z a b c de f XÊ U^% Imn op q p s t Ti vw xy z a 1> o d e f yti Al mu 0 :P q p s t dJ vwxy z a| i Gf CoLORNi, Seo'.og raphia, overe Seienza di sericerê o^euro; Prague, 159d,

The text on this page is estimated to be only 16.52% accurate

^ 3t £mparea^ou8 des hauteurs^ chiffré avec la clef BAC, donutera le cryiptograaime saivant : e mp aT e Z V o Ti s d e s h a-at e xir s BAC BAC BAC BAC BAC BAC BAC B X on "^ jy c f o Il i z -X i V ^SJ xg 1 • = xonbjycfohizxivùgjxglj. Voyons maintenant comment on procède. Pointez la lettre e dans le premier alphabet horizontal, descendez en ligne droite jusqu'à la rencontre de b; là, faites un demi-tour, soit à gauche, soit à droite; avancez jusqu'à l'extrémité de la colonne, et la lettre x, que vous y rencontrez, est le signe cryptographique cherché; et ainsi de suite avec les autres lettres. Les décfaiffreurs anglais, que le système de Beaufort a tant émerveillés, ne se doutaient certainement pas qu*on pût obtenir le même résultat avec les systèmes de Vigenère ou de Saint-Cyr en retournant tout simplement Tàlp^abet normale Il est facile de s'en assurer par l'inspection des deux figures vîx y z a ^ c etc. a T c 1 ef ^ ^i ï ¥ Im 1) o R il p s t n V w xy z H ra c [ïï] etc. ^ IVJ ^e_ 3 ^ t ^h ' J 11 T in tl o É S. r s t u V w X y z a f^ c d e etc. 1 u est probable que l'amiral anglais lui-même n'a jamais cru à la possibiJité de transformer son système en chiffre carré ordinaire ; on ne s'expliquerait pas, sans cela, que M. Morris Beaufort réclame encore énergiquement e» 06 moment, pour son illustre père, Tfaonneur d'ayolr doté son pays d*an système de cryptographie indéchiffrable {Cryplographif a tysiem of iceret wrUing^ bj/ thelate admirai sir Francis Bea\jvov(t),

— 32 — Le résultat serait encore le môme si, au lieu d'intervertir l'ordre des lettres dans l'alphabet normal, on mettait en nombre carré l'alphabet azyxwvuisrqponmlkjikgfedcb d'après le principe suivant : A B C D E F G H I •J etc. A a z y X ysr V TI t s T B b a z y X w V XI t s C c b. a z y X W V XL t D d c 1> a z y X. w V u e. Système de Qronsfeld. Ce système ne diffère des deux précédents qu'en ce que le travail peut être fait de tête, au lieu d'exiger le concours d'un tableau ou d'un appareil quelconque. Voici comment M. Bonlemps, inspecteur des lignes télégraphiques, s'exprime à ce sujet* : « Supposons qu'on ait choisi pour clef un nombre quelconque; « sous la phrase qu'on veut transmettre on l'écrit autant de fois « qu'il peut y être contenu, en établissant la correspondance « entre les lettres et les chiffres successifs. On prend pour lettre « h envoyer celle qui est placée dans l'alphabet, à une dislance « de la véritable égale au chiffre posé endossons, et l'on compose « ainsi un grimoire dont il est impossible de découvrir la clef, « fût-on doué de la perspicacité que suppose à son héros Edgar « Poe dans le roman du Scarabée d'or, ou de l'inlelligence des « agents employés à déchiffrer la correspondance de la duchesse « de Berry en 1832, d'après le récit qu'on trouve dans les mé« moires de M. Gisquel. » N'en déplaise à l'auteur que je viens de citer, le système du comte de Gronsfeld n'est pas beaucoup plus difficile à déchiffrer qu'un modeste chiffre à simple clef; il n'est, d'ailleurs, qu'une forme déguisée du tableau de Vijrenère •. i Les syilèmes télégraphiques aériens, électriques, pneumatiqttes ; Paris, 1876, p. 261. . > Dans une coufërence faite, en 1873, à la Société des Sciences miUtaires de Vienne, le D' Orges a soutenu que ce chiffre avait été inventé par le général Trochu (voy. Fleissner, loe. cit.j p. 19).

-33 Reprenons notre exemple, et soit encore une fois à chiffrer Détruisez le tunnely avec la clef 102 : chaque lettre du texte en clair sera respectivement représentée par une autre, avancée de un, zéro o^Tdeux rangs : de i \ 0 Z e e V. PTll 10 2 9 ixli S e £ 1-0 2 i cl) \ e t 10 2 me V U.II n 10 2 VTl-Q e 1 To" f 1 = èevsUktebmevvnpfL A la condition de prendre une clef composée exclusivement de nombres inférieurs à 10, ce système réalise parfaitement notre troisième desideratum^ et offre même, si les nombres sont très bas, certaines commodités pratiques; mais ces avantages perdent considérablement de leiïr valeur, en présence des facilités que cette disposition fournit aux investigations des déchiffreurs. (• Système à olef variable. Nous verrons plus loin que le déchiffrement des systèmes à double clef est principalement bdsé sur la connaissance du nombre de lettres composant la clef. On a songé à diverses combinaisons pour empêcher les déchiffreurs d'en faire le calcul; une des mieux imaginées est due à un membre de la Commission de télégraphie militaire. Il propose d'arrêter, à des intervalles irréguliers, Tordre de succession des alphabets, tel que l'indique la clef, pour revenir brusquement à la leltre initiale, ou alphabet premier. Ainsi, si la clef est Epamtnondas, au lieu de la répéter régulièrement par séries de onze lettres, il la coupe arbitrairement, et il écrit : epa -}- epaminondas epaminondas -}- epami + epaminon -}- etc. Le point d'arrêt est indiqué par une des letlres de la clef, qu'on intercale aux endroits voulus dans le texte chiffré. En voici un exemple, où j'ai pris pour lettre d'arrêt la deuxième de la clef, soit P : N on 8 ♦ part on s ♦ de ♦ ma i n EPA.M ♦ E PAM I NO ♦ E P ♦ EPAM • • • • ç P * • P * • • • KerckhoIRi.

- 34 Pour éviter tonte confusion dans Ut significatiba' attribuera la lettre d'arrêt, celle-ci est: remplacée dans le texte cryptograf^ique par un chiffre arabe correspondant à la place qu'elleHuéme occupe dans le mot de clef; ainsi, dans l'exemple Sfàe9;s^&, où le P est la deuxième lettre de la clef, on la remplacera par un % h tous les endroits où elle ne ddit^pas jouer le rôle de lettre d'arrêt. z ^ : ^ . ^ Avec le chiffre carré nous aurions le cryptogramme suivant ; rduePtïrfwagPfttPcfsaz, Pour empêcher le déchiffreur de faire un tâtonnement sur les premières lettres de la dépèche, on la fait précéder de quelques nulles f en ayant soin d'indiquer par la lettre d*àrrèt le point où commence le texte vraL Notre cryptog^mme pourrait donc s'écrire finalement : • « i •-. xmoprduept2rfwagphtpq2az. 4® Déchiffrement des systèmes à double clef. Excepté un petit travail, écrit en 1863 par le major allemand Kasiski S il n'a été publié, à ma connaissance, aucun essai pour le déchiffrement des écritures secrètes k double clef. Tout ce qui se trouve dans Porta^ Cospi, Breithaupt, 'S Gravezande, Thickenesse, Kliiber, Lacroix, Vesin, Joliet et autres, ne s'applique qu'aux systèmes à simple clef, et encoi*e ces auteurs n'ontiis guère songé qu'à déchiffrer des cryptogrammes où la séparation des mots est indiquée ostensiblement^. Un passage de V Interprétation des Chiffres de Cospi, le secrétaire du grand-duc de Toscane, tendrait à faire croire que les déchiffreurs ont évité de tout temps de révéler aux profanes leurs procédés de déchiffrement. On y lit à la page 3 : a II y a deux « sortes de chiffres, les uns simples et les autres composés; lais(c santà part ces derniers comme presque impossibles à déchiffrer, « nous ne parlerons que des premiers qui sont les simples». » ^ Die Geheimtchriften und die Dechiffrirkunit, > Le colonel Fleissner {Handhuch der Kryptographie) a adopté^ sans modification aucune, la méthode de déchiffrement d a major Kasiski. s Je citj d'après la traduction du Père Nicéron.

