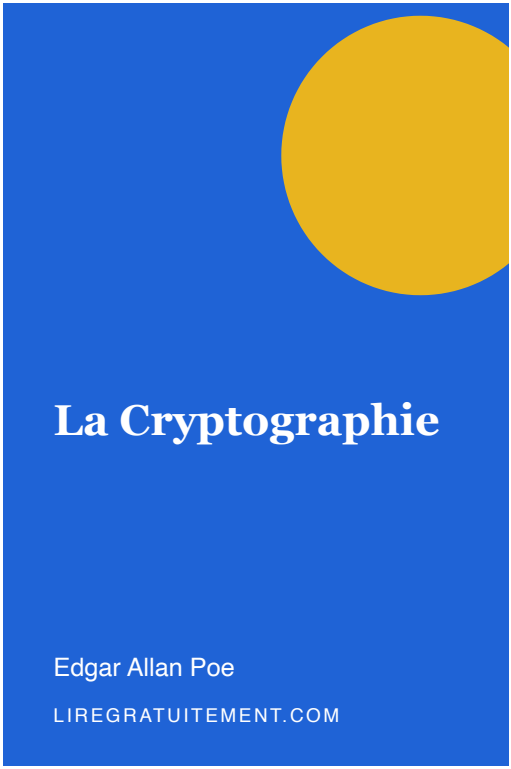


La Cryptographie

Edgar Allan Poe

LU AVEC LIREGRATUITEMENT.COM

Livre libre de droits, lisible gratuitement en ligne et en quinze minutes par jour.

LA CRYPTOGRAPHIE

Il nous est difficile d'imaginer un temps où n'ait pas existé, sinon la nécessité, au moins un désir de transmettre des informations d'individu à individu, de manière à déjouer l'intelligence du public ; aussi pouvons-nous hardiment supposer que l'écriture chiffrée remonte à une très haute antiquité. C'est pourquoi, De la Guilletière nous semble dans l'erreur, quand il soutient, dans son livre : « Lacédémone ancienne et moderne », que les Spartiates furent les inventeurs de la Cryptographie. Il parle des scytales, comme si elles étaient l'origine de cet art ; il n'aurait dû les citer que comme un des plus anciens exemples dont l'histoire fasse mention.

Les scytales étaient deux cylindres en bois, exactement semblables sous tous rapports. Le général d'une armée partant, pour une expédition, recevait des Éphores un de ces cylindres, et l'autre restait entre leurs mains. S'ils avaient quelque communication à se faire, une lanière étroite de parchemin était enroulée autour de la scytale, de manière à ce que les bords de cette lanière fussent exactement accolés l'un à l'autre. Alors on écrivait sur le parchemin dans le sens de la longueur du cylindre, après quoi on déroulait la bande, et on l'expédiait. Si par hasard, le message était intercepté, la lettre restait inintelligible pour ceux qui l'avaient saisie. Si elle arrivait intacte à sa destination, le destinataire n'avait qu'à en envelopper le second cylindre pour déchiffrer l'écriture. Si ce mode si simple de cryptographie est parvenu jusqu'à nous, nous le devons probablement plutôt aux

usages historiques qu'on en faisait qu'à toute autre cause. De semblables moyens de communication secrète ont dû être contemporains de l'invention des caractères d'écriture.

