BULLETIN DE L'A.R.C.

AMICALE DES RÉSERVISTES DU CHIFFRE

Nouvelle série - 10e Année

— Décembre 1963 —

APERÇUS SUR LA CRYPTOGRAPHIE MÉDIÉVALE

par Gérard de Sède.

Messieurs,

Sans l'amabilité ou, pour mieux dire, sans l'excessive indulgence des organisateurs de votre congrès, ma présence parmi vous aujourd'hui n'aurait aucune justification. En effet, non seulement je n'ai jamais appartenu au Chiffre, ni à titre militaire ni à titre civil, mais encore je ne suis même pas un décrypteur amateur. Je suis donc ici dans la position peu confortable du profane parmi des initiés, et si je suis très heureux d'être votre invité, ce n'est pas que je pense vous instruire : c'est que je pense m'instruire auprès de vous. Je suis sûr d'apprendre lors de la discussion qui s'engagera tout à l'heure.

Après cet aveu d'ignorance, vous vous demandez sûrement ce que je peux bien avoir à faire avec la cryptographie. Voici : j'ai rencontré la cryptographie en explorant des domaines où j'étais bien loin de penser la trouver : l'histoire et l'archéologie médiévales. En découvrant dans ces domaines des problèmes de cryptographie, j'ai été extrêmement surpris. Peut-être qu'en bons initiés vous sourirez de ma surprise de profane, mais peut-être aussi, qui sait, partagerez-vous cette surprise en constatant que votre discipline, de très loin plus antique que ne le croit le public, avait jadis un champ d'application beaucoup plus vaste qu'aujourd'hui.

« Celui-là est insensé qui n'écrit pas ce qu'il veut conserver secret en le cachant au vulgaire, de manière à n'être compris que des plus studieux et des plus savants. »

Cette phrase fut écrite au XIII^e^ siècle par le moine anglais Roger BACON, philosophe et alchimiste auquel on doit notamment la réinvention de la poudre à canon. A elle seule, elle atteste l'existence d'une cryptographie médiévale.

Mieux encore : on peut affirmer que le Moyen Age fut l'âge d'or de la cryptographie ; car si celle-ci était alors moins savante, elle était beaucoup plus répandue qu'aujourd'hui. Presque tout le monde chiffrait et on chiffrait presque tout. (Bien entendu, je n'emploie pas ici le terme « chiffrer » au sens strict, car la cryptographie médiévale comprenait, comme nous le verrons, non seulement des chiffrements proprement dits, mais aussi des codages et l'emploi de langages conventionnels).

De nos jours, les militaires, les diplomates et les négociants sont presque seuls à chiffrer. Pour autant qu'on sache, le chiffre militaire n'était guère en usage au Moyen Age ; quant au chiffre diplomatique,

*

on sait par les travaux de l'Allemand Aloys MEISTER (1) que la Curie pontificale était, à cette époque, seule à l'utiliser. Par contre, la cryptographie était employée par toutes sortes de gens qui n'en font aujourd'hui aucun usage : presque tous les corps de métier, à commencer par les bâtisseurs, clergé, savants, philosophes, artistes. Elle était aussi employée, et de main de maître, par les membres de deux institutions défuntes dont les activités ont toujours gardé un certain mystère : ces moines, soldats, diplomates, bâtisseurs et savants qu'étaient les Templiers ; ces officiers d'état-civil d'un genre très spécial qu'étaient les hérauts d'armes.

Aussi, loin de se limiter comme de nos jours aux informations d'ordre militaire, diplomatique ou commercial, la cryptographie médiévale s'étendait à toutes sortes d'informations, d'écrits ou d'images que nous diffusons aujourd'hui en clair. On « chiffrait » des théories religieuses ou philosophiques, des découvertes scientifiques, des œuvres littéraires et des tableaux. Aussi étrange que cela puisse nous paraître, les bâtisseurs chiffraient même des monuments et les hérauts d'armes des renseignements généalogiques ou biographiques.

Ces usages de la cryptographie, surtout les deux derniers, semblent invraisemblables : en effet, à première vue, on conçoit mal ce que peuvent être un monument ou une généalogie chiffrés. Pour y croire, vous désirez sûrement des preuves, c'est-à-dire des exemples. Permettez-moi de vous demander quelques instants de patience. En effet, l'examen de ces exemples n'est guère séparable de l'examen des méthodes cryptographiques du Moyen Age, et l'examen de ces méthodes elles-mêmes exige qu'on rappelle d'abord brièvement l'état d'esprit de cette époque, profondément différente de la nôtre.

***

Pour nous, la religion n'est qu'un domaine de la vie sociale parmi beaucoup d'autres ; mais au Moyen Age, une vision religieuse du monde présidait à l'ensemble des activités humaines : à l'économie et à l'organisation des métiers, à la politique et à l'organisation des pouvoirs, à la vie intellectuelle sous toutes ses formes et à la sensibilité sous tous ses aspects. De plus, il n'existait alors qu'une Eglise, dont la doctrine avait force de loi.

Or la religion, c'est avant tout l'affirmation qu'il existe un monde caché derrière notre monde visible et que l'interprétation des symboles permet de découvrir ce monde caché. C'est pourquoi le grand médiévaliste Etienne GILSON a pu écrire : « Comprendre et expliquer une chose consistaient pour le penseur de cette époque à montrer qu'elle était le symbole ou le signe d'une réalité plus profonde, qu'elle proclamait ou signifiait quelque chose d'autre. »

Ainsi le monde dans lequel il vit n'est en quelque sorte pour l'homme du Moyen Age que le cryptogramme d'un monde inconnu dont les clefs sont les symboles. Aussi, face à ce monde, son attitude

---

(1) Aloys MEISTER : *Die Geheimschrift im Dienste der papstlichen Kurie von ihren Anfängen bis zum Ende des XVI. Jahrhunderte.* 1906. (La cryptographie dans les services de la curie pontificale des origines à la fin du XVIe siècle).

est-elle beaucoup moins celle d'un savant que celle d'un décrypteur ; car il ne cherche pas comme le savant à remonter de l'effet à la cause : il cherche comme le décrypteur à remonter du signe à la signification.

Mais l'Eglise — dont le chef, ne l'oublions pas, a la double clef pour emblème — était seule à détenir le fameux « pouvoir des clefs » ; c'est-à-dire qu'elle se réservait le monopole de l'interprétation symbolique dont elle écartait avec rigueur les laïcs, allant jusqu'à interdire à ceux-ci de lire les *Saintes Ecritures.*

Aussi, science tantôt sacrée tantôt maudite, l'interprétation des symboles était-elle tenue secrète non seulement par l'Eglise qui voulait être seule à la pratiquer mais aussi par tous ceux qui la pratiquaient malgré l'Eglise.

Dans un monde et une société entièrement peuplés de symboles, cela faisait au total beaucoup de gens, et beaucoup de choses à cacher !

***

Ici, peut-être me reprocherez-vous de m'écarter de mon sujet en glissant insensiblement de la cryptographie au symbolisme.