 Or, il n'est guère probable qu'un homme du talent de Cospi n'ait pas su déchiffrer les systèmes que Porta et Vigenère avaient publiés un demi-siècle auparavant. Le major Kasiski a basé son système de déchiffrement sur la détermination^ en quelque sorte exclu sive» des lettres du mot de clef. Tout en rendant hommage au savoir-faire de l'auteur, je ne puis m'empêcher de trouver que c'est là une méthode singulièrement compliquée et qui, dans un grand nombre de cas, doit donner un résultat négatif. Je vais indiquer un procédé qui me paraît non seulement plus sûr, mais encore plus simple et plus méthodique» Sans vouloir donner un travail complet, ce dont je ne vois pas trop la nécessité, je tâcherai néanmoins de développer assez la question pour que le lecteur qui voudra s'exercer à r«art de déchiffrer, » puisse trouver par lui-même et sans difficulté tous les petits détails dont l'exposition complète exigerait au moins une cinquantaine de pages; fabricando fit faber, on devient déchiffreur en déchiffrant. J'ai dit plus haut que, dans tout système par interversion, le • -déchiffrement d'un cryptogramme dont on n'a pas la clef comporte un calcul de probabilité et un travail de tâtonnement. Dans les systèmes à simple clef, où l'on ne fait usage que d'un seul alphabet, calcul et tâtonnement se bornent nécessairement à déterminer la disposition de cet alphabet; dans les systèmes h double clef il s'agit de trouver deux inconnues : 1® le nombre des alphabets, 2^ leur disposition respective. dm X^oxxibre des ali>bia1;>ets. Il semblerait au premier abord que les éléments d'investigation dussent faire défaut pour établir le nombre des lettres ou alphabets de la clef; rien n'est cependant plus facile. Supposons qu'on ait à cryptographier une phrase comme celle-ci : Vous ne pouvez vous défendre sans vous exposer^ etc. Comme il y a entre les deux premiers vous une distance de 8 lettres, et entre le deuxième et le troisième une distance de 12 lettres, il arrivera, si je prends une clef de 4 lettres, que les trois vous se trouveront chiffrés avec les mêmes alphabets, et

— 36 — donneront trois tétragrammcs semblables. S'il y avait un quatrième vous dans la suite du texte, il donnerait encore un tétragramme semblable, pourvu qu'il fût espacé du dernier d'un nombre de lettres formant un multiple de 4. Prenons un autre exemple : la présence de soldats ennemis nous a de nouveau été annoncée ce matin de différents côtés, et supprimons les intervalles : lapresencedesoldatsennemisnousadenouveaueteannonceece matindedifferentscotes. Il se présente, sur ces 75 lettres, 18 répétitions, dont 3 trigrammes nou, sen^ nce; et 15 bigrammes en, es, de^ ce, no, te, ts, etc. On aura beau prendre une clef de 5, 6, 7, 8, 9^ 10 alphabets différents, il arrivera toujours que Tune ou l'autre de ces répétitions se trouvera cryptograpbiée avec les mêmes alphabets, et qu'on aura ainsi un texte chiffré présentant, aax endroits correspondants, des groupes de lettres semblables ^ Je généralise maintenant le cas, et je pose les deux principes suivants : 1<> dans tout texte chiffré, deux poly grammes semblables sont le produit de deux groupes de lettres semblables, eryptographiés avec les mêmes alphabets ; i^ le nombre de chiffres compris dans Fintervalle des deux polygrammes est un multiple du nombre des lettres de la clefK Pour avoir le nombre exact des alphabets de la clef, il n'y a donc qu'à chercher le facteur commun contenu dans les nombres qui représentent les lettres des intervalles respectifs. Appliquons ce raisonnement au cryptogramme suivant : RMUUWQPMQGXHWBGGKKKNITMUXWWTMGGXHEPH Nous avons ici 4 répétitions : 1 trigramme GXH^ et 3 bigrammes MU, GG, TM. i En cryptographiant cette phrase avec une clef de 3 alphabets, on aurait 9 répétitions ; ayec 4, 5, 6 et 12 alphabets, on en aurait 8; on n'en aurait que 3 avec 13 alphabets, et on n'en aurait aucune avec une clef de 11, 14 ou 18 alphabets. s Je n*ai pas besoin de faire ressortir qu*il peut très bien arriver que deux bigrammes semblables (pour un trigramme c'est déjà bien rare) soient le produit de deux groupes de lettres différents.

— 37 — Or, de MD à M'U' U y a 21 chiffres = 7 x3 — GG à G'G' — 15 — =5x3 — TxM à T'M' — 6 — =2x3 — GXH à G'X'H' — 21 — =7x3 Le fadeur commun est 3 ; et, en effet, le cryptogramme a été chiffré avec une clef de 3 lettres. On comprend facilement que les chances de rencontrer des combinaisons de lettres produites par la rencontre des mêmes alphabets, sont en raison inverse de la longueur de la clef et en raison directe de la longueur du cryptogramme. Lorsque le rapport des lettres de la clef à celles des chiffres du cryptogramme est tel qu'aucune répétition n'a pu se produire, le déchiffrement présente des difficultés, et l'on est obligé d'avoir recours au tâtonnement ; c'est un point sur lequel je reviendrai plus loin. 6. Ordonnaxxoe des alphabets. Remarquons d'abord que le nombre des alphabets différents ne peut guère aller au delà du nombre même des lettres de l'alphabet; avec un nombre inférieur ou supérieur il devient en effet impossible de représenter la clef par un mot, ou du moins il y a certaines difficultés dans le maniement de la clef. D'ailleurs, ce n'est pas la possiblité de se servir d un grand nombre d'alphabets différents qui donne de la valeur à un système, mais plutôt la difficulté plus ou moins grande de déterminer le nombre des alphabets employés K Ces 26 alphabets peuvent être ordonnés de trois manières dif< rentes : lo Ou bien les lettres se suivent dans Tordre de l'alphabet normal, comme dans le tableau de Vigenère; 2o Ou bien cet ordre est interverti d'une façon quelconque (voy. p. 46), mais les 26 alphabets n'en sont pas moins disposés en nombre carré ; i Uq auteur allemand, Krohn (Btuhttaben'Und Zaklemysteme fur die Chiffri" rung tnm. TeUgrammen*^ Berlin, 1873), ne s'est pas rendu compte de ce principe, et il a composé» à Tusage dé la correspondance cryptographiqae, un die* tionnaire contenant 3,200 alphabets; c'est à la fois trop et trop peu.

- 38 ^ 3<> Ou bien encore les S6 lettres sont placées dans un ordre différent dans chacun des 26 alphabets. Le déchiffreur n'a généralement aucune peine à constater laquelle de ces trois dispositions a été adoptée. a. Alphabets non interveriU» Reprenons le cryptogramme précédent et partageons-le en tranches de trois chiffres : 123 123 123 123 123 123 123 123 123 123 123 123 RMU UWQ PMQ GXH WBG GKK KNI TMU XWW TMG GXH EPH Nous savons que c'est la lettre E qui doit revenir le plus fréquemment; si donc je réunis les lettres qui dans les diverses tranches appartiennent au même alphabet, il me sera facile de constater quels sont les trois chiffres qui représentent la lettre E. De plus, comme chacun des 26 alphabets se trouve caractérisé par le chiffre qui correspond à TE, la connaissance de ce seul chiffre entraînera nécessairement celle de tous les autres du même alphabet, que le cryptogramme ait été chiffré avec le tableau de Vigenère ou avec les systèmes de Saint-Cyr et de Gronsfeld. Nous aurons donc : I II III R M U U W Q P M Q 6 X H W B G G K K K N I T M U X W W T M G G X H E P H 1" colonne, G =E soit (2® colonne, M = E 3» colonne, H = E Si Ton H^herche maintenant dans notre tableau de la page 26 quels sont les alphabets où la lettre E est figurée par les chiffres

The text on this page is estimated to be only 28.86% accurate

q V B t ■a-v w X z z a 1> I 1 • li 1 m n 0 V 4 T s t ni v w X z z a 1) eM e T I 3> [3 e T m E [S tï k T m n 0 £ ^ r s t TL -V w X Z z a 15 c = Personne ne peut déchiffrer votre dépêche. • Lorsque la dépêche est courte, il arrive parfois que le coeflScient des répétitions, dans telle ou telle série, nous laisse dans le doute sur le chiffre qui correspond à TE. Cet inconvénient n'est pas bien grand, surtout si la clef n'a que 5 ou 6 lettres, car le contexte nous met immédiatement sur la voie. Il peut même arriver que, dans un cryptogramme de plusieurs lignes, aucun des chiffres le plus fréquemment répétés ne corresponde à la lettre £. Il existe un moyen bien simple de déterminer, en dépit de cette anomalie, les différents alphabets de la clef. Pour bien saisir ce procédé il faut se rappeler que, dans les alphabets non intervertis, la place relative des lettres est toujours la même ; ^dans Talphabet où le / correspond à l'E, la lettre suivante ou le m correspond nécessairement au F, et le r correspondra au K et le (/ au W; de même, dans l'alphabet où la lettre E est figurée par un /?, les lettres K et W seront représentées par les chiffres v et A. Or, comme le K et le W ne se renoontrent qu'exceptionnellement en français, le déchiffreur rejetiera tout alphabet où les chiffres correspondant à ces lettres auront un coefiScient un peu élevé. 1 Gomme dans (e système de Gronsfeld le premier alphabet est représenté par an zéro, U faut diminuer le numéro d'ordre de chaque "alphabet d*une unité. s Lorsque le déchiffreur sait qu'un texte en langue étrangire a été cry^togra-phié dans ces conditions, il n*a pas à se préoccuper, pour la bonne jréussite de son trayail, de savoir s'il comprend la langue ou non ; il lui suffit d'être renseigné sur la lettre qui» dans cette langue, se prés^ate le plus Bouvent (voy. p. 49).