Il faut remarquer, en passant, que dans aucun des traités de Cryptographie venus à notre connaissance, nous n'avons rencontré, au sujet du chiffre de la scytale, aucune autre méthode de solution que celles qui peuvent également s'appliquer à tous les chiffres en général. On nous parle, il est vrai, de cas où les parchemins interceptés ont été réellement déchiffrés ; mais on a soin de nous dire que ce fut toujours accidentellement. Voici cependant une solution d'une certitude absolue. Une fois en possession de la bande de parchemin, on n'a qu'à faire faire un cône relativement d'une grande longueur — soit de six pieds de long — et dont la circonférence à la base soit au moins égale à la longueur de la bande. On enroulera ensuite cette bande sur le cône près de la base, bord contre bord, comme nous l'avons décrit plus haut ; puis, en ayant soin de maintenir toujours les bords contre les bords, et le parchemin bien serré sur le cône, on le laissera glisser vers le sommet. Il est impossible, qu'en suivant ce procédé, quelques-uns des mots, ou quelques-unes des syllabes et des lettres, qui doivent se rejoindre, ne se rencontrent pas au point du cône où son diamètre égale celui de la scytale sur laquelle le chiffre a été écrit. Et comme, en faisant parcourir à la bande toute la longueur du cône, on traverse tous les diamètres possibles, on ne peut manquer de réussir. Une fois que par ce moyen on a établi d'une façon certaine la circonférence de la scytale, on en fait faire une sur cette mesure, et l'on y applique le parchemin.

Il y a peu de personnes disposées à croire que ce n'est pas chose si facile que d'inventer une méthode d'écriture secrète qui

puisse défier l'examen. On peut cependant affirmer carrément que l'ingéniosité humaine est incapable d'inventer un chiffre qu'elle ne puisse résoudre. Toutefois ces chiffres sont plus ou moins facilement résolus, et sur ce point il existe entre diverses intelligences des différences remarquables. Souvent, dans le cas de deux individus reconnus comme égaux pour tout ce qui touche aux efforts ordinaires de l'intelligence, il se rencontrera que l'un ne pourra démêler le chiffre le plus simple, tandis que l'autre ne trouvera presque aucune difficulté à venir à bout du plus compliqué. On peut observer que des recherches de ce genre exigent généralement une intense application des facultés analytiques ; c'est pour cela qu'il serait très utile d'introduire les exercices de solutions cryptographiques dans les Académies, comme moyens de former et de développer les plus importantes facultés de l'esprit.

Supposons deux individus, entièrement novices en cryptographie, désireux d'entretenir par lettres une correspondance inintelligible à tout autre qu'à eux-mêmes, il est très probable qu'ils songeront du premier coup à un alphabet particulier, dont ils auront chacun la clef. La première combinaison qui se présentera à eux sera celle-ci, par exemple : prendre a pour z, b pour y, c pour x, d pour n, etc. etc. ; c'est-à-dire, renverser l'ordre des lettres de l'alphabet. À une seconde réflexion, cet arrangement paraissant trop naturel, ils en adopteront un plus compliqué. Ils pourront, par exemple, écrire les 13 premières lettres de l'alphabet sous les 13 dernières, de cette façon :

et, ainsi placés, a serait pris pour n et n pour a, o pour b et b pour o, etc., etc. Mais cette combinaison ayant un air de régulari-

té trop facile à pénétrer, ils pourraient se construire une clef tout à fait au hasard, par exemple :

Tant qu'une solution de leur chiffre ne viendra pas les convaincre de leur erreur, nos correspondants supposés s'en tiendront à ce dernier arrangement, comme offrant toute sécurité. Sinon, ils imagineront peut-être un système de signes arbitraires remplaçant les caractères usuels. Par exemple :

Une lettre composée de pareils signes aurait incontestablement une apparence fort rébarbative. Si toutefois ce système ne leur donnait pas pleine satisfaction, ils pourraient imaginer un alphabet toujours changeant, et le réaliser de cette manière :

Prenons deux morceaux de carton circulaires, différant de diamètre entre eux d'un demi-pouce environ. Plaçons le centre du plus petit carton sur le centre du plus grand, en les empêchant pour un instant de glisser ; le temps de tirer des rayons du centre commun à la circonférence du petit cercle, et de les étendre à celle du plus grand. Tirons vingt-six rayons, formant sur chaque carton vingt-six compartiments. Dans chacun de ces compartiments sur le cercle inférieur écrivons une des lettres de l'alphabet, qui se trouvera ainsi employé tout entier ; écrivons-les au hasard, cela vaudra mieux. Faisons la même chose sur le cercle supérieur. Maintenant faisons tourner une épingle à travers le centre commun, et laissons le cercle supérieur tourner avec l'épingle, pendant que le cercle inférieur est tenu immobile. Arrêtons la révolution du cercle supérieur, et écrivons notre lettre en prenant pour a la lettre du plus petit cercle qui correspond à l'a du plus grand, pour b, la lettre du plus petit cercle qui correspond au b du plus grand, et ainsi de suite. Pour qu'une lettre ainsi écrite puisse être lue par la personne à qui elle est destinée,

