Petite histoire des procédés de chiffrement

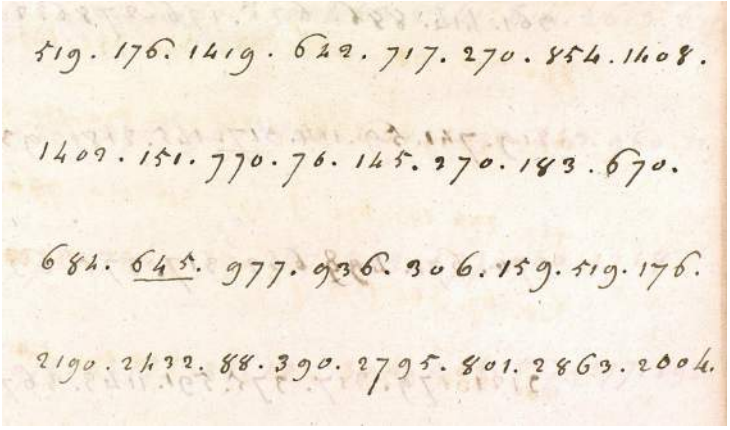
Par Daniel TANT

ex-rédacteur chef des Archives municipales et communautaires de la Ville de Reims,
ex-chiffreur à l'Etat-major de la 6° Région militaire à Metz,
Réserviste du Chiffre et de la Sécurité de l'Information,

Début 2009, une de mes collègues découvre dans le fonds ancien des Archives municipales de Reims, 15 documents curieux composés de mots et de chiffres. Elle me montre sa trouvaille que j'identifie immédiatement comme étant une nomenclature ayant permis pendant la Fronde de coder des messages secrets entre le roi et certains de ses représentants en province.

Passé la phase de saisie sur informatique et le contrôle paléographique, des revues culturelles sont contactées mais en vain car elles ne comprennent pas l'intérêt de ce document.

Pour faire connaître cette découverte et attirer l'attention des historiens, une exposition est prévue avec l'espoir de lever de belles pièces dans les autres services d'archives. Mais leurs réponses montrent l'ampleur du problème : la plupart ignorent tout d'un message chiffré et sont incapables de préciser s'ils en ont ou pas. D'autres *« pensent en avoir »* ou *« croient en avoir vu »*. Et certains enfin, m'invitent à venir consulter moi-même leurs fonds d'archives !...

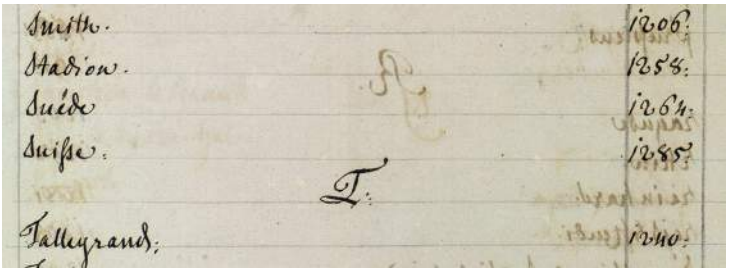

519. 176. 1419. 622. 717. 270. 854. 1408.
1409. 151. 770. 76. 145. 270. 183. 670.
684. 645. 977. 936. 306. 159. 519. 176.
2190. 2432. 88. 390. 2795. 801. 2863. 2004.

Pourtant les documents chiffrés sont des pièces maitresses pour l'historien.

ci-dessus, exemple d'une lettre chiffrée.

ci-dessous, exemple d'une nomenclature : Smith devra être remplacé par 1206, Suède par 1264, Suisse par 1285, Talleyrand par 1240, etc….

Le codage ou chiffrement est aussi vieux que l'écriture. Dès que les rois ou les puissants ont voulu communiquer des informations à ceux de leur parti, ils ont codé leurs messages pour éviter toute indiscrétion suite à la capture éventuelle de leurs messagers par l'ennemi. Un message déchiffré permet donc de connaître la vérité. Dans ce document figurent les vraies alliances, les vraies motivations, les vraies intentions, ce que pense vraiment l'expéditeur, ce que doit faire vraiment le destinataire. Nous sommes donc loin du language politique.


Smith. 1206.
Madrion. 1258.
Suède 1264.
Suisse. 1285.
T.
Talleyrand. 1240.

Les rois ont pris l'habitude de s'entourer de « cabinets noirs » qui chiffrent leurs messages et essayent aussi de décrypter les messages capturés sur l'ennemi, c'est-à-dire de les traduire en clair sans en avoir les codes.

Un message chiffré se présente le plus souvent sous la forme incompréhensible d'une suite de chiffres ou de lettres.

Le code appelé aussi nomenclature est produit en deux exemplaires, un pour l'expéditeur et l'autre pour le destinataire. Le décodage ne pose pas le moindre problème pour qui possède ce code. Il suffit de remplacer les chiffres ou signes par les mots correspondants.