— 40 — Supposons maintenant que, dans le calcul des lettres de telle ou telle colonne, je trouve pour les plus fortes fréquences Ml,9r, Sd, 6v, 5A^ 5u, ix, 3o, 3q; je verrai tout de suite, à l'inspection du tableau, que l'alphabet cherché doit être celui où TE est représenté par le chifTre h, car dans les 8 autres alphabets les chiffres /, r, d, A, u, etc., correspondent tantôt à un K, tantôt à un W, un H, un Y ou un Z, ce qui, vu la minime importance de ces lettres, est un cas inadmissible. Au point de vue de la déchiffrabilité des dépèches, les systèmes à alphabets non intervertis ne présentent pas plus de garanties qu'une interversion à simple clef où la séparation des mots n'est pas indiquée ^ b. Alphabett irrégulièrement intervertie. Lorsque, dans le déchiffrement d*un cryptogramme, il est impossible de construire un sens avec les alphabets que les retours de la lettre E semblaient indiquer, on doit supposer qu'on se trouve en présence d'un système à alphabets intervertis, et il faut en quelque sorte prendre d'assaut, l'un après l'autre, les premiers chiffres de la dépèche. Si le cryptogramme est assez long, la solution du problème présente rarement des difficultés insurmontables; elle demande seulement un peu de patience et un certain esprit d'induction. C'est alors que, en dehors du calcul des répétitions isolées, il faut marquer les retours de certaines combinaisons binaires et ternaires dont j'ai parlé à la page 20; il faut également savoir mettre à profit les renseignements qui sont fournis sur la nature probable de la correspondance, et tenir compte du style que les circonstances ou la situation respective des correspondants comportent. Ainsi, pour citer un exemple, la combinaison binaire ez est extrêmement rare dans la correspondance entre personnes qui se tutoient, tandis que, d'un autre côté, la plupart des instructions remises, en campagne, à des Inférieurs commencent par vous ou le, 1 M. d'Aoriol {Manuel de la eorreepondance teerète, poitale ou télégraphique ; Paris, 1867) a pubUë an tableau qui permet de chiffrer, deux par deux, les lettres du texte en clair. Abstraction faite qu'on peut établir sur les combinaisons de lettres le même calcul que sur les lettres prises isolément, le système donne trop de prise an tâtonnement, et exige de plus un secret absolu.

The text on this page is estimated to be only 13.70% accurate

\ - 41 — Nous allons déchiffrer une dépèche envoyée de Londres à l'Agence Havas, au sujet des affaires militaires d'Egypte. Londres, 2 septembre. Rbnbj — jhgts — ptabg — jxzbg — jicem — qamnw — ivgag — neimw — rezkz — suabr — rbpbj — cgybg — jjmbe — npmuz — chgwo — udcko •-^ jkkbc — pypmj — npgkw — pwadw — cpbvm — rbzbh — jwzdo — meaao — jlbmn — kexbz — awmwk — aqmtg •— Irghc — qbmwe — zèukw — retew — cpbym — ebamn — rbjcz — eaauz — kbcbx — rbjej -* dtdor — Ikcey «— ifbhx — jbsbo — dfèhk -— zaaak - — swmyz — skanz — ikedr — abayl — njsbj — sbpal — gdyfz — gbaqk — nbauz — gdpvr — sajex — ndnbj — gdujx — Imxjl — skkbo — hamnz — iagwo — rbjej — dtmkz sbsbe — dwzmj — jqqjx — jzmkz — jjyhg — dtxij — juypv — jvxi^a — jlmhc — jjbso — cejtz •— ijbwx — eexwx — jwgwx — jwsbe -— jjmkx •— Idxjb — dboaj — jjqdj — ctmjz — Iqxpz — hmjeh — ueuig — daauw — ivgag — ne. Cherchons d'abord h déterminer le nombre des alphabets de la clef : RB — R'B' =r 55 = Il X 5 R B — R"B" = i05 = 21 X 5 B J — B' J' = 50 = 10 X 5 B J — B' J' == 225 = 45 X » BG — B'G' = 5 = 5 B G — B" G" = 40 = 8 X » ou 4 X 10 R E — R' E' = 115 = 23 X 25 MW — M' W = 94 = 47 X 2 M J — M'J' = 105 = 21 X 5 F Q _ F Q' ^ 305 = 61 X » Je n'ai noté ici que la moitié des répétitions, mais cela nous suffit pour voir que la clef doit être composée d3 5 lettres. Si nous partageons ensuite le cryptogramme en tranches de 5 chiffres et que nous fassions le calcul des répétitions par coionne, nous trouvons : 1" colonne : 19 j, 8 r, 7 d, 7 n, 7 s, 7 c, 6 i, 5 1, 4 g, 3 p, 3 u, 2 h, 2 k, 2q, 2 e, 2 a, 2 z, 1 m; 2« colonne : 14 b, 10 e» 7 w, 7 j, 6 a, 5 p» 5 t, 5 y, 5 d, 5 k, 4 f, 3 a, 3 h, 3 q, 2 m, i 1, 1 i, 1 z, i g, i X ; 3* colonne : 12 m, 9 g, 9 a, 7 x, 6 j, 6 u, 6 b, 6 c, 5 z^ 4 s, 4 p, 4 y, 2 k, 2 n, 2 i, 1 q, 1 0, 1 i, 1 t ; 1

— 42 4

— 43 — le, leff, les pronoms je, me, ce, cet, ces, mes, ses, la négation ncy on la préposition de. Si c'est la négation ne, un verbe au participe présent doit suivre, tel que recevant, revenant, et GTS représente la terminaison ant'y or c*est inadmissible, le t étant une lettre très usitée et le chiffre S ne se présentant qu'une seule fois dans la 5* colonne. Il faut encore rejeter les, cet, ces, mes, ses^ le troisième chiffre N ne pouvant guère être la lettre s ou t, par la raison qu'il ne se présente en tout dans sa colonne que deux fois. Gomme le premier chiffre R revient huit fois, il est également impossible que nous soyons en présence d'un ; {je)-, c'est donc le ou ce, mais plutôt le que ce, à cause de la fréquence du chiffre R. Le ou ce doivent être suivis d'un substautif, d'un adjectif ou d'un nom de nombre, et, remarquons-le bien, le mot doit avoir un e dans les deux premières syllabes. Aucun nom de nombre ne se trouve dans ce cas; les adjectifs récent, décent et téméraire qui ont les deux e, doivent être rejetés, le coeflScient 1 du chiffre N étant, comme cela a déjà été dit, trop faible pour un t; détes^ table ne va pas non plus, le 12® chiffre T n'étant pas un e; les substantifs désert et télégraphe se trouvent, à cause de leur t, dans le même cas que décent et téméraire. On ne trouve que général qui remplisse les conditions voulues; nous nous décidons par suite pour le au lieu de ce. J'inscris ces deux mots, et je continue. SPTABGJX Le général . . . . e . e . Il est à présumer que la dépêche dise de quel général il est question: c'est donc un nom propre qui va suivre. Le chiffre S doit être une lettre fort peu usitée, telle que k, w, y, z, car, avons-nous dit, il ne se rencontre qu'une seule fois dans sa co lonne; nous avons de plus un e au S" et au 7® rang, et ce dernier e est suivi d'un chiffre avec le coefficient 1 : cela répond exactement à Wokeley. ZBGJICEMQAM Le général Wolseley .«le e