une seule chose est nécessaire, c'est qu'elle ait en sa possession des cercles identiques à ceux que nous venons de décrire, et qu'elle connaisse deux des lettres (une du cercle inférieur et une du cercle supérieur) qui se trouvaient juxtaposées, au moment où son correspondant a écrit son chiffre. Pour cela, elle n'a qu'à regarder les deux lettres initiales du document qui lui serviront de clef. Ainsi, en voyant les deux lettres a m au commencement, elle en conclura qu'en faisant tourner ses cercles de manière à faire coïncider ces deux lettres, elle obtiendra l'alphabet employé.

Àpremière vue, ces différents modes de cryptographie ont une apparence de mystère indéchiffrable. Il paraît presque impossible de démêler le résultat de combinaisons si compliquées. Pour certaines personnes en effet ce serait une extrême difficulté, tandis que pour d'autres qui sont habiles à déchiffrer, de pareilles énigmes sont ce qu'il y a de plus simple. Le lecteur devra se mettre dans la tête que tout l'art de ces solutions repose sur les principes généraux qui président à la fonction du langage lui-même, et que par conséquent il est entièrement indépendant des lois particulières qui régissent un chiffre quelconque, ou la construction de sa clef. La difficulté de déchiffrer une énigme cryptographique n'est pas toujours en rapport avec la peine qu'elle a coûtée, ou l'ingéniosité qu'a exigée sa construction. La clef, en définitive, ne sert qu'à ceux qui sont au fait du chiffre ; la tierce personne qui déchiffre n'en a aucune idée. Elle force la serrure. Dans les différentes méthodes de cryptographie que j'ai exposées, on observera qu'il y a une complication graduellement croissante. Mais cette complication n'est qu'une ombre : elle n'existe pas en réalité. Elle n'appartient qu'à la composition du chiffre, et ne porte en aucune façon sur sa solution. Le dernier

système n'est pas du tout plus difficile à déchiffrer que le premier, quelle que puisse être la difficulté de l'un ou de l'autre.

En discutant un sujet analogue dans un des journaux hebdomadaires de cette ville, il y a dix-huit mois environ, l'auteur de cet article a eu l'occasion de parler de l'application d'une méthode rigoureuse dans toutes les formes de la pensée, — des avantages de cette méthode — de la possibilité d'en étendre l'usage à ce que l'on considère comme les opérations de la pure imagination — et par suite de la solution de l'écriture chiffrée. Il s'est aventuré jusqu'à déclarer qu'il se faisait fort de résoudre tout chiffre, analogue à ceux dont je viens de parler, qui serait envoyé à l'adresse du journal. Ce défi excita, de la façon la plus inattendue, le plus vif intérêt parmi les nombreux lecteurs de cette feuille. Des lettres arrivèrent de toutes parts à l'éditeur ; et beaucoup de ceux qui les avaient écrites étaient si convaincus de l'impénétrabilité de leurs énigmes qu'ils ne craignirent pas de l'engager dans des paris à ce sujet. Mais en même temps, ils ne furent pas toujours scrupuleux sur l'article des conditions. Dans beaucoup de cas les cryptographies sortaient complètement des limites fixées. Elles employaient des langues étrangères. Les mots et les phrases se confondaient sans intervalles. On employait plusieurs alphabets dans un même chiffre. Un de ces messieurs, d'une conscience assez peu timorée, dans un chiffre composé de barres et de crochets, étrangers à la plus fantastique typographie, alla jusqu'à mêler ensemble au moins sept alphabets différents, sans intervalles entre les lettres, ou même entre les lignes. Beaucoup de ces cryptographies étaient datées de Philadelphie, et plusieurs lettres qui insistaient sur le pari furent écrites par des citoyens de cette ville. Sur une centaine de chiffres, peut-être reçus en tout, il n'y en eut qu'un que nous ne parvînmes pas immédia-

tement à résoudre. Nous avons démontré que ce chiffre était une imposture — c'est-à-dire un jargon composé au hasard et n'ayant aucun sens. Quant à l'épître des sept alphabets, nous eûmes le plaisir d'ahurir son auteur par une prompte et satisfaisante traduction.