Certes, on ne saurait en aucune façon confondre les deux. Mais entre le symbolisme et la cryptographie il n'existe pas de barrière infranchissable tandis qu'il existe de nombreux rapports, sur lesquels il n'est peut-être pas inutile d'insister.

Sans entrer dans des considérations théoriques d'un grand intérêt mais qui n'ont pas leur place ici, remarquons d'abord que toute écritude est un système de symboles. Or, si les lettres et les chiffres nous apparaissent comme des formes choisies arbitrairement et de façon purement conventionnelle, c'est là une pure illusion, très vite dissipée quand on se penche sur l'origine des diverses écritures.

Quand il appelle, par exemple, le chiffre 33 « les deux bossus », le langage populaire est plus près que nous de la vérité : en effet, le symbolisme de l'écriture est figuratif. Ceci se passe de commentaires quand il s'agit de l'écriture hiéroglyphique des Egyptiens ou de l'écriture idéographique des Chinois. Mais ce qu'on sait moins, c'est que l'alphabet grec et l'alphabet latin qui sont encore le nôtre dérivent du même principe : en effet c'est le symbolisme astrologique qui, dans ces alphabets, a présidé au choix des caractères ; car ces derniers, pour la plupart, ne sont pas autre chose que les signes du Zodiaque : *alpha* et *gamma* le Bélier, *pi* Ophiucus, *sigma* le Cancer, A majuscule le Taureau, *m* minuscule le Scorpion, etc.

En hébreu, chaque lettre est associée à la fois à une valeur numérique distincte de son numéro d'ordre dans l'alphabet et à un concept : par exemple, la lettre *beth* (B) a une valeur numérique de 2 et le mot « maison » se dit *beth.* Or, ce sont ces caractéristiques qui, dès le XIII^e^ siècle et peut-être plus tôt, ont servi de point de départ au système des kabbalistes.

Considérée comme système de symboles, toute graphie est donc, au sens large, une cryptographie. Au début de son livre *La cryptographie,* Rémy CEILLIER écrit : « Dans les sociétés illettrées, tout mode d'écriture, réservé à de rares adeptes, était déjà pour tous les

autres une véritable cryptographie » (1). C'est pourquoi l'écriture et la création des images furent longtemps des sciences secrètes, réservées aux uniques détenteurs d'une autre science secrète, celle des symboles, — c'est-à-dire à la caste sacerdotale, qui formait ainsi une véritable cryptocratie. Rappelons seulement à ce sujet que « hiéroglyphe » signifie « écriture sacrée » et que la Bible (*Exode*, XX, 4.) formule l'interdiction suivante : « Tu ne feras pas d'image taillée ni aucune figure de ce qui est en haut dans le ciel, ou de ce qui est en bas sur la terre, ou de ce qui est dans les eaux au-dessous de la terre. »

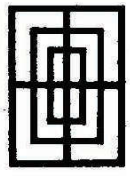
Certes, il existe une diffférence capitale entre l'interprétation des symboles et la cryptographie proprement dite : c'est qu'un symbole a toujours plusieurs sens possibles, tandis qu'il est hautement souhaitable qu'un véritable cryptogramme n'en ait qu'un seul. Aussi, bien qu'il soit toujours possible d'interpréter un symbole alors qu'on ne réussit pas toujours à décrypter un cryptogramme, l'interprétation d'un symbole est toujours incertaine tandis qu'un décryptement réussi aboutit toujours à une quasi certitude.

Néanmoins, soulignons-le fortement, il existe des cas-limites où disparaît cette différence de nature entre l'interprétation symbolique et le déchiffrement. L'un de ces cas est celui du rébus : considéré isolément, chacun des éléments d'un rébus se prête à une interprétation symbolique ou phonique et par conséquent polyvalente ; pourtant, l'ensemble du rébus ne comporte qu'une seule solution car il constitue un cryptogramme obéissant à une convention systématique, et cette convention n'est autre qu'un chiffrement par substitution constante : la substitution à chaque emblème du phonème qui lui correspond. Or le rébus, cryptogramme pour analphabètes — ce qui ne veut nullement dire pour gens incultes — est l'une des formes de langage secret que rencontre le plus fréquemment l'archéologue en général et le médiévaliste en particulier. Un exemple : sur un tombeau d'enfant romain on voit, gravé dans la pierre, un enfant tenant dans ses mains un oiseau. Considéré du point de vue symbolique, cette image évoque des résonances multiples laissant, un peu comme un poème, une vaste marge à l'interprétation. Par contre, considéré du point de vue cryptographique, cette image est un rébus qui comporte une solution unique. En effet, « enfant à l'oiseau dans les mains » se lit en latin « puer ave manibus », or cela signifie également : « enfant sois le bienvenu chez les mânes », souhait dont on comprend alors parfaitement qu'il ait été gravé sur une tombe.

Ces rapports entre la cryptographie et le symbolisme méritaient d'autant plus d'être soulignés qu'au Moyen Age, nous allons le voir, symbolisme et cryptographie étaient étroitement combinés.

***

Il est temps, maintenant, de passer aux exemples, qui nous ramèneront au cœur de notre sujet : comment chifffrait-on au Moyen Age ?

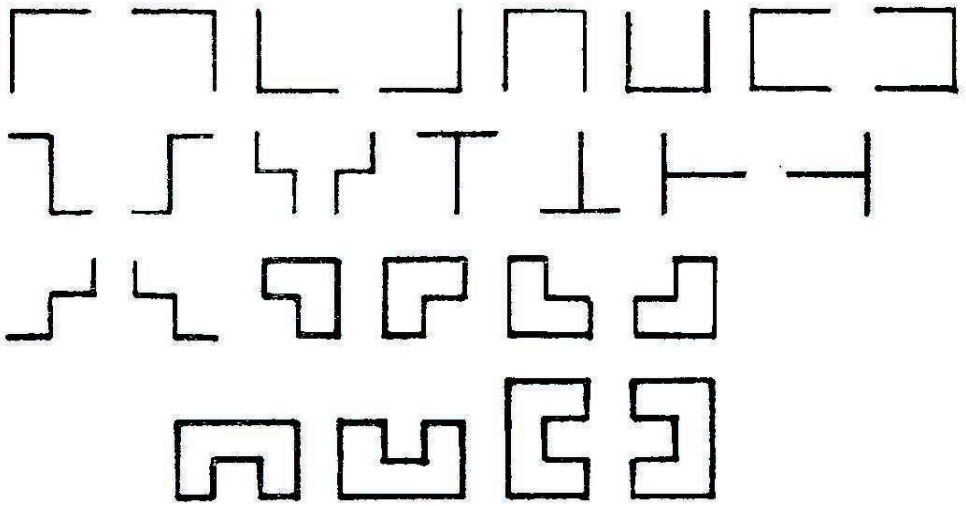
Prenons tout d'abord l'emblème suivant :  Cet emblème est bien connu des archéologues qui l'appellent la Triple Enceinte. En effet, on le rencontre aux époques et aux endroits les plus divers :

(1) Presses Universitaires de France. Collection " Que sais-je ? ", 1958.