II est encore probable que le verbe va suivre son sujet : nous connaissons déjà la valeur des2«, i^ et i^ chiffres, et nous savons que le Z a un assez fort coefficient ; si Z est le verbe auxiliaire a, le participe qui suit est élevé ou électrisé; mais ceux-ci n'ont pas IV final au rang voulu; donc le verbe est à un temps simple. Des seuls verbes possibles dépend, dément, mène^ retenu et télégra^ phie, il faut préférer le dernier, h cause de ïe final. UWIVGAGNE télégraphie .... a i 1 . a Il y a tout lieu de supposer que télégraphie est suivi de que ou qu'il, ou bien d'un nom de lieu : cen*estpas que, puisque I n'est pas un tf ; ce n'est pas qu'il, car nous connaissons le / (= T) de la S« colonne; c'est donc probablement un nom de lieu. Le nom de lieu doit être précédé de la préposition de ; ici cependant ce doit être un simple d\ car Ye de la 3* colonne est figuré par uù B. En fait de noms de lieu commençant par une voyelle, ayant un a au 4* rang et un / au 6«, on ne peut citer q\x*Ismaïlia. IMWREZKZSUABRRBPBJC d'Ismaïlia ..il at.e.d se.le.en* La tournure de la phrase^ ainsi que la présence de il, indiquent tout de suite que IM signifient qu; le verbe doit suivre et on devine aisément, aux lettres que nous connaissons, déjà que ce verbe est attend. Quant au groupe final le dictionnaire ne donne que les mots selle et seulement, qui cadrent avec l'ensemble : c'est évidemment le dernier que nous avons ici. GYBGJJMHENPM qu'il attend seulement ..e le .er.i.e L'adverbe :^eu/emen^ est rarement suivi d'un que; mais comme le G ne revient qu'une fois dans sa colonne, ce qui s'applique très bien au q^ et que nous avons au 3« rang un e, nous devons admettre le que. Le dernier groupe est un mot commençant par une consonne, puisqu'il est précédé de le, et cette consonne

— 45 revient assez souvent; il y a de plus un i au S* rang : œrvice répond seul à ces données.
UZCHGWOUDCKOJKKBCPVPMJNPGKWPWA de tra..*.rt.et.e. ommun i c a t i o n s Ce passage ne présente aucune difficulté et nous lisons : de transports et de communications. La fin de la phrase est encore plus facile : soit complètement o.ga.ise .our ,a,re .ne n.u.elle marche en ..ont c. a. d. soit complètement organisé pour faire une nouvelle marche en avant Je m'arrête ici ; il sera facile au lecteur de déchiffrer lui-même le reste. Abstraction faite du nombre, il n'est possible au déchiffreur de déterminer la valeur des lettres qui composent la clef, que lorsque la dépêche a été chiffrée avec le système de Saint-Cyr. A moins d'admettre que la clef doive nécessairement être un mot français ou ayant un sens quelconque, toute dépêche, écrite avec des alphabets mis en nombre carré, comporte 26 ciefs différentes, selon l'alphabet initial du tableau. Rien ne prouve mieux que cette considération combien le major Kasiski a eu tort de fonder sa méthode de déchiffrement sur la valeur même des lettres de la clef. Dans le cas présent la clef est dégel avec le système de SaintCyr, etpuluy avec le tableau qui va suivre (p. 46). Une fois qu'on a pu déterminer le nombre des lettres de la clef, étant admis que la dépêche a une certaine étendue et qu'on a pu recueillir quelques renseignements sur les correspondants ou la nature probable du contenu, il est bien rare qu'un cryptogramme ne puisse être déchiffré. Dans les cas un peu difficiles ce sont généralement les deux ou trois premiers mots qui viennent jouer le rôle de traîtres ; or, rien n'est plus facile au déchiffreur que de se faire une liste des mots qui, en temps de guerre, peuvent commencer une dépêche et de les classer ensuite d'après la place de l'E qui s'y trouve ; ceux qui ne contiennent pas d'Ë n'en seront que mieux signalés à son attention.

The text on this page is estimated to be only 22.42% accurate

«, Alphabeti régulièrement iHtorwrlw. — Sym«trt« dt poiUion, J'ai déchiffré la dépèche précédente sans rechercher si elle avait été cn^tographiée d'après un système qui ordonne ses alphabets en nombre carré, ou si les correspondants s'étaient bornés li choisir au hasard cinq alphabets diRérents. C'est cependaot UD point très important et que le déchiffreur ne doit jamais négliger. Du moment, en effet, que les alphabets sont disposés en nombre carré, et que la signification d'un chiffre commun a été trouvée dans deux ou plusieurs alphabets, on peut, au moyen d'une simple addition, déterminer la place que doit occuper dans ces différents alphabets tout nonveau chiffre dont la valeur pourra être établie dans un seul. Pour nous rendre compte de cette particularité, qui n'a encore été relevée dans aucun ouvrage de cryptogi'aphie, considérons un instant Le tableau qui a servi à chiffrer notre cryptogramme.

The text on this page is estimated to be only 29.77% accurate

— 47 — La disposition de ce tableau ae diffère de celui de Yigenère qu'eace que Fordre normal des lettres a été iatervertî; : les mêmes lettres^ tout en n'occupant jamais deux fois la même place, par rapport au numéro d'ordre des colonnes verticales, se suivent néanmoins toujours dans le même ordre dans les colonnes horizontales. Ainsi, dans chacune de ces dernières, le R est toujours suivi de TE, et TE est toujours à un rang d'intervalle du P et à quatre rangs d'intervalle du L. Une fois donc qu'on connaîtra la place du H dans deux alphabets, la place des chiffres E, P et L se trouvera déterminée dans le second alphabet, dès qu'on aura pu l'établir dans le premier. Prenons un exemple : je suppose qu'en essayant de déchiffrer une dépêche cryptographiée avec une clef de trois alphabets, on ait déjà trouvé la valeur des 19 chiffres indiqués ci-dessous; soit EPBLAFN pour le premier alphabet, UAT pour le deuxième, et TDFHKMRSIG pour le troisième. Comme les chiffres des trois alphabets pris deux à deux ont uae lettre commune, A et T, je puis reporter les lettres d'un alphabet dans l'autre, à la simple condition de les placer, daas les trois alphabets, à des distances respectivement égales de la lettre commune. ABCDEFGttlJK.LMN0P9RS TUVWXYZ . e . p . b 1 » ^ a .' . t . . d f . Ti . km . . f a , . 8 \ . . . 1 c * pespubl ica. .t . .d^.li. km . n • • . îi . km. . n . . p e s p iil> 1 i c a . . t . . d. t . .t. .df.h.km.n. ,vespiiblica Si j'avais tenu compte de cette particularité dans le déchiffrement de notre dépêche, f aurais pu m'arrêter au cinquième mot, le nombre des lettres déjà déchiffrées, augmenté de celui des lettres connues par symétrie de position, étant plus que suffisant pour déchiffrer en quelque sorte au courant de la plume le reste du cryptogramme. i II importe peu, et c'est on pcÂnt essentiel à noter, que Tordre de saeœssion des lettres dans les colonnes verticales soit le même que dans les colonnes horizontales ; cet ordre n*est généralement observé que pour permettre aux corresgodants d'étabMr plus ûtcUement leur tableau de mémoire.

The text on this page is estimated to be only 25.46% accurate

— 48 — Il sera focile de s'en rendre compte par l'inspection du tableau ci-dessous, où les lettres connues par le déchiffrement des cinq premiers mots sont représentées par des majuscules, tandis que celles dont la valeur est révélée par le principe de symétrie de position sont Qguréos par des mîauscules : II est d'autant plus important de ne pas négliger cette particularité des alphabets mis en nombre carré, qu'on ne peut guère avoir occasion de déchiffrer un cryptogramme dont les 26 alphabets soient ordonnés au hasard; ce serait un système peu pratique et par cela même inapplicable en temps de guerre. Car, si l'obligation de confier t la mémoire la disposition d'un seul alphabet peut parfois présenter certaines difficultés, quel ne sera pas l'embarras, lorsqu'il s'agira de retenir 36 alphabets différents, ordonnés chacun d'après un plan qui exclut toute régularité? On serait obligé d'avoir recours k des notes écrites, et la valeur ou la sécurité du système ne dépendrait plus que de la prudence de l'agent appelé à l'appliquer. Aussi toutes les combinaisons de quelque valeur qui ont été imaginées dans ces dernières années, comme, par exemple, le cryptographe de Wheatstone, reposent-elles sur une interversion régulière de l'alphabet, et le principe que je viens d'exposer leur est parfaitement applicable. d. AtphtU>tU inditervMtii. Si dans le déchiffrement d'un cryptogramme à alphabets intervertis il est impossible de déterminer le nombre des alphabets de la cler, soit parce que la dépêche est trop courte, soit parce que la clef est trop longue, la solution du problème présente des difScultés, sinon insurmontables, du moins capables de lasser la patience du plus habile déchiffreur. La situation change si l'on se trouve en possession de plusieurs cryptogrammes écrits avec la même cle", si courts qu'ils soient