Le journal en question fut, pendant plusieurs mois, grandement occupé par ces solutions hiéroglyphiques et cabalistiques de chiffres qui nous venaient des quatre coins de l'horizon. Cependant à l'exception de ceux qui écrivaient ces chiffres, nous ne croyons pas qu'on eût pu, parmi les lecteurs du journal, en trouver beaucoup qui y vissent autre chose qu'une hâblerie fieffée. Nous voulons dire que personne ne croyait réellement à l'authenticité des réponses. Les uns prétendaient que ces mystérieux logogriphes n'étaient là que pour donner au journal un air drôle, en vue d'attirer l'attention. Selon d'autres, il était plus probable que non seulement nous résolvions les chiffres, mais encore que nous composions nous-même les énigmes pour les résoudre. Comme les choses en étaient là, quand on jugea à propos d'en finir avec cette diablerie, l'auteur de cet article profita de l'occasion pour affirmer la sincérité du journal en question, — pour repousser les accusations de mystification dont il fut assailli, — et pour déclarer en son propre nom que les chiffres avaient tous été écrits de bonne foi, et résolus de même.

Voici un mode de correspondance secrète très ordinaire et assez simple. Une carte est percée à des intervalles irréguliers de trous oblongs, de la longueur des mots ordinaires de trois syllabes du type vulgaire. Une seconde carte est préparée identiquement semblable. Chaque correspondant a sa carte. Pour écrire une lettre, on place la carte percée qui sert de clef sur le papier, et

les mots qui doivent former le vrai sens s'écrivent dans les espaces libres laissés par la carte.

Puis on enlève la carte, et l'on remplit les blancs de manière à obtenir un sens tout à fait différent du véritable. Le destinataire, une fois le chiffre reçu, n'a qu'à y appliquer sa propre carte, qui cache les mots superflus, et ne laisse paraître que ceux qui ont du sens. La principale objection à ce genre de cryptographie, c'est la difficulté de remplir les blancs de manière à ne pas donner à la pensée un tour peu naturel. De plus, les différences d'écriture qui existent entre les mots écrits dans les espaces laissés par la carte, et ceux que l'on écrit une fois la carte enlevée, ne peuvent manquer d'être découvertes par un observateur attentif.

On se sert quelquefois d'un paquet de cartes de cette façon : Les correspondants s'entendent, tout d'abord, sur un certain arrangement du paquet. Par exemple : on convient de faire suivre les couleurs dans un ordre naturel, les piques au dessus, les cœurs ensuite, puis les carreaux et les trèfles. Cet arrangement fait, on écrit sur la première carte la première lettre de son épître, sur la suivante, la seconde, et ainsi de suite, jusqu'à ce qu'on ait épuisé les cinquante-deux cartes. On mêle ensuite le paquet d'après un plan concerté à l'avance. Par exemple : on prend les cartes du talon et on les place dessus, puis une du dessus que l'on met au talon, et ainsi de suite, un nombre de fois déterminé. Cela fait, on écrit de nouveau cinquante-deux lettres, et l'on suit la même marche jusqu'à ce que la lettre soit écrite. Le correspondant, ce paquet reçu, n'a qu'à placer les cartes dans l'ordre convenu, et lire lettre par lettre les cinquante-deux premiers caractères. Puis il mêle les cartes de la manière susdite, pour déchiffrer la seconde série et ainsi de suite jusqu'à la fin. Ce que l'on

peut objecter contre ce genre de cryptographie, c'est le caractère même de la missive. Un paquet de cartes ne peut manquer d'éveiller le soupçon, et c'est une question de savoir s'il ne vaudrait pas mieux empêcher les chiffres d'être considérés comme tels que de perdre son temps à essayer de les rendre indéchiffrables, une fois interceptés. L'expérience démontre que les cryptographies les plus habilement construites, une fois suspectées, finissent toujours par être déchiffrées.