Paul Le Cour et Louis Charbonneau-Lassay l'ont relevé sur des monuments mégalithiques comme les menhirs de Suèvres près d'Orléans et de Kermaria en Bretagne, sur le Parthénon à Athènes; on l'a trouvé gravé sur des disques d'os dans des tombeaux mérovingiens ; il figure dans l'église d'Ardin et dans l'abbaye de Seuilly, où séjourna Rabelais; les Templiers l'ont tracé sous forme de graffitti dans les donjons de Chinon et Gisors ; enfin il figure — très mystérieusement — sur une tapisserie de 1510 représentant la cueillette des fruits et qui se trouve au Louvre.

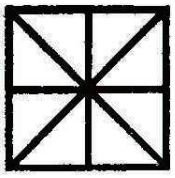
La présence d'un tel emblème en des temps et des lieux si variés pose évidemment à l'archéologue le problème de sa signification. Aussi a-t-on beaucoup écrit sur le symbolisme de la Triple Enceinte ; et, comme toujours quand il s'agit de symboles, on a trouvé diverses solutions : pour les uns, elle symbolise les trois âges de la vie humaine, pour les autres les trois degrés de l'initiation, pour d'autres encore elle représente la rédemption (la croix) agissant sur les trois mondes : terrestre, céleste et angélique (le monde, au Moyen Age, étant souvent figuré par un carré, — nous disons encore une *carte* géographique.) Or, tant qu'on reste sur ce terrain, toutes les interprétations se valent.

Par contre, si on étudie la triple enceinte au point de vue cryptographique, on s'aperçoit qu'elle peut dissimuler un alphabet de 26 lettres qu'on obtient par exemple en la décomposant comme suit :



S'agit-il d'un alphabet simplement possible, ou bien de tels alphabets étaient-ils réellement en usage au Moyen Age ? La réponse va nous être donnée par d'autres exemples du même type.

Soit la figure suivante :



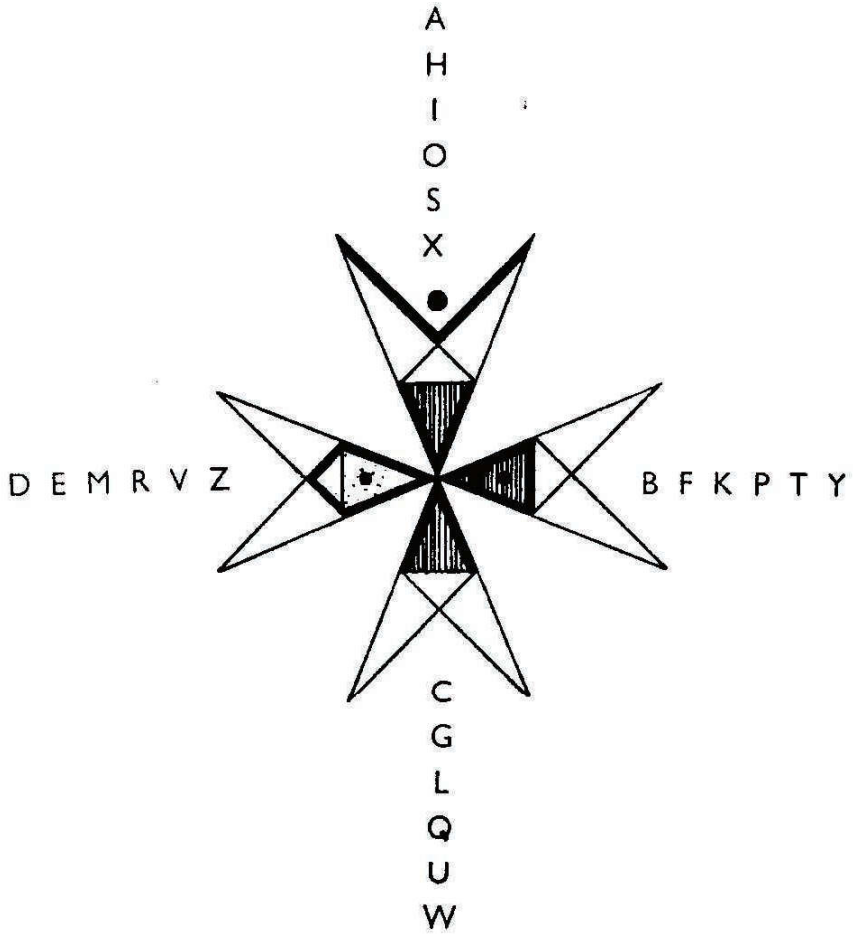
La décomposition de cette figure pourrait nous donner aussi un alphabet de 26 lettres :

etc...

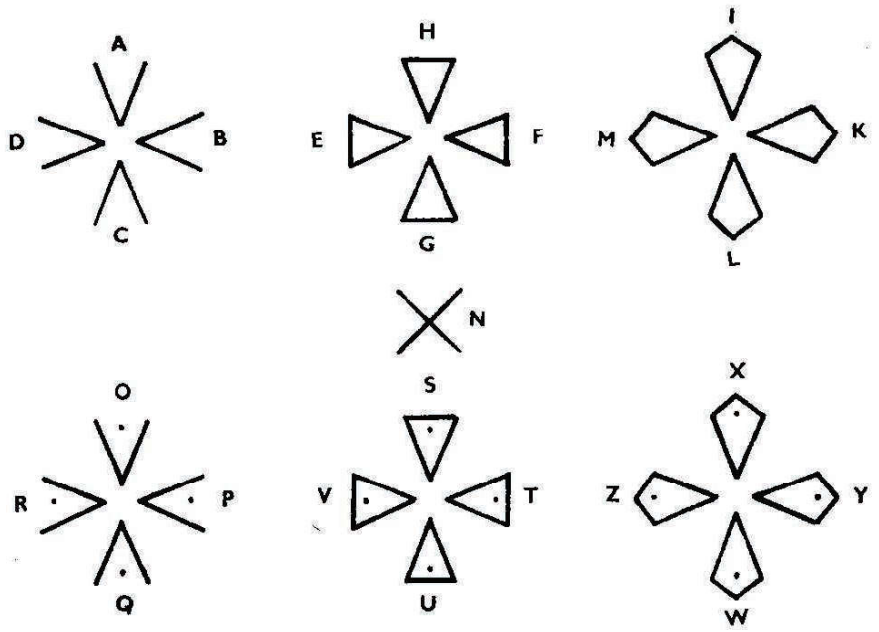
Or dans ce dernier cas nous savons qu'il s'agit de l'alphabet secret qu'employaient effectivement les membres des unions compagnonniques.