— 49 d'ailleurs; en les ordonnant les uns au-dessous des autres on peut faire sur la répétition des lettres un calcul analogue à celui que nous avons fait, page 38, sur les chiffres groupés par tranches ou par colonnes. Voici une douzaine de cryptogrammes très courts, qui ont été chiffrés d'après le tableau précédent, et cela avec une phrase entière : je me mets sur la défensive', nous allons voir que le déchiffrement en est assez Faci'e. N» \.
uhyrejïMbg^fammVjtdmriq NO 2.
UHWPRBQLKlfiEWRBJRBKLGIXBQEXHM No 3.
lEWHCHÛKpjÎTMVGJJEDZVA No 4.
UWVRRHÎKMGWWEGHDGXSRQH j No, S.
UHSHAHKSYCJWZVXJYNDMQQN i No 6.
YHVHM4GQKC.WXPVIHHWLZVLTHV NO 7.
LHVHAAGRLPFMSOHIPWZZJELQRBW N» 8.
SWUIRXIGJUFSHGWRSZBAAL No 9.
UHWHVAYULGJWOBKDEBKQ NoIO.
YWXHYSlALGBVPSWIWWJRRH Non. WQREXBÏENHMVYMHSIYM No 12. SWUHDïîPJJGKXGMHJ. No 13. GQVQRVqTQQSPWR Notons en passant que sur les 22 lettres dont se compose la clef, il y en a 3 qui sont répétées et qu'ainsi nous n'avons en réalité que 14 alphabets différents; c'est un cas qu'il n'est guère possible d'éviter et dont le déchiffreur doit savoir tirer parti. Afin de ne pas étendre ' la démonstration outre mesure, je ne m'attacherai qu'aux deux premiers mots des numéros IV, V, VI et VII; de plus, pour que le lecteur puisse plus facilement suivre mon raisonnement je vais mettre d'avance les lettres de la clef au-dessus des colonnes correspondantes. Kerckhoffs.

The text on this page is estimated to be only 22.04% accurate

- oO — " 1 2 3 ^ 5 6 7 8 9 10 ■ j E IVI E M E T S S u etc. I u h y b V • J • l P m b c f aimntj t chnpi q 11 \x 11 w p r b q 1 k • 1 bl>vpejrb,elo. m » 1 e w h c h < q k q m Imvgjrjedzva IV XL w V r r h • 1 k m c TV"we g'hdcxsrc]!! V U h S h a h k S V c jwz etc. VI y h V h m a g q k c wxpvî etc. YB 1 h V h â a ^. r 1 P fm.soJil etc. vm s AV u • 1 p X • 1 c • J n fslig^vrszbaai K TX h w 11 V a ^ XL \ c • j\voukdebkq X y AV X h y 11 1> a 1 z b vp s wiwvvjr p h Xï w q V e X b • 1 e n h mvymhsiym xn s w IX 11 d h P • J ■ c kxgmhl xm g ^ y q p V o t q q spwr £n appliquant le calcul des répétitions, nous admettons la présence de Ve dans les colonnes 2 (=H), 4 (==H),5 (=R), 6 (=z H), 7 (= I), 9 (= L), 10 ^= C) ; nous voyons de plus que le chiffre représentant la lettre e est le même pour les colonnes 2, 4 et 6, ce qui nous permet de conclure que celles-ci correspondent à un seul et même alphabet. Les colonnes 3 et 5, ainsi que les colonnes 8 et 9, appartiennent également au même alphabet respectif; mais comme nous sommes censés ignorer la clef, ce n'est que plus tard que nous pourrons le constater; nous comptons donc provisoirement, sur les 10 colonnes, 8 alphabets différents. Commençons par le n'» IV ; 12 3 4 5 6 7 N« IV. U W V R R H I è è . e e e Nous avons admis que les chiffres RHI représentent tous les

— 51 — trois la lettre e. Aucun mot ne pouvant en français commencer par deux e, nous avons là un mot finissant en ée ; le nombre de chiffres qui précèdent cette terminaison nous indique aussitôt que nous sommes en présence du mot armée, précédé de /'. Inscrivons donc 6 chiffres, dont 2 sont donnés par la symétrie de position*. 123456789 N» V. UHSHAHKSV Nous venons de voir que U = /; le mot qui suit le bl \in e au 2^ et au 4« rang; c'est le cas de la dépêche que nous avons déchiffrée page 42; il est donc inutile de recommencer notre raisonnement, et nous disons tout de suite que c'est général. Le déchiffrement de ce dernier mot nous fait connaître 10 chiffres nouveaux, soit les 5 du mot général^ S. A. KSV, plus 5 autres fournis par la symétrie de position; la rencontre du S dans les alphabets 8 et 9 montre en même temps que les deux colonnes ont été chiffrées avec le même alphabet. 1234S6789 No VI. YHVHMAGGK Comme le M ne correspond pas à un n(= A), le premier mot ne peut guère être que ferez ou serez; il est impossible pour le moment de décider entre fei 5, mais, quel que soit le verbe, il doit être suivi de vous. Inscrivons 15 nouveaux chiffres, dont 4 obtenus par déchiffrement et 11 par symétrie de position. 1 234 5 678910 NoVII. LHVHAAGRLP . e r e n V o . e . Nous avons ici : le renvoi, je renvoie, ou ne renvoyez ; or; la symétrie de position s'oppose à ce que le R de la 8* colonne soit 1 Le lecteur ne saisira bien ce qui est dit ici de Tapplication du principe de symétrie de position que 8*U se dresse sur une feuille de papier un tableau avec l'alphabet normal en tête^ en laissant en blanc des cases pour huit alphabets (i, 2,4,6), 3, 5, 7, 8, 9, iO), cases qu'il remplira à mesure que nous avancerons.

- 52 un t; car nous aurions alors dans le 3^ alphabet un R placé h un seul rang d'intervalle du S, et un autre R placé à 17 rangs d'intervalle du S dans le 8« alphabet; c'est donc un y, et nous traduisons : ne renvoyez. Le déchiffrement ne nous a donné ici que la signification de 3 nouveaux chiffres; mais la symétrie de position nous en fait connaître dans les différents alphabets réunis 46; rien qu'en inscrivant le L dans Talphabet de la i^^ colonne, où nous ne connaissions encore que ru = /, nous pouvons y déterminer la place de 11 chiffres nouveaux. Nous constatons en même temps que les colonnes 3 et 5 sont ci^ ptographiées avec le même alphabet. Le lecteur n'éprouvera aucune difficulté à déchiffrer le reste lui-même, surtout s'il continue par les n»* XI et XIIL Concluons de ce qui précède que, quelle que soit la disposition adoptée des alphabets, les correspondants sont toujours tenus d'écrire chacune de leurs dépêches avec line clef différente. c. Système à olef veiiriable. 11 a été question à la page 33 des systèmes à clef variable. Une dépêche écrite d'après le système indiqué n'est guère déchiffrable qu'autant que le déchiffreur peut retrouver la lettre d'arrêt. Ce n'est pas facile avec une dépêche très courte; mais lorsqu'elle a quatre ou cinq lignes, on constate aussitôt une certaine régularité dans l'irrégularité même des retours de la lettre; c'est le seul chiffre, par exemple, qu'on ne rencontre jamais deux fois de suite. Or, une fois que la lettre d'arrêt est trouvée, le déchiffrement est assuré; il n'y a qu'à mettre en colonnes les différents groupes formés par les intervalles d'une lettre d'arrêt à l'autre, et faire le calcul que nous connaissons. Un renseignement précieux est, en outre, fourni par le chiffre arabe qui indique la place occupée par la lettre d'arrêt dans la clef ^ Le déchiffrement ne peut présenter quelques difficultés que lorsque l'ordre alphabétique des lettres a été irrégulièrement interverti; aussi ai-je pu déchiffrer, en moins de deux heures de i En cas de difficultés imprévues on fait le tâtonnement sur les 26 lettres de l'alphabet*