On pourrait imaginer un mode de communication secrète d'une sûreté peu commune ; le voici : les correspondants se munissent chacun de la même édition d'un livre — l'édition la plus rare est la meilleure — comme aussi le livre le plus rare. Dans la cryptographie, on emploie les nombres, et ces nombres renvoient à l'endroit qu'occupent les lettres dans le volume. Par exemple — on reçoit un chiffre qui commence ainsi : 121-6-8. On n'a alors qu'à se reporter à la page 121, sixième lettre à gauche de la page à la huitième ligne à partir du haut de la page. Cette lettre est la lettre initiale de l'épître — et ainsi de suite. Cette méthode est très sûre ; cependant il est encore possible de déchiffrer une cryptographie écrite d'après ce plan — et d'autre part une grande objection qu'elle encourt, c'est le temps considérable qu'exige sa solution, même avec le volume-clef.

Il ne faudrait pas supposer que la cryptographie sérieuse, comme moyen de faire parvenir d'importantes informations, a cessé d'être en usage de nos jours. Elle est communément pratiquée en diplomatie ; et il y a encore aujourd'hui des individus, dont le métier est celui de déchiffrer les cryptographies sous l'œil des divers gouvernements. Nous avons dit plus haut que la solution du problème cryptographique met singulièrement en jeu

l'activité mentale, au moins dans les cas de chiffres d'un ordre plus élevé. Les bons cryptographes sont rares, sans doute ; aussi leurs services, quoique rarement réclamés, sont nécessairement bien payés.

Nous trouvons un exemple de l'emploi moderne de l'écriture chiffrée dans un ouvrage publié dernièrement par MM. Lea et Blanchard de Philadelphie : — « Esquisses des hommes remarquables de France actuellement vivants. » Dans une notice sur Berryer, il est dit qu'une lettre dressée par la Duchesse de Berri aux Légitimistes de Paris pour les informer de son arrivée, était accompagnée d'une longue note chiffrée, dont on avait oublié d'envoyer la clef. « L'esprit pénétrant de Berryer, » dit le biographe, « l'eut bientôt découverte. C'était cette phrase substituée aux 24 lettres de l'alphabet : — « Le gouvernement provisoire. »

Cette assertion que « Berryer eut bientôt découvert la phrase-clef, » prouve tout simplement que l'auteur de ces notices est de la dernière innocence en fait de science cryptographique. M. Berryer sans aucun doute arriva à découvrir la clef ; mais ce ne fut que pour satisfaire sa curiosité, une fois l'énigme résolue. Il ne se servit en aucune façon de la clef pour la déchiffrer. Il força la serrure.

Dans le compte-rendu du livre en question (publié dans le numéro d'avril de ce Magazine) nous faisions ainsi allusion à ce sujet.

« Les mots « Le gouvernement provisoire » sont des mots français, et la note chiffrée s'adressait à des Français. On pourrait supposer la difficulté beaucoup plus grande, si la clef avait été en langue étrangère ; cependant le premier venu qui voudra s'en

donner la peine n'a qu'à nous adresser une note, construite dans le même système, et prendre une clef française, italienne, espagnole, allemande, latine ou grecque (ou en quelque dialecte que ce soit de ces langues) et nous nous engageons à résoudre l'énigme. »

Ce défi ne provoqua qu'une seule réponse, incluse dans la lettre suivante. Tout ce que nous reprochons à cette lettre, c'est que celui qui l'a écrite ait négligé de nous donner son nom en entier. Nous le prions de vouloir bien le faire au plus tôt, afin de nous laver auprès du public du soupçon qui s'attacha à la cryptographie du journal dont j'ai parlé plus haut — que nous nous donnions à nous-même des énigmes à déchiffrer. Le timbre de la lettre porte Stonington, Conn.