Mais nous savons aussi qu'en héraldique cette figure est une partition de l'écu ou, comme on disait au Moyen Age, du cartel — c'est-à-dire du carré ; nous savons aussi que cette partition porte le nom de « gironné », c'est-à-dire « secret » ; nous savons enfin qu'elle forme le drapeau britannique et que celui-ci s'appelle l' « Union Jack ». Or les unions compagnonniques se réclamaient d'un mystérieux fondateur nommé « Maître Jacques » ; les compagnons s'appelaient eux-mêmes (et ceux qui subsistent s'appellent encore) les « Maîtres-Jacques ». L'Union Jack dissimule dans son giron le secret des Maîtres-Jacques : leur alphabet. Bel exemple médiéval de combinaison entre symbolisme et cryptographie :

Autre exemple de figure dissimulant un alphabet : la croix pattée des Templiers. Elle se présente ainsi :

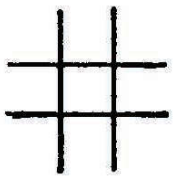


On voit que chacune des branches comporte six éléments, avec ou sans point :

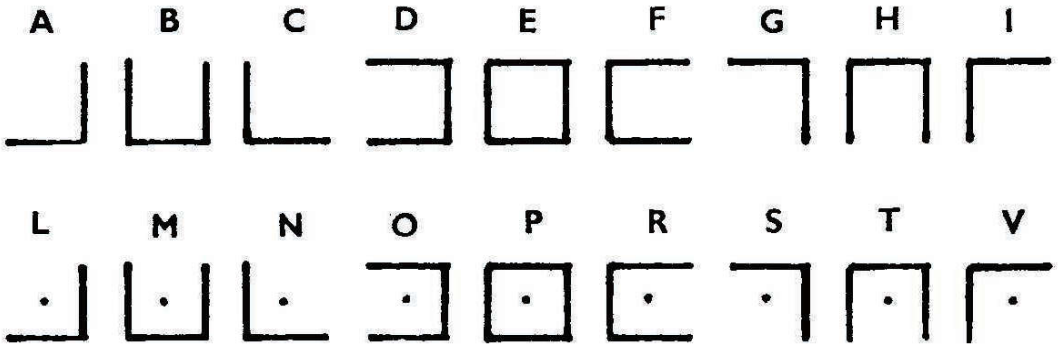


Donc au total 24 éléments, le X central formant un 25e. Cette croix pattée fournit ainsi un alphabet complet.

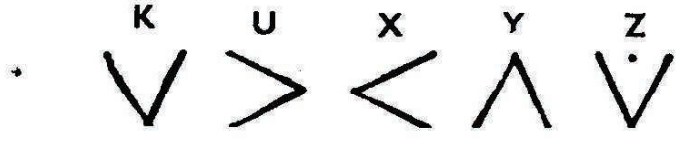
Un dernier exemple du procédé est celui de l'alphabet engendré par la figure suivante :



Dans son « Traité des chiffres » publié en 1561, Vigenère nous apprend que cet alphabet était déjà en usage parmi les anciens kabbalistes. Aujourd'hui, il est encore en usage dans la franc-maçonnerie. Il s'obtient en décomposant ainsi la figure, par exemple :

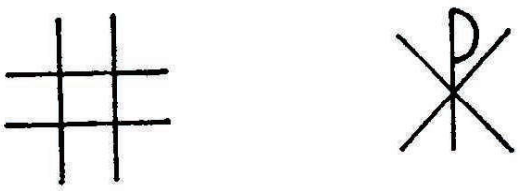


En ajoutant un X on obtient les cinq dernières lettres :



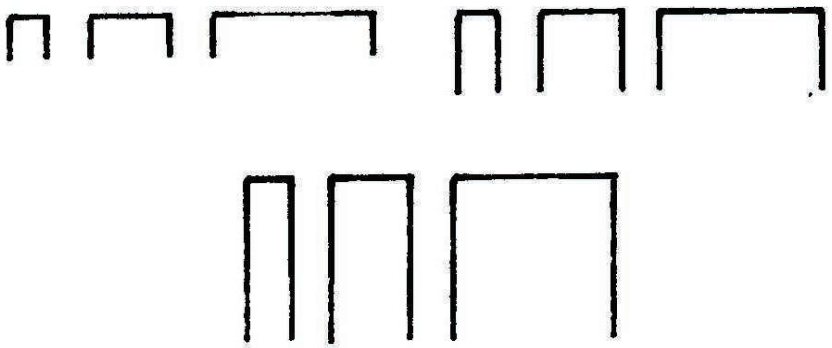
A côté de la figure on représente l'X, et dans l'X le signe P qui indique le sens de lecture de l'ensemble. Il est à noter que la symbo-

lique a joué son rôle dans tout cet ensemble, puisqu'il forme la croix et le monogramme du Christ.



L'usage des alphabets engendrés par des figures géométriques semble à première vue d'une simplicité enfantine, mais quand on y regarde de près il se révèle assez ingénieux. D'abord, le nombre des figures géométriques qui se prêtent au procédé est pratiquement illimité. Ensuite, chacune de ces figures peut engendrer plusieurs substitutions différentes selon le sens dans lequel on la décompose ; les « signes kabbalistiques », dépourvus de signification apparente qu'on est surpris de trouver dans certains manuscrits ou sur certains monuments ne sont en général pas autre chose que les « clavicules » indiquant le sens dans lequel il faut lire ou décomposer.

En outre, comme le révèle Vigenère, les utilisateurs de ces alphabets procédaient à des surchiffrements. Vigenère en donne un exemple à propos de l'alphabet maçonnique que nous venons de décrire : par convention, on attribuait à chacun des traits constitutifs d'une lettre trois dimensions : courte, moyenne ou longue ; grâce à ce procédé, chaque lettre, selon la taille de ses éléments constitutifs, pouvait dissimuler neuf lettres : la lettre apparente et huit autres ; ainsi la lettre H (⌐) engendrera huit groupes de trois lettres selon qu'elle est écrite.

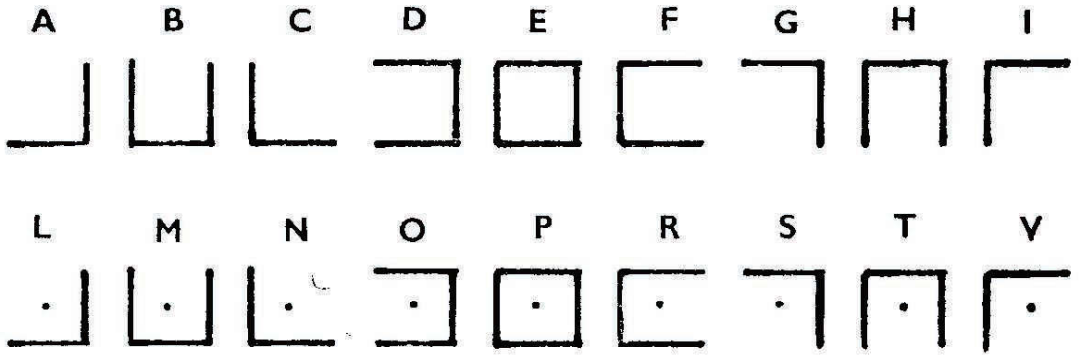


C'est pourquoi Vigenère écrit de ce système : « Je ne vois pas qu'un esprit quelconque, tant subtil pût-il être, sût pénétrer à le démêler sans la communication du secret duquel dépendent d'infinis autres artifices et ouvertures. »

Enfin, la plus grande difficulté pour le curieux est de savoir *où* trouver le cryptogramme et sa clef ; car les gens du Moyen Age faisaient preuve, pour les dissimuler, d'une ingéniosité sans limites. Voyons-en quelques exemples :

Voici le texte exact de Vigenère, dans son « Traité des chiffres ». (Orthographie moderne du texte afin de rendre cet extrait plus lisible.)