- S3 temps, les cryptogrammes composés d'après ce système, qui m*onl été remis par la Commission de télégraphie militaire. 5** Un chiffre à triple clef. Il résulte de nos essais de déchiffrement que de tous les systèmes de cryptographie à base variable qui sont usités aujourd'hui, aucun ne présente de garanties sérieuses d'indéchiffrabilité. Certes, il peut arriver que telle ou telle dépêche, d'une longueur de quatre à cinq lignes, cryptographiée avec des alphabets non intervertis et avec une clef n'ayant que cinq ou six lettres, résiste aux efforis du meilleur déchiffrenr; rien n'est même plus facile à celui qui sait déchiffrer, que de combiner des cryptogrammes indéchiffrables avec le plus vulgaire des systèmes. Mais si la cryptographie doit jamais devenir, comme Ta dit un de nos meilleurs généraux, un auxiliaire puissant de la tactique militaire, il faut que le système adopté puisse défier, alors même qu'il se trouve manié par des mains inexpérimentées, les investigations les plus laborieuses des déchiffreurs. S'il était permis de négliger un instant le côté essentiellement pratique que doit présenter tout système de cryptographie destiné aux besoins de l'armée, pour n'attacher de prix qu'au desideratum qui demande Pexclusion du secret, on pourrait adopter un système à triple clef ^ et combiner un procédé de transposition avec un système d'interversion à base variable. Le système de Sainl-Cyr, combiné avec la méthode de transposition indiquée page 13, permettrait le minimum dé notes écrites, et donnerait un cryptogramme, sinon mathématiquement indéchiffrable, du moins ne comportant aucun calcul de probabilité. Les deux clefs devraient être représentées par des mots différents, tels qu'un adjectif et un substantif; le premier mot, composé d'un petit nombre de lettres, servirait de clef au travail d'interversion, et le deuxième, d'un nombre de lettres plus considérable, donnerait la formule de la transposition ; par exemple : chose problématique y affaire exceptionnelle i. 1 L'emploi simultané des deux procédés cryptographiques ne saurait dispen* ser les correspondants de changer de clef pour chaque dépêche.

The text on this page is estimated to be only 28.99% accurate

^ 54 Chiffrons une dépêche d'après ce système : Vous ferez ce soir une attaque simulée, en prenant pour clef sénat romain et en nous servant du tableau de Vigenère. vous ferezce soi v ixaea t l aquesinitil ee SEW AT SET^ATSEiyAT SE7VATSE1NATSETVATSE Dsli sy^vvp z v"ww"b 1 kinr rainl e dxixlcmzuewi Romain donne pour formule numérique 653124; on a donc : B 1 2 3 ^ 5 6 1 11 s h s y w 2 V p z V w w 3 T) • 1 le in V V ^ a ■m l e d ■Q 6 JC k m z n e e M^ • 1 a b c d e 5 3 1 2 ' ^ 6 d c a w • 1 "b 5 e XI m X k Z 3 r r k \> • 1 m 1 w y h n S s 2 XV w z V V V k u d 1 a TO e = dcawibeumxkzrrkbimwyhnsswwzvrvudlame. Mais, je le répète, ce procédé a beau dispenser de la nécessité du secret et garantir une indéchiflfrabilité presque complète, il laisse trop à désirer au point de vue pratique pour qu'il soit possible de songer à l'appliquer au service de la guerre. Aussi n'est-ce qu'à titre de curiosité que j'ai voulu indiquer un système dispensant de la nécessité du secret et réalisant ainsi le principal desideratum de la cryptographie militaire. C, Dictionnaires chiffrés. Il est difficile d'avoir des renseignements précis sur lesdiflférents systèmes de cryptographie qui, depuis le siècle dernier, ont été en usage dans l'armée française ; on sait cependant positivement que, dès avant la Révolution, l'état-major avait fait dresser, à Tusage de la correspondance secrète, des tables analogues à celles qu'emploie encore aujourd'hui le ministère des affaires étrangères. Ces tables contenaient, à côté de phrases toutes faites, un certain nombre de mots usuels; en face se

trouvaient un ou deux nombres pour les représenter. Le général Lewal a cité, dans le Journal des Sciences militaires, le fragment d'une lettre adressée, sous la date du 2 mai 1818, par le ministre de la guerre Davout à son collègue des affaires étrangères, pour lui demander deux chiffres de ce genre pour la correspondance militaire. Ces chiffres, ou tables chiffrantes, comme on les appelait autrefois, sont devenus le dictionnaire chiffré dont on se sert aujourd'hui dans Tarmée. Dès 1850, Brachet* avait songé à composer pour le public un dictionnaire analogue, oti chaque mot est invariablement représenté par un nombre de cinq chiffres. M. Sitller^a imaginé depuis un petit vocabulaire d'une cinquantaine de feuilles, où chaque page contient 100 mots, représentés par des nombres allant de 00 à 99; on détermine le mot qu'on veut écrire en ajoutant à ce nombre le numéro de la page. La pagination, qui est laissée en blanc, et qui doit être indiquée à la main, d'après un système conventionnel, constitue le secret de la méthode. Le plan de l'ouvrage est assez bien conçu ; il n'en est que plus à regretter que l'auteur ait oublié d'indiquer les précautions à prendre pour assurer le secret des dépêches, au cas où le dictionnaire viendrait à tomber entre les mains de l'ennemi. MM. Brunswick' et Gallian* ont cherché à combler cette lacune, en composant, le premier, un dictionnaire où les lettres avec leurs diverses combinaisons binaires, et quelques milliers de mots avec leurs flexions grammaticales, sont représentés par des groupes de chiffres allant de 0000 h. 9999, et le second en dressant un dictionnaire analogue, où les groupes de 4 chiffres sont remplacés par des combinaisons de trois lettres '. 1 Dictionnaire chiffré. Nouveau système de correspondance occulte; Paris, i850. > Dictionnaire abréviatif chiffré; Paris, 1868. s Dieiionnaire pour la correspondance télégraphique seerète, par un secrétaire do légation; Paris, 1868. « Dieiionnaire télégraphiqtie économique et secret , par Marner t-Gallian ; Paris, 1874. C'est sur le môme principe que reposent les dictionnaires aUemands de NiETBE (Berlin, 1877) et de Walter (Winterthûr, 1877), ainsi que celui pour la correspondance anglaise de Bolton. M. Louis, le directeur du Journal des Postes, a également publié un Dictionnaire pour la correspondance secrète , contenant plus de 20,000 mots. B Dans la catégorie des dictionnaires chiffrés rentre le système qui consiste ax^^

- 56 — La méthode adoptée par les deux auteurs pour déjouer les calculs des déchiffreurs est très ingénieuse. Voici en quelques mots le procédé de M. Brunswick : on intervertit d'abord, et cela d'après une formule convenue. Tordre des chiffres de chaque groupe ou nombre, puis on augmente ou diminue ce nombre interverti d'un autre nombre ; ce dernier nombre constitue, avec la formule d'interversion, la clef de la combinaison» Prenons un exemple : je suppose qu'on veuille écrire avancez, et que le nombre correspondant donné par le dictionnaire soit 2143; ce nombre peut être interverti de 12 manières différentes : 2134, 4321, etc.; adoptons 213i. Si le nombre conventionnel à ajouter est 214, le chiffre final sera 2134 + 214 = 2348. Comme on a une grande latitude dans le choix du nombre h additionner ou à soustraire, il est impossible, tant qu'on n'a pas le dictionnaire, d'établir le moindre calcul sur les groupes ainsi obtenus. Mais une fois en possession du dictionnaire, il suffit de connaître deux groupes quelconques d'une dépêche pour retrouver aussitôt la clef de l'ensemble. Or, les circonstances dans lesquelles une dépêche a été écrite étant connues, il est très facile de reconnaître aux répétitions de certains groupes la présence de tel ou tel mot. Ainsi les quatre groupes suivants, 4213, 6555, 6555, 2140, placés au commencement d'un cryptogramme, contiendraient probablement le pronom nous, vous ou ce répété; il serait en effet difficile de combiner en français un commencement de phrase où un mot autre que nous, vous ou ce pftt se trouver répété au deuxième et au troisième rang; par exemple: Pouvezvous vous défendre? Devons-nous nous retirer ? Est-ce ce soir? Il serait trop long d'entrer dans tous les détails que peut com^ remplacer les mots les plus importants de la correspondance par d'aulres mots détoarnés de leur sens usuel. Ce procédé a été appliqué bien souvent, mais il ne peut avoir son coté pratique que dans des circonstances exceptionnelles. Dans la correspondance relative au complot organisé en I83i par le parti bonapartiste, on trouva une pièce écri'e de la main du prince Louis-Napoléon, qui contenait une liste des mots de convention adoptés par les conjurés pour désigner les personnes et les choses dont les noms devaient se reproduire le plus souvent : on désignait la reine Hortense par M. Antoine, le prince Louis- Napoléon par ilf"* Ckarhs, l'Angleterre par ilf"' Lir$on, les bonapartistes par Jlf"« Goek, Tarmée par Af' i« Amélie, la police par M. Pamberg, etc. (Voy. Mémoires de Gisquet, ancien préfet de police; 1840, p. 351.)