S...., Ct, 21 Juin, 1841.

Àl'éditeur du Graham's Magazine.

Monsieur, — Dans votre numéro d'avril, où vous rendez compte de la traduction par M. Walsh des « Esquisses des hommes remarquables de France actuellement vivants », vous invitez vos lecteurs à vous adresser une note chiffrée, « dont la phrase-clef serait empruntée aux langues française, italienne, espagnole, allemande, latine ou grecque », et vous vous engagez à la résoudre. Vos remarques ayant appelé mon attention sur ce genre de cryptographie, j'ai composé pour mon propre amusement les exercices suivants. Dans le premier la phrase-clef est en anglais — dans le second, en latin. Comme je n'ai pas vu (par le numéro de Mai) que quelqu'un de vos correspondants ait répondu à votre offre, je prends la liberté de vous envoyer ces chiffres,

sur lesquels, si vous jugez qu'ils en vaillent la peine, vous pourrez exercer votre sagacité.

Respectueusement à vous,

S. D. L.

N 1.

Cauhiif aud ftd sdftirf ithot tacd wdde rdchtdr tiu fuaefshffheo fdoudf hetiusafhie tuis ied herhchriai fi aeiftdu wn sdaef it iuhfheo hiidohwid fi aen deodsf ths tiu itis hf iaf iuhoheaiin rdff hedr ; aer ftd auf it ftif fdoudfin oissiehoafheo hefdiihodeod taf wdde odeduaiin fdusdr ouasfiouastn. Saen fsdohdf it fdoudf iuhfheo idud weiie fi ftd aeohdeff ; fisdfhsdf a fiacdf tdar iaf fiacdr aer ftd ouiie iuhffde isie ihft fisd herdihwid oiiiiuheo tiihr, atfdu ithot ftd tahu wdheo sdushffdr fi ouii aoahe, hetiusafhie oiiir wd fuaefshffdr ihft ihffid raeodu ftaf rhfoicdun iiir defid iefhi ftd aswiiafiun dshffid fatdin udaotdrhff rdffheafhie. Ounsfiouastn tiidcdu siud suisduin dswuaodf ftifd sirdf it iuhfheo ithot aud uderdudr idohwid iein wn sdaef it fisd desiacafium wdn ithot sawdf weiie ftd udai fhoehthoafhie it ftd ohstduf dssiindr fi hff siffdffiu.

N 2.

Ofoiioiiaso ortsii sov eodisoioe afduiostifoi ft iftvi si tri oistoiv oiniafetsorit ifeov rsri afotiiiiv ridiiot irio rivvio eovit atrotfetsoria aioriti iitri tf oitovin tri aerifei ioreitit sov usttoi oioittstifo dfti afdooitior trso ifeov tri dfit otftfeov softriedi ft oistoiv oriofiforiti suiteii viireiiitifoi it tri iarfoisiti iiti trir uet otiiiotiv uitfti rid io tri eoviieeiiiv rfasiieostr ft rii dftrit tfoeei.

La solution du premier de ces chiffres nous a donné assez de peine. Le second nous a causé une difficulté extrême, et ce n'est

qu'en mettant en jeu toutes nos facultés que nous avons pu en venir à bout. Le premier se lit ainsi :

« Various are the methods which have been devised for transmitting secret information from one individual to another by means of writing, illegible to any except him for whom it was originally destined ; and the art of thus secretly communicating intelligence has been generally termed cryptography. Many species of secret writing were known to the ancients. Sometimes a slave's head was shaved and the crown written upon with some indelible colouring fluid ; after which the hair being permitted to grow again, information could be transmitted with little danger that discovery would ensue until the ambulatory epistle safely reached its destination. Cryptography, however pure, properly embraces those modes of writing which are rendered legible only by means of some explanatory key which makes known the real signification of the ciphers employed to its possessor. »

La phrase-clef de cette cryptographie est : — « A word to the wise is sufficient. »

La seconde se traduit ainsi :

« Nonsensical phrases and unmeaning combinations of words, as the learned lexicographer would have confessed himself, when hidden under cryptographic ciphers, serve to perplex the curious enquirer, and baffle penetration more completely than would the most profound apophtegms of learned philosophers. Abstruse disquisitions of the scoliasts were they but presented before him in the undisguised vocabulary of his mother tongue… »

Le sens de la dernière phrase, on le voit, est suspendu. Nous nous sommes attaché à une stricte épellation. Par mégarde, la lettre d a été mise à la place de l dans le mot perplex.