« Ne fait encore à oublier cette invention que touche AGRIPPA Liv. 3, chapitre 30, autrefois en très grande recommandation envers les anciens Cabalistes. Depuis on en a fait litière. Ce sont quatre lignes s'entrecroisant à angles droits ; deux d'icelles perpendiculaires et deux transversales, qui par ce moyen viennent à établir neuf caractères différents, qu'on accommode à autant de lettres. Si que diversifiez par un point assis au milieu, des autres neuf qui en sont vides, en résulteront dix-huit lettres de cette manière.



Mais vous les pouvez transposer, et si gardant néanmoins toujours leurs figures, vous voulez varier l'étendue des lignes en chaque caractère de deux manières, comme il se peut voir, et non davantage, vous aurez pour chacun trois lettres ; qui avec les espaces d'entre eux comme dessus feront quatre.

Ajoutez des nombres, ou autres notes servant de lettres dans les espaces, ce sera un chiffre à cinq en-têtes toutes ensembles.

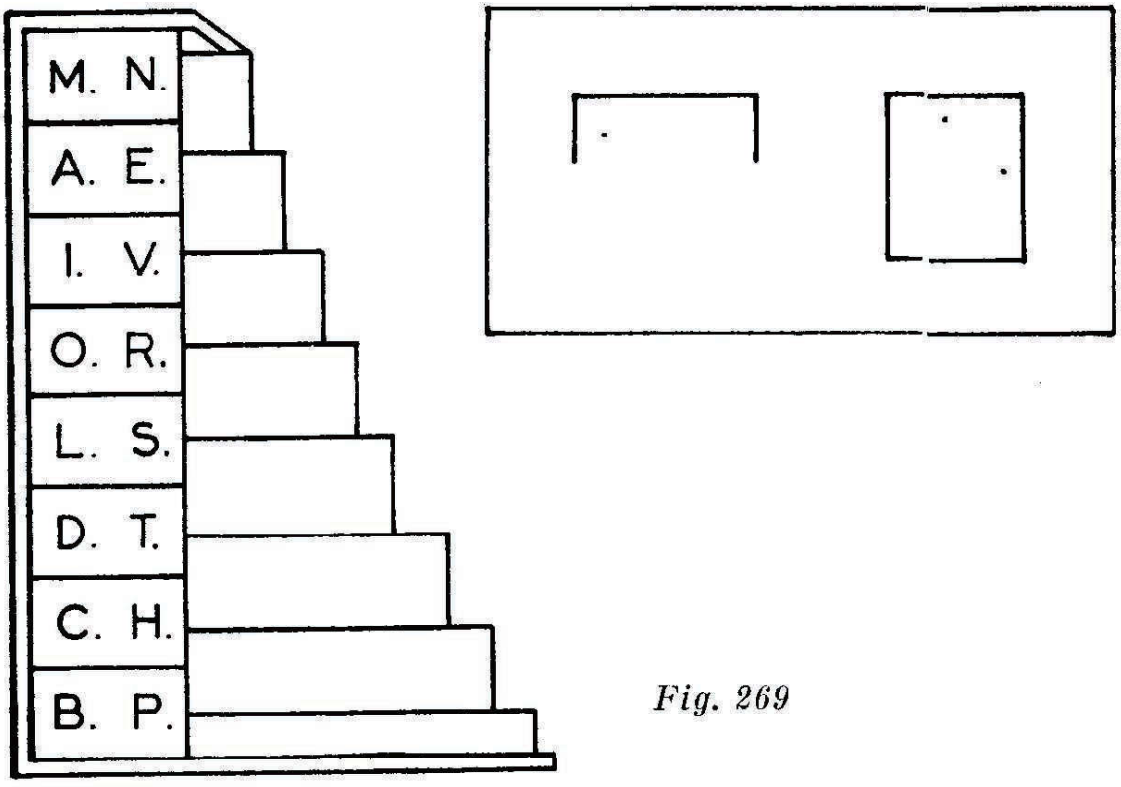


Fig. 269

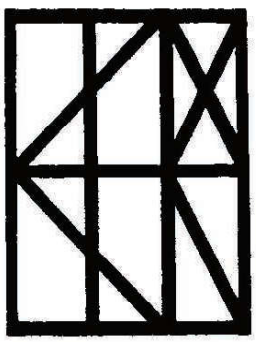
Pour un exemple de trois lettres en chacun de ces caractères, prenons les trois premières du mot HONNEUR, à savoir HON. H en sera la fondamentale, selon qu'elle est figurée en cet alphabet ; dont la ligne s'étendant de long en travers au-dessus, par les dimensions de la figure 269 exprimera O ; et les deux perpendiculaires de côté et d'autres N. De la sorte que vous voyez à la figure suivante. Là où pour autant que N est la seconde des deux lettres associées, car O est la première, afin de la remarquer d'avec sa compagne M, il a été besoin d'apposer un petit point auprès des deux lignes perpendiculaires qui la représentent.

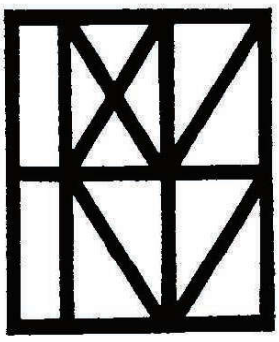
L'autre caractère est pour les trois lettres qui suivent EVR, dont E sera de même la principale exprimée par la figure de l'alphabet qui est un carré, sans point, et aussi, dont les deux lignes transversales d'en haut et d'en bas, semblables entre elles, seront pour V, et les perpendiculaires des deux côtés pour R, toutes deux les secondes parce qu'il y a des points appliqués.

Vigenère reproduit dans son ouvrage une gravure représentant un mur fait de briques irrégulières : il montre que ce mur dissimule le verset d'un psaume cryptographié au moyen de l'alphabet maçonnique, avec le surchiffrement dont nous venons de parler.

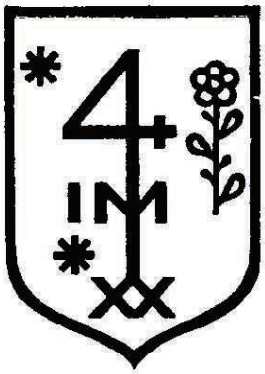
Dans le chœur de l'église Saint-Gervais, à Paris, est représenté un maçon, muni de l'équerre et du compas, agenouillé sur un escalier. Comme j'avais à ce moment là l'attention portée sur les problèmes de cryptographie maçonnique, j'ai été frappé par un détail : le maçon était représenté le genou gauche découvert, c'est-à-dire dans la pose de l'initié. J'ai donc soupçonné que la sculpture dissimulait un cryptogramme. En effet, celui-ci était formé par le compas, l'équerre et les marches de l'escalier. Traduite de l'alphabet maçonnique en clair, l'inscription donne la phrase : « Etudie l'œvre ». En dépit de la faute d'orthographe (« œvre » est écrit sans U), le sens, en cet endroit, est suffisamment adéquat pour être incontestable.