- 57 — porter le déchiffrement d'une dépêche cryplographiée avec un dictionnaire chiffré; je vais me borner à un seul exemple. Je suppose que certains indices m'autorisent à croire que dans une dépêche interceptée le groupe 9648 signifie colonel, el le groupe 7457 régiment. Voici comment je procéderai pour retrouver la formule de transposition ainsi que le nombre de clef. Admettons que le dictionnaire donne pour colonel et régiment les nombres 4913 et 2734; si je compare ces deux groupes aux nombres 9648 et 7457 du texte chiffré, je vois à la présence du 9 et du 7, restés intacts et placés au premier rang, que la clef n'est composée que de trois chiffres, et que, dans la permutation du nombre primitif, le deuxième chiffre a été porté au premier rang; de plus, le chiffre 6 du premier nombre indique clairement que la clef comporte une addition et non une soustraction. Les nombres 645 et 457 représentent donc la somme du nombre de clef, augmenté du nombre produit par la permutation de 413 et 234. Or, si je soustrais successivement des deux premiers nombres les six permutations obtenues, j'aurai pour les deux opérations une différence commune, qui représentera le nombre conventionnel, en même temps qu'elle fera connaître quelle a été la formule de permutation adoptée. 413 = 232 / 234 = 223 431 —214 1 243 = 214 . 143 = 502 „»- 423 = 034 ^*^-^34 = 811 *^' ^432 = 025 341 == 304 324 = 133 314 = 331 \ 342 = 115 Je dis que 214 est le nombre de clef, et i a d c la formule de permutation. L'opération ne peut donner de différence commune, qu'autant que les groupes du texte chiffré correspondent réellement aux mots supposés. De toutes les méthodes de cryptographie connues, ce sont assurément les dictionnaires chiffrés, du moins ceux qui sont basés sur un double principe de combinaison, comme ceux de Brunswick, Gallian et Niethe, qui garantissent le mieux le secret de la correspondance. Mais, à côté de cet avantage réel, ils présentent

 de si grands inconvénients dans leur application à la correspondance en temps de guerre, qu'on ne peut que s'étonner de la faveur dont ils ont joui jusqu'ici auprès de certains chefs de l'armée. Le plus grand reproche qu'on puisse faire aux dictionnaires chiffrés, c'est d'exiger le secret, et de constituer, par le fait même de leur adoption, un obstacle à la généralisation de la correspondance cryptographique. Cette condition du secret peut d'ailleurs causeries plus graves embarras. On rapporte que, le 8 janvier 1871, un cryptogramme, venu du quartier général du roi de Prusse, fut remis au général de Werder, qui ne put le déchiffrer immédiatement, le dictionnaire contenant la clef de la correspondance secrète se trouvant renfermé dans une valise placée sur une voiture éloignée. Pendant la guerre turco-russe, Selim -Pacha, sous-chef politique de Mehemet-Ali, s'absenta pour quefquesjout*s en septembre 1877, et emporta par mégarde le livre à déchiffrer. Le général en chef reçut pendant ce temps un grand nombre de dépêches cryptographiées qu'il lui fut impossible de lire. Maïs, outre qu'un vocabulaire imprimé peut être acheté par l'ennemi, et que l'adoption d'un dictionnaire doit nécessairement restreindre la correspondance secrète, il y a les plus grands inconvénients à faire dépendre la signification d'un mot ou d'une phrase entière de la bonne transcription d'un nombre; qu'un seul chiffre dans un groupe soit fautif, que le télégraphe ou le copiste mettent, par exemple, un 3 où il faut un 5 et le sens sera complètement changé. Généralement il n'y a qu'un simple contre-sens, ou une phrase incompréhensible; mais l'erreur peut avoir des suites plus fâcheuses, et il est arrivé plus d'une fois qu'un chiffre mal transmis ou mal lu a dénaturé complètement le sens d'un ordre ou d'un renseignement. S'il n'est pas rare de voir les personnes les plus habituées à manier des chiffres faire, dans un moment d'excitation, des erreurs dans une simple addition, rien n'est plus commun que de voir les employés du télégraphe se tromper dans la transmission des groupes chiffrés. Cet inconvénient, qui a été vivement senti pendant la guerre de 1870,. où la moitié des dépêches envoyées pai' l'autorité militaire aux préfets contenaient des parties illisibles, a encore été éprouvé à plusieurs reprises pendant notre campagne

~ de Tunisie ; plus d'une fois il a été impossible, au ministère de la guerre, de déchiffrer les dépêches de l'armée d'Afrique. Il n'y a pas bien longtemps, le ministère italien fut singulièrement intrigué par la nouvelle que lui transmit son ambassadeur de Saint-Pétersbourg, que le comte Andrassy était attendu dans la capitale russe. C'était tout simplement une erreur de chiffre, qui avait fait prendre le nom d'un attaché d'ambassade pour celui du célèbre homme d'État. Les dictionnaires chiffrés ne sont réellement d'un usage pratique et sûr que pour les chancelleries, dont le personnel, avec ses papiers et ses bagages, est inviolable dans tous les pays civilisés, et qui font chiffrer et déchiffrer leurs dépêches par des employés exercés à ce genre de travail, et ayant tous les moyens de vérifier, à leur aise, la transmission fidèle des correspondances. IV. LES CarPTOGRAPHES. Si les quelques essais de déchiffrement qui précèdent ont fait ressortir le côté faible de nos principaux systèmes de correspondance secrète, ils nous permettent également d'apprécier toutes les difficultés que présente l'élaboration d'un procédé cryptographique réalisant le desideratum que j'ai indiqué comme la base de toute méthode de cryptographie militaire, à savoir la non-nécessité du secret. Nous avons vu qu'il est impossible de remplacer les phrases et les mots par des groupes de lettres ou de chiffres sans créer par là même un dictionnaire qui demande le secret ; nous savons également que les procédés de transposition ne garantissent l'indéchiffrabililé qu'à la condition d'être basés sur quelque appareil secret; il s'ensuit, et j'insiste sur ce point, qu'il ne peut être établi de méthode, à la fois sûre et pratique, que sur une interversion conventionnelle des lettres. Il est vrai que, si le système est simple et repose sur quelque procédé régulier ou quelque combinaison systématique, il prête nécessairement le flanc aux calculs des déchiffreurs; si, d'autre part, il est tant soit peu compliqué et s'il comporte de nombreuses combinaisons, il demande le secret, ou bien il cesse d'être pratique.

-- 60 — Mais je crois que la solution du problème doit être cherchée dans l'application de quelque appareil mécanique, basé sur le principe d'interversion, c'est-à-dire dans l'emploi d'un cryptographe. Cette idée, d'ailleurs, n'est pas nouvelle. La scytale lacédémonienne; la planchette d'^Enéas (percée de vingt-quatre trous figurant les lettres de l'alphabet, trous à travers lesquels on passait une ficelle pour indiquer Tordre de succession des lettres de la missive secrète), le tonneau de Kessler, élaient de véritables cryptographes. Le premier modèle d'un cryptographe digne de ce nom se trouve dans le Traité des Chiffres de Porta ; c'est le système à cadran dont j'ai déjà eu l'occasion de parler. Le P. Kircher avait également imaginé un appareil mécanique qu'il avait appelé Arca ghtlotaclica * ; c'était une espèce de catalogue mobile, où les mots étaient classés dans un certain ordre correspondant aux diverses lettres de l'alphabet. Le télégraphe aérien de Chappe, comme le télégraphe Morse, sont encore de véritables cryptographes. Dans ces derniers temps, des appareils cryplographiques ont été imaginés par MM. Mouilleron, Vinay et Gaussin, Rondepierre, Wheatstone, Silas et autres. Le système de M. Mouilleron, dont on trouve la description dans V Exposé des applications de T électricité de Du Moncel*, est un mécanisme monté sur un pupitre, assez compliqué et ne présentant aucun avantage pratique. L'auteur ne paraît pas avoir fait une étude bien approfondie des chiffres à double clef, car son volumineux mécanisme n'aboutit qu'à nous donner un cryptogramme chiffré d'après le tableau de Vigenère. Il est facile de s'assurer de la parfaite exactitude de ce que j'avance, en cryptographiant l'exemple que donne Tauteur, La victoire est à nous, avec notre tableau de la page 26; avec la clef kzirh^ on obtiendra le mftme cryptogramme que celui qui est donné par l'appareil de M. Mouilleron, avec la clef /jarô», soit: * Voy. ScHOTT, Schola steganographiea, p. 27. > 3' édition, tome III, p. 529. 3 Kzirh n'est autre chose que Paris, écrit avec Tapliabet renversé.