La phrase-clef est celle-ci : « Suaviter in modo, fortiter in re. »

Dans la cryptographie ordinaire, comme on le verra par la plupart de celles dont j'ai donné des exemples, l'alphabet artificiel dont conviennent les correspondants s'emploie lettre pour lettre, à la place de l'alphabet usuel. Par exemple — deux personnes veulent entretenir une correspondance secrète. Elles conviennent avant de se séparer que le signe

Il s'agit de communiquer cette note :

« We must see you immediately upon a matter of great importance. Plots have been discovered, and the conspirators are in our hands. Hasten ! »

On écrirait ces mots :

§. °£][ ].. ¡†£ ?°°.*?)[.&¡ £‡†‘) °)[[.☞ †, ;☞.)[?°‡†☞[)‘—. ‡&†[] :)£. (..‘ *&]—†£.☞.*)‘* [:. —†‘]‡?☞)[†☞])☞. ?‘ †£☞ :)‘*] :)][.‘

Voilà qui a certainement une apparence fort compliquée, et paraîtrait un chiffre fort difficile à quiconque ne serait pas versé, en cryptographie. Mais on remarquera que a, par exemple, n'est jamais représenté par un autre signe que), b par un autre signe que (et ainsi de suite. Ainsi, par la découverte, accidentelle ou non, d'une seule des lettres, la personne interceptant la missive aurait déjà un grand avantage, et pourrait appliquer cette connaissance à tous les cas où le signe en question est employé dans le chiffre.

D'autre part, les cryptographies, qui nous ont été envoyées par notre correspondant de Stonington, identiques en construction avec le chiffre résolu par Berryer, n'offrent pas ce même avantage.

Examinons par exemple la seconde de ces énigmes. Sa phrase-clef est : « Suaviter in modo, fortiter in re. »

Plaçons maintenant l'alphabet sous cette phrase, lettre sous lettre ; nous aurons :

De cette façon n représente deux lettres et e, o et t en représentent chacune trois, tandis que i et r n'en représentent pas moins de quatre. Treize caractères seulement jouent le rôle de tout l'alphabet. Il en résulte que le chiffre a l'air d'être un pur mélange des lettres e, o, t, r et i, cette dernière lettre prédominant surtout, grâce à l'accident qui lui fait représenter les lettres qui par elles-mêmes prédominent extraordinairement dans la plupart des langues — à savoir e et i.

Supposons une lettre de ce genre interceptée et la phrase-clef inconnue, on peut imaginer que l'individu qui essaiera de la déchiffrer arrivera, en le devinant, ou par tout autre moyen, à se convaincre qu'un certain caractère (i par exemple) représente la lettre e. En parcourant la cryptographie pour se confirmer dans cette idée, il n'y rencontrera rien qui n'en soit au contraire la négation. Il verra ce caractère placé de telle sorte qu'il ne peut représenter un e. Par exemple, il sera fort embarrassé par les quatre i formant un mot entier, sans l'intervention d'aucune autre lettre, cas auquel, naturellement, ils ne peuvent tous être des e. On remarquera que le mot wise peut ainsi être formé. Nous le remarquons, nous, qui sommes en possession de la clef ; mais

à coup sûr on peut se demander comment, sans la clef, sans connaître une seule lettre du chiffre, il serait possible à celui qui a intercepté la lettre de tirer quelque chose d'un mot tel que iiii.