Dans le *Livre d'heures d'Etienne Chevalier*, publié en 1455, une enluminure de Jean Fouquet représente le Châtelet, à Paris. Ici, c'est dans les colombages des maisons que se dissimule une inscription cryptographique ; je la soumets à votre perspicacité, ainsi que celle de l'édition originale des œuvres de Villon (1489), cachée dans la gravure sur bois représentant les pendus.

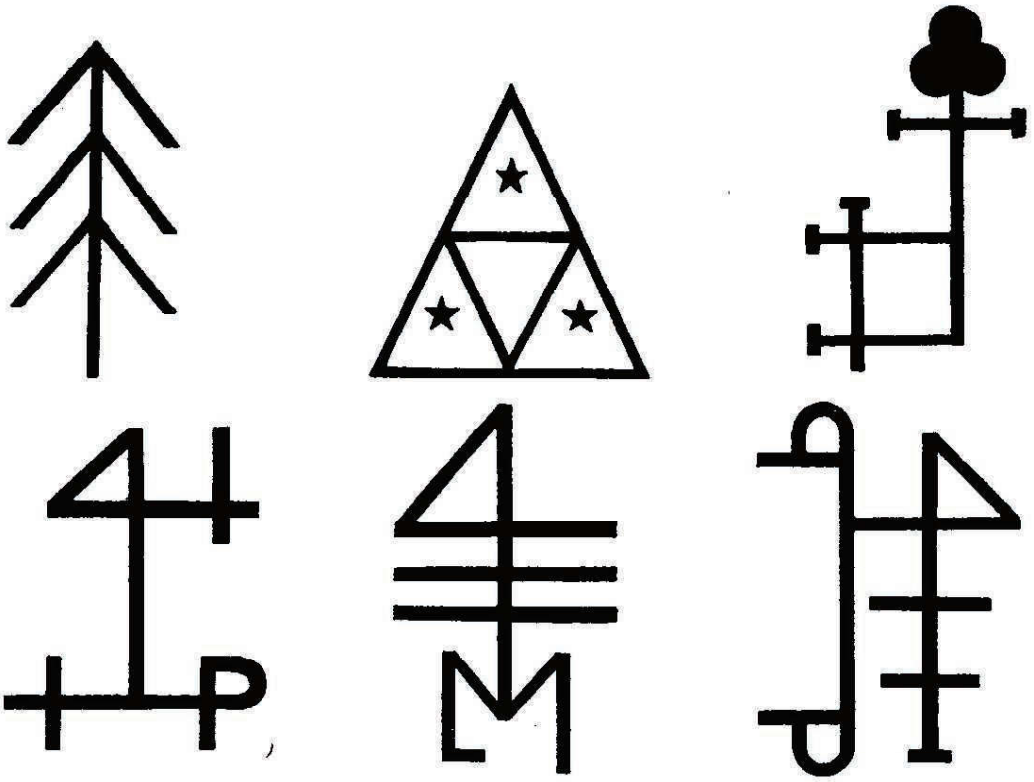




Autre exemple : au château de Fontenay-le-Comte, on remarque sur la cheminée, au milieu de sculptures très curieuses, le blason suivant :



Ce blason est, comme disent les héraldistes, « à l'enquerre », c'est-à-dire qu'il invite à chercher quelque chose. Il figure plus que probablement une « clavicule » complexe et doit être mis en rapport avec toute la décoration de la cheminée sur laquelle figure également une devise (« devise », du latin « divinare » signifie étymologiquement « devinette »). A noter que le château de Fontenay-le-Comte appartenait à une famille d'alchimistes, les d'Estissac. Cette catégorie de blasons, sans être courante, n'était pourtant pas exceptionnelle : j'en ai à moi seul relevé six parmi les vitraux allemands armoriés qui se trouvent au musée de Cluny.



La comparaison avec celui de Fontenay-le-Comte est saisissante. On peut dire aussi qu'une figure absolument identique est gravée sur une paroi de grotte à USSAT (Ariège). Cette grotte a servi de refuge au XIII^e siècle aux CATHARES, et au XVI^e siècle aux HUGUENOTS.

Une autre méthode cryptographique déjà employée au Moyen Age était celle des grilles, trop connue pour qu'on s'y étende. Signalons seulement à ce sujet que les cryptogrammes à grilles passaient le plus souvent inaperçus car ils étaient eux aussi dissimulés dans des images inoffensives.

Vigenère en cite deux exemples : un ciel étoilé où la disposition du texte est fonction de celle des étoiles; une tige de laurier permettant de lire selon la disposition des baies, les feuilles ne comptant pas.

Passons maintenant à un troisième procédé cryptographique médiéval, plus curieux tant en raison des problèmes qu'il pose à l'archéologue qu'en raison de ses prolongements.

Il existe une inscription étrange qui a toujours été un casse-tête pour les archéologues. C'est l'inscription

S A T O R
A R E P O
T E N E T
O P E R A
R O T A S

Cette inscription dont le sens latin est incohérent se trouve en effet dans les endroits les plus divers : sur une médaille découverte dans les ruines de Pompéï, sur une bible latine de l'an 822 et sur un manuscrit grec de XIIe siècle (tous deux conservés à la Bibliothèque Nationale de Paris), dans un manuscrit d'archives des ducs de Cobourg, sur des monnaies autrichiennes du XVIe siècle, sur divers monuments comme l'église de Crémone, le couvent Sainte-Marie-Madeleine à Vérone, en France l'église Saint-Laurent à Rochemaure et le château de Jarnac en Charente, en Espagne à Saint-Jacques-de-Compostelle. Personne n'a jamais pu expliquer les raisons de la présence de cette inscription en ces lieux variés.

Or l'inscription en question offre la particularité de pouvoir être lue indifféremment dans le sens horizontal et dans le sens vertical ; elle forme donc un « carré de mots » identique aux « carrés de chiffres » connus sous le nom de carrés magiques. On sait que les carrés magiques sont des expressions arithmétiques rangées en carré de telle sorte que les nombres formant chaque ligne et chaque colonne donnent la même somme. Ces carrés possèdent un certain nombre de propriétés mathématiques.

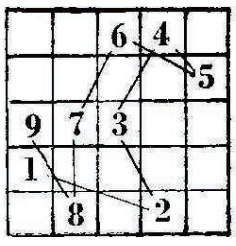
Or si l'inscription SATOR AREPO etc., correspond à la suite des 25 premiers nombres dans leur ordre de succession normal, il est bien évident qu'aux mêmes nombres disposés en carré magique correspondra une inscription brouillée par transposition.

Ainsi, si pour un carré normalement ordonné, on a l'inscription

1 2 3 4 5	R O T A S
6 7 8 9 10	O P E R A
11 12 13 14 15	T E N E T
16 17 18 19 20	A R E P O
21 22 23 24 25	S A T O R

Pour un carré magique

17 23 6 4 15	qui donne la clef
20 14 10 16 5	de relèvement (ou
9 7 3 24 22	clavicule) dont
1 13 21 19 11	nous indiquons
18 8 25 2 12	le commencement



nous aurons l'inscription dans le désordre :

R T O A T
O E A A S
R P T O A
R N S P T
E E R O E

Voici un exemple véritable qui fera mieux comprendre l'usage cryptographique du « carré » au Moyen Age et à la Renaissance. La présence du carré, en lettres ou en chiffres, ou bien la présence d'une clavicule sur un monument, indique comment il faut lire une inscription chiffrée existant dans le voisinage (ou comment le pèlerin devait chiffrer ce qu'il avait à dire).