 lavicl oiree staiious RZ I RHKZT RHKZ I RHK zT vzdzj dnqi lor'bpnyla = vzdzjdnqilorbrnyla Le cpyptographe de MM. Vinay et Gaussin est un mécanisme imprimeur au moyen duquel les dépêches sont à la fois imprimées et cryptographiées. Tout en étant plus portatif que le précédent, il est encore trop volumineux pour que son application soit possible en temps de guerre; au point de vue cryptographique proprement dit, il n'a d'ailleurs aucune valeur*. Le cryptographe ou phyrographe de M. Rondepierre est basé sur le système de transposition qui a été exposé à la page 13. Les colonnes verticales sont représentées par des baguettes en ivoire sur lesquelles sont tracées des divisions destinées h recevoir une lettre , on les transpose d'abord d'après une formule numérique, puis on inscrit au crayon la dépêche sur les baguettes mêmes. Celles-ci sont ensuite remises à leur place primitive, et les lettres sont copiées dans le nouvel ordre où elles se présentent. Le système est, à un certain point de vue, assez pratique, mais il n'offre qu'une sécurité relative*. Je ne dirai rien du cryptographe de M. Silas, ancien attaché à l'ambassade française de Vienne; quoique ce soit un travail sérieux et très bien combiné, il est trop compliqué, à mon sens, pour les usages de la guerre. De tous les cryptographes qui ont été inventés dans ces dernières années, celui de Wheatstone me paraît être, sinon le plus sûr, du moins le plus simple. Comme je n'ai pu me procurer un spécimen de l'appareil, j'en emprunte la description au Rapport de la Commission militaire sur l'Exposition universelle de 1867». 1 Voir DU MoNCBL, l&c, eil. s Pour des motifs particuliers, l'appareil n'a pu élre mis en vente, mais on en peut voir des spécimens chez M. Luard, gaînier, rue Dauphine, 16. 8 Cf. BoNTEMPS, Les systèmes télégi^phiqties, p. 257 , du Mongel, Exposé des appUealions de VéUctriciié, 1. III, p. 532. Wheatsthone a déchiffré, en i858, plusieurs lettres trè

The text on this page is estimated to be only 21.76% accurate

— 62 — < L'iDstmment très simple proposé par M. Wheatstone pour H écrire les dépfiches en chiffres est d'un emploi facile, dit le i< rapporteur, et assure le secret te plitu absolu (?) pour tous ceux rc qui no possèdent pas la clef du système. « Voici le principe d'après lequel on forme l'alphabet fictif " On choisit un mot quelconque pour servir de clef, France, [I exposition, projectile, etc. Supposons que l'on adopte le « projectile; on écrit ce mot en espaçant les lettres qui le com* posent, et au-dessous on écrit celles des lettres de l' alphabet V qu'il ne contient pas, dans un ordre régulier, comme suit: projectile a b dfg hkninq « En relevant les lettres dans l'ordre où elles se présentent 1 dans les colonnes verticales successives, on obtient l'a" ' conventionnel ci-après: pasrbuodvjfxegychztkwimlnq (1 Les lettres de l'alphabet conventionnel sont écrites sur un <. cercle="" en="" carton.="" ce="" s="" concentriquement="" sur="" un="" cadran="" m="" qui="" porte="" sa="" circonf="" alphabet="" c="" ordinaire="" compl="" par="" le="" signe="" d="" lequel="" on="" re="" vient="" la="" fin="" de="" chaque="" mot="" mais="" n="" pas="" dans="" chiffre.="" deux="" aiguilles="" et="" se="" meuvent="" simultan="" double="" avec="" des="" vitesses="" diff="" suivant="" une="" loi="" telle="" qu="" ramenant="" premi="" lettre="" b=""/>

— 63 t deuxième ne revient pas sur la même lettre, telle que V, indi« quée sur la figure, mais sur une autre lettre du cadran inté« rieur. » Lorsqu'on veut traduire une lettre quelconque en langue chiffrée, on fait avancer la grande aiguille jusqu'à la place occupée par cette lettre dans l'alphabet normal, et l'on marque la lettre sur laquelle s'est arrêtée la petite aiguille dans l'alphabet conventionnel. Le système comporte ainsi deux clefs : la disposition de l'alphabet cryptographique et le point de départ. Quoi qu'eu pense le colonel Laussedat, auteur du rapport que je viens de citer, les dépêches écrites avec le cryptographe de Wheatstonesont parfaitement déchiffrables. Le système ne donne qu'un nombre très limité d'alphabets différents; la même disposition alphabétique revient donc après un nombre d'arrêts déterminé. Supposons que ce soit après la 26® ou 30* lettre; je n'ai alors qu'à considérer le cryptogramme à déchiffrer comme étant écrit avec une clef de 26 ou 30 alphabets et à le mettre en colonnes par séries de 26 ou 30 chiffres, comme nous avons fait pour la dépêche de la page 41. Mais le plus grand inconvénient que présente l'appareil, c'est qu'il demande un secret absolu; car une fois tombé entre les mains de l'ennemi, il suffit de quelques tâtonnements sur les premières lettres de la dépêche pour retrouver le point initial. Lorsque plusieurs dépêches, écrites avec la même clef, ont été interceptées, il n'est plus besoin de posséder l'appareil pour en faire le déchiffrement. On applique le procédé que j'ai indiqué à la page 50. Il vient d'être présenté à la Commission de télégraphie militaire un nouveau système de cryptographe, qui me parait réaliser tous les desiderata que j'ai exposés en commençant : indéchiffrabilité complète, simplicité, non-nécessité du secret; des considérations de haute convenance m'empêchent d'en dire davantage pour le moment. Sans vouloir préjuger l'accueil que ce nouvel essai pourra trouver auprès des juges compétents, je tiens, en terminant, à insister sur ce point, que la valeur d'un système de cryptogra* phie destiné aux besoins de la guerre est en raison inverse du secret qu'exige son maniement ou sa composition. Il dépendra donc de l'Administration d'assurer l'avenir de la cryptographie

— 64 — militaire, en n'accordant ses suffrages qu'à Tinvention qui s'appuiera sur le principe que du Carltt, un des maîtres de notre art au XVII® siècle, avait inscrit comme devise en tête de sa méthode S principe qui résume d'ailleurs toute ma Ihè^e, à savoir qu'un chiffre n'est bon qu'autant qu'il reste indéchiffrable pour le maître lui-même qui l'a inventé : Ars ipn sécréta magisiro. i La Cryptographie, contenant une très subtile manière d'escrire secrètement, composée par maistre Jean Bobert du Garlet; 1644.

The text on this page is estimated to be only 2.15% accurate

^/ * • I f i. f l j i I L

The text on this page is estimated to be only 28.86% accurate

-^ ABONNEMENT POUR L'ANNÉE 1883 AU mm m Hds «mai (1) Dlreotenvii t Ii. BA.UDOI9I et <3* 59' ANNÉB (1883) Le Journal des Sciences militaires est le plus ancien recueil français de science, d'art et d'histoire militaires. Fondé en i8S5 par H. J. Gorréard, placé en 1872 sous la direction de M. J. Dumaine, il compte plus d'un demi- siècle d'existence. Les travaux qu'il a publiés, depuis cette nouvelle direction, l'ont mis aux premiers rangs de la pressé militaire de l'Europe; ils lui ont valu le suffrage d'un grand nombre d'officiers de toutes les nations et l'appui confraternel des organes des armées étrangères. L'élite des écrivains militaires lient à honneur de collaborer à eette publication, pour laquelle la direction s'est assuré le concours des spécialistes les plus estimés dans le monde militaire. (1) Parait le 15 de chaque mois en une livraison de au moins 10 feailles d^impression (160 pages), avec cartes, plans et dessins. Les douze livraisons de l'année forment quatre volumes compactes d'aviron 500 pages chacun. PRIX Itt L*ABOimBIIBHT : Un ai. Sic moli. Trois moli. Pour la France ....••• 35 fr. 20 fr. 10 fr. Pour l'Etranger (port simple) iO» 22» H» — (port double) . . . . . 45 • 24 • 12 • Nota. -^ Les abonnements ne sont reçus que partant dn premier Jour de chaque trimestre. Paris. —Imprimarie L. Baodori 6l G*, raa GhristfaM^ 1. . t; i \ -xr:^>;=k

The text on this page is estimated to be only 8.57% accurate

V. 'r i I ^ l EZU^

The text on this page is estimated to be only 9.00% accurate

N, à