Mais voici qui est plus fort. On pourrait facilement construire une phrase-clef, où un seul caractère représenterait six, huit ou dix lettres. Imaginons-nous le mot iiiiiiiiii se présentant dans une cryptographie à quelqu'un qui n'a pas la clef, ou si cette supposition est par trop scabreuse, supposons en présence de ce mot la personne même à qui le chiffre est adressé, et en possession de la clef. Que fera-t-elle d'un pareil mot ? Dans tous les manuels d'Algèbre on trouve la formule précise pour déterminer le nombre d'arrangements selon lesquels un certain nombre de lettres m et n peuvent être placées. Mais assurément aucun de mes lecteurs ne peut ignorer quelles innombrables combinaisons on peut faire avec ces dix i. Et cependant, à moins d'un heureux accident, le correspondant qui recevra ce chiffre devra parcourir toutes les combinaisons avant d'arriver au vrai mot, et encore quand il les aura toutes écrites, sera-t-il singulièrement embarrassé pour choisir le vrai mot dans le grand nombre de ceux qui se présenteront dans le cours de son opération.

Pour obvier à cette extrême difficulté en faveur de ceux qui sont en possession de la clef, tout en la laissant entière pour ceux à qui le chiffre n'est pas destiné, il est nécessaire que les correspondants conviennent d'un certain ordre, selon lequel on devra lire les caractères qui représentent plus d'une lettre ; et celui qui écrit la cryptographie devra avoir cet ordre présent à l'esprit. On peut convenir, par exemple, que la première fois que l'i se présentera dans le chiffre, il représentera le caractère qui se trouve sous le premier i dans la phrase-clef, et la seconde fois, le second

caractère correspondant au second i de la clef, etc., etc. Ainsi il faudra considérer quelle place chaque caractère du chiffre occupe par rapport au caractère lui-même pour déterminer sa signification exacte.

Nous disons qu'un tel ordre convenu à l'avance est nécessaire pour que le chiffre n'offre pas de trop grandes difficultés même à ceux qui en possèdent la clef. Mais on n'a qu'à regarder la cryptographie de notre correspondant de Stonington pour s'apercevoir qu'il n'y a observé aucun ordre, et que plusieurs caractères y représentent, dans la plus absolue confusion, plusieurs autres. Si donc, au sujet du gant que nous avons jeté au public en avril, il se sentait quelque velléité de nous accuser de fanfaronnade, il faudra cependant bien qu'il admette que nous avons fait honneur et au delà à notre prétention. Si ce que nous avons dit alors n'était pas dit suaviter in modo, ce que nous faisons aujourd'hui est au moins fait fortiter in re.

Dans ces rapides observations nous n'avons nullement essayé d'épuiser le sujet de la cryptographie ; un pareil sujet demanderait un in-folio. Nous n'avons voulu que mentionner quelques-uns des systèmes de chiffres les plus ordinaires. Il y a deux mille ans, Æneas Tacticus énumérait vingt méthodes distinctes, et l'ingéniosité moderne a fait faire à cette science beaucoup de progrès. Ce que nous nous sommes proposé surtout, c'est de suggérer des idées, et peut-être n'avons-nous réussi qu'à fatiguer le lecteur. Pour ceux qui désireraient de plus amples informations à ce sujet, nous leur dirons qu'il existe des traités sur la matière par Trithemius, Cap. Porta, Vignère, et le P. Nicéron. Les ouvrages des deux derniers peuvent se trouver, je crois, dans la bibliothèque de Harvard University. Si toutefois on s'attendait à ren-

contrer dans ces Essais des règles pour la solution du chiffre, on pourrait se trouver fort désappointé. En dehors de quelques aperçus touchant la structure générale du langage, et de quelques essais minutieux d'application pratique de ces aperçus, le lecteur n'y trouvera rien à retenir qu'il ne puisse trouver dans son propre entendement.

Sources et licence

Texte : https://fr.wikisource.org/wiki/La_Cryptographie. Domaine public ; transcription Wikisource CC BY-SA 4.0. Mise en forme : liregratuitement.-com. Tout ce que nous ajoutons reste libre.