Sur l'église de ROCHEMAURE, on trouve le carré sous la forme

S A T O R
A R E P O
T E N E T
O P E R A
R O T A S

Et à 4 km de là, sur le mur d'une chapelle romaine dédiée à la « Vierge du Chêne », on trouve l'inscription suivante :

I O S A Q ⊕ S C V S I A
V R C A T A O L N A I L

Nous savons que le signe ⊕ était une figuration courante de la pierre philosophale. Si nous mettons l'inscription en carré, en négligeant la case centrale (probablement case clé, qui doit se trouver autre part, mais que nous n'avons pas remarquée), nous avons :

I O S A Q
⊕ S C V S
I A V R
C A T A O
L N A I L

correspondant au carré

1 2 3 4 5
6 7 8 9 10
11 12 13 14 15
16 17 18 19 20
21 22 23 24 25

et un carré magique, identique à celui indiqué plus haut, et ayant le 3 pour centre, nous donnera :

C I A S
S A N I C
O L A S O
V I L A ⊕
T R O V A

En supposant que la lettre clef manquante est P, nous pourrons lire :

CI PASSA NICOLAS QVI LA « Pierre Philosophale » TROVA.

Il est vraisemblable que cette inscription peut, avec une grande chance de certitude, être attribuée à NICOLAS FLAMEL.

Etant donné qu'il existe 1 052 solutions magiques du carré de 25 cases, les ressources cryptographiques de ce système sont naturellement assez étendues.

L'étude des carrés magiques nous conduit à un des aspects les plus curieux de la cryptographie médiévale : la cryptographie par les jeux. Soit en effet un carré de 25 cases et soit N sa case centrale. Si on considère la case N comme le point de départ des différentes pièces d'un ancien jeu d'échecs, on s'aperçoit que ces pièces, disposées selon leur marche respective, sont disposées en carré magique :

A	C	T	C	A
C	V	S	V	C
T	S	N	S	T
C	V	S	V	C
A	C	T	C	A

(S = Schah, Roi ; V = Vizir, Dame ; A = Alfil (éléphant), Fou) ; C (cavalier) ; T (tour).

Cette caractéristique ne joue que dans le jeu d'échecs médiéval, où la marche des pièces était différente de ce qu'elle est aujourd'hui, sauf pour la Tour et le Cavalier.

On connaît aussi le problème du saut du Cavalier : il consiste à faire parcourir au Cavalier les 64 cases de l'échiquier sans se poser deux fois sur la même case. Or, si on matérialise la solution en numérotant les cases de l'échiquier dans l'ordre où les parcourt le Cavalier, on constate que dans certains cas les numéros des cases forment un carré magique.

Eh bien, il existe diverses indices tendant à prouver que le Moyen Age s'est servi du jeu d'échecs à des fins cryptographiques. Cela est notamment révélé par un manuscrit arabe du x^{e} siècle trouvé en 1931 par le chercheur soviétique Isaiev. *L'Encyclopédie* de Diderot et d'Alembert nous apprend même que le problème du saut du Cavalier était connu des brahmines hindous il y a 2 000 ans. D'autre part, il existe au Musée de Cluny un Cavalier d'échecs donné à saint Louis lors des croisades par le chef de la société initiatique des Ismaéliens qui faisait pendant aux Templiers du côté musulman : il y a ainsi tout lieu de croire que ce Cavalier servait de guide pour le déchiffrement de la correspondance échangée. Enfin, toujours au musée de Cluny, vous pourrez voir une très étonnante boîte à jeux du xiv^{e} siècle composée d'un échiquier, d'une sorte de jeu de l'oie et d'un jeu dont j'ignore les règles mais qui se jouait sur une « Triple Enceinte ».

L'art du blason peut, lui aussi, être rangé sans hésitation parmi les procédés cryptographiques du Moyen Age. On sait en effet que c'est à cette époque qu'il fut codifié selon des règles très précises par les hérauts d'armes, en particulier par celui du roi d'Aragon, surnommé Sicile, qui, au XIIe siècle, écrivit un traité à ce sujet. Ce qu'on sait moins, c'est que ces règles étaient considérées comme un secret professionnel inviolable par lesdits hérauts, de sorte que ceux-ci ne nous en ont fait connaître que les principes, mais non les clefs.

Divers érudits se sont efforcés de découvrir les clefs en question. Dans ce domaine, il faut citer les travaux de Cadet-Gassicourt et Du Roure de Paulin sur l'hermétisme dans l'art héraldique et, plus récemment, les travaux de M. Robert Viel, publiés sous les auspices du Centre National de la Recherche Scientifique. Mais le chercheur qui me semble en avoir su le plus long à ce sujet est Grasset d'Orcet, qui publia sur la question au siècle dernier, dans la *Revue Britannique* un article d'une grande importance intitulé « Le Noble Savoir ».

Selon Grasset d'Orcet, l'art héraldique combinait le symbolisme et la cryptographie au moyen du procédé du rébus. Il était donc, pourrait-on dire, une cryptophonie. Je vais illustrer ce procédé par un exemple simple : l'écu de la famille dauphinoise des Beaumont était de gueules plein, c'est-à-dire tout rouge jusqu'au jour où Humbert de Beaumont négocia le rattachement du Dauphiné à la France. A ce moment, le roi Philippe VI de Valois fit aux Beaumont une concession d'armoiries leur donnant droit d'ajouter à leur écu trois lys d'azur ; cette adjonction était bien entendu un symbole, les lys étant l'emblème du roi ; mais elle était aussi, de façon beaucoup plus précise, l'énoncé sous forme de rébus de la concession d'armoiries. En effet, en vieux français, l'un des noms de la couleur bleue était le mot « baille ». Trois lys d'azur se traduisent donc phonétiquement par « Trois lys baille », Te roi l'y baille — le roi te le donne.

Il existe des exemples beaucoup plus complets — et complexes — de ce procédé. Ainsi, quand on le blasonnait correctement, c'est-à-dire quand on le lisait dans l'ordre rigoureux et selon le vocabulaire immuable de l'héraldique, un écu cachait souvent une phrase entière commémorant un événement ou livrant un secret d'un genre ou d'un autre : appartenance à une société secrète, emplacement d'une sépulture, d'un dépôt d'archives ou d'un trésor, secret de fabrication, formule chimique, etc.

L'art héraldique nous conduit ainsi aux frontières incertaines de la cryptographie et du symbolisme. Nous pouvons ainsi mesurer la difficulté majeure à laquelle on se heurte quand on cherche à percer les énigmes médiévales : cette difficulté résulte du manque d'unité et de rigueur des procédés de dissimulation.

Les ouvrages d'alchimie sont, à ce point de vue, très caractéristiques. Pour voiler leurs messages, les auteurs de ces ouvrages font en effet flèche de tout bois : ils combinent le récit allégorique, le jeu de mots et l'à peu près, le rébus, le dessin muet, le blason et la cryptographie proprement dite. Comment s'orienter dans cette forêt vierge ? Un exemple : dans le Lapidaire d'Alphonse X le Sage,

un dessin nous montre un homme avec une tête de dromadaire ayant une longue chevelure tombant sur ses épaules. Or un autre traité — la copie des « Cyranides » faite au XIII^e siècle — nous dit : « Tu trouveras dans la pierre un dromadaire ». Mais un troisième traité — l'Apothicaire de Chartres — écrit : « Tu trouveras Andromède dans la pierre ». Ainsi, en vertu d'un à peu près, Andromède (Andromeda) est devenue Dromadaire (Dromaderius). Pourquoi le dromadaire du dessin a-t-il de longs cheveux ? Parce qu'il existe une constellation nommée la Chevelure d'Andromède. Et pourquoi nos traités, dans les mêmes passages, nous parlent-ils d'une pierre qui empêche les chevaux de tomber ? Parce que ces chevaux sont en réalité des cheveux. Du coup, nous finissons par découvrir quel est le minéral que les auteurs ont pris tant soin de nous cacher : c'est la pierre appelée capillaire parce que, selon Pline, elle combat la calvitie. Or la mythologie nous apprend qu'Andromède fit don de cette pierre à Persée. Mais qu'est-ce que le capillaire ? C'est une pyrite de fer dont on a découvert — ou redécouvert — tout récemment l'importance pour la métallurgie à très haute température.

On pourrait multiplier les exemples, mais le temps passe, et il faut conclure.

Peut-être penserez-vous que la cryptographie médiévale n'offre pas plus d'intérêt par rapport à la cryptographie moderne que l'huile bouillante et le plomb fondu par rapport au bombardier supersonique.

Cela peut paraître logique, et pourtant, tout le monde ne pense pas ainsi : la preuve en est que, dans les bibliothèques et les archives publiques, on trouve rarement un texte relatif à ces questions qui n'ait pas été mutilé par des mains expertes aux pages susceptibles de fournir des indications. Quand cela vous arrive des dizaines de fois, comme cela m'est arrivé, cela donne quand même à réfléchir.

Grasset d'Orcet, l'auteur des recherches héraldiques dont je vous ai parlé tout à l'heure, passait de son vivant pour un demi-fou auprès de beaucoup d'universitaires chevronnés. Il n'empêche que quelques heures à peine après sa mort, un libraire se présentait chez lui pour tenter d'acquérir la malle où il conservait ses archives. Mais le libraire arriva trop tard : avant lui, des inconnus étaient venus et avaient dérobé cette malle.

Mais alors, pourquoi ces agissements ? Et la cryptographie médiévale dissimule-t-elle donc des secrets si importants ? On a peine à le croire. Je voudrais donc terminer sur deux anecdotes :

En 1912, un bibliophile de New York, Wilfried Voinych, achète en Italie une caisse de manuscrits médiévaux. Parmi eux, un volume

de 15 cm sur 20, d'une écriture fine, régulière et orné de dessins curieux. Le texte était entièrement chiffré à l'aide d'un alphabet inconnu, à l'exception de la dernière phrase, chiffrée en alphabet latin. Sur la page de titre figurait le nom de l'auteur : Roger Bacon. Expertisé, le manuscrit se révèle comme étant bien de la main du copiste habituel de Roger Bacon. On procède alors pendant des années à des tentatives infructueuses de déchiffrement, dont vous trouverez le détail, si cette histoire vous amuse, dans l'ouvrage de Fletcher Pratt traduit par le Colonel ARNAUD ici présent, sur l'histoire de la cryptographie. En fin de compte, un spécialiste de l'histoire et de la philosophie médiévale, le docteur William Newbold, de l'Université de Pennsylvanie, émet une hypothèse de travail au moyen de laquelle il s'attaque aux légendes des dessins. Mais les résultats sont incroyables : selon le déchiffrement de Newbold, Roger Bacon aurait connu le microscope, le télescope et aurait découvert les cellules végétales. Newbold, n'osant pas croire à ce qu'il avait trouvé, expérimenta donc la même méthode sur un autre manuscrit chiffré de Roger Bacon. En déchiffrant, il y lut le récit d'un événement ayant eu lieu en 1375 à Oxford et auquel Bacon avait participé. Or des recherches historiques établirent que cet événement avait bien eu lieu et s'était déroulé exactement comme le disait Bacon. Newbold, jugeant alors qu'il ne s'était pas trompé, publia l'ensemble de ses conclusions, ce qui créa évidemment certains remous !

Et voici la dernière anecdote, encore plus étonnante, si c'est possible. Bien qu'elle sorte de la cryptographie pure, je ne puis résister au désir de vous la conter. Au lendemain de la première guerre mondiale, on trouva par hasard dans le grenier d'un musée de Constantinople une carte géographique ancienne, accompagnée d'un texte chiffré. Le déchiffrement n'offrait pas de difficulté. Il révéla que l'auteur de la carte était l'amiral turc Piri Raïs, qui l'avait dressée en 1513. C'était une carte du continent américain, et Piri Raïs indiquait qu'il avait utilisé pour la dresser d'une part une carte que lui avait communiquée un membre de l'expédition de Christophe Colomb, d'autre part des cartes antérieures à l'époque d'Alexandre le Grand, ce qui était évidemment plus étonnant.

Un spécialiste américain, le capitaine Arlington Mallery prit alors cette étrange carte en mains et fit travailler dessus les services hydrographiques et cartographiques de la marine de guerre américaine. On commença par transcrire le système de projection original en système de projection Mercator, et on s'aperçut que la carte de Piri Raïs décrivait avec une grande précision toute la côte allant de Punta del Este au détroit de Magellan, que Christophe Colomb ne connaissait pas. Mais il y avait mieux : la carte contenait des profils de terres antarctiques qui n'existent plus aujourd'hui, car ils ont été recouverts par la glaciation il y a environ 5 000 ans. Si ces profils étaient exacts, cela impliquait que l'Amérique était connue dès cette époque par des gens capables de réunir des équipes de cartographes qualifiés. Arlington Mallery profita donc de l'expédition de Paul-Emile Victor dans l'Antarctique pour lui confier la carte de Piri Raïs. Et Paul-Emile Victor eut la surprise de constater sur le terrain que les profils de la carte étaient rigoureusement exacts.

Quels étaient les navigateurs qui, cinquante siècles avant nous, trouvèrent et jalonnèrent kilomètre par kilomètre les terres antarctiques ? Quels moyens utilisaient-ils pour établir des cartes qui, de l'avis des spécialistes, nécessitent normalement l'emploi de l'avion ?

Et surtout, par l'intermédiaire de qui, par quels canaux mystérieux transmirent-ils, de génération en génération, leurs précieux documents jusqu'à un amiral turc du XVI^e siècle, expert en cryptographie ? C'est leur secret mais, avouons-le, un de ces secrets des temps anciens qui valent bien la peine d'être percés.

GÉRARD DE SEDE