Ce chiffrement représente la majorité des cas rencontrés par l'historien. Voyons maintenant l'évolution des procédés de chiffrement.

Les « cabinets noirs » avaient également pour mission de trouver la signification des messages chiffrés capturés sur les messagers ennemis. Ce travail où l'opérateur tente de découvrir le message en clair sans en posséder le code, se nomme le décryptement.

Ils ont remarqué que dans la langue française la lettre **e** est la plus fréquente dans un texte. Viennent ensuite, dans l'ordre, les lettres s a r i n t u l o. Selon d'autres chercheurs, ce sont les lettres e n a i r s t u o l. Des fréquences sont également étudiées pour trouver les syllabes à partir de chacune de ces lettres. Ce n'est pas une méthode exacte, car il faut beaucoup de tâtonnements, mais si la même lettre en clair correspond toujours à la même lettre ou nombre en code, le travail du décrypteur en sera facilité.

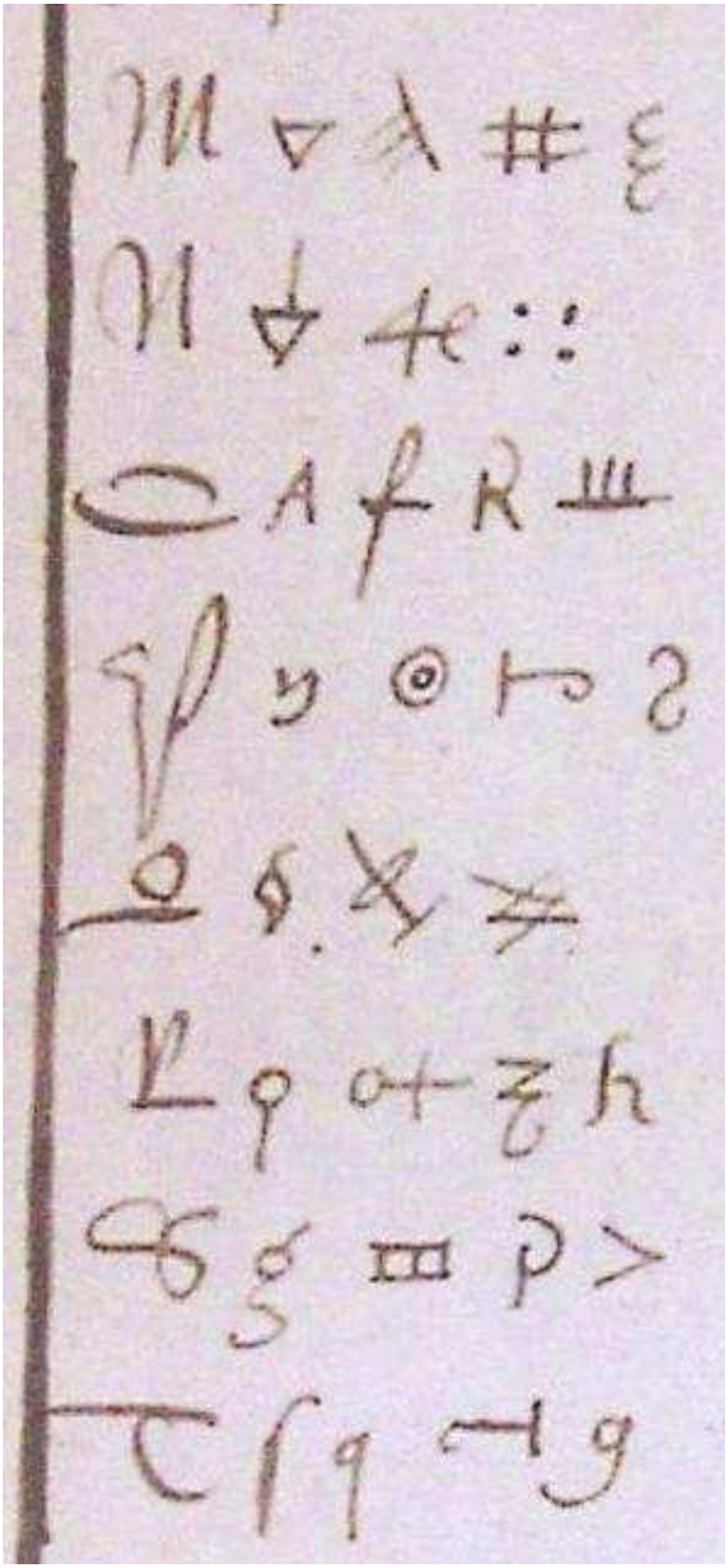
Comment faire pour qu'une lettre d'un message en clair, ait plusieurs correspondances cryptées ? la solution a été apportée par les signes cabalistiques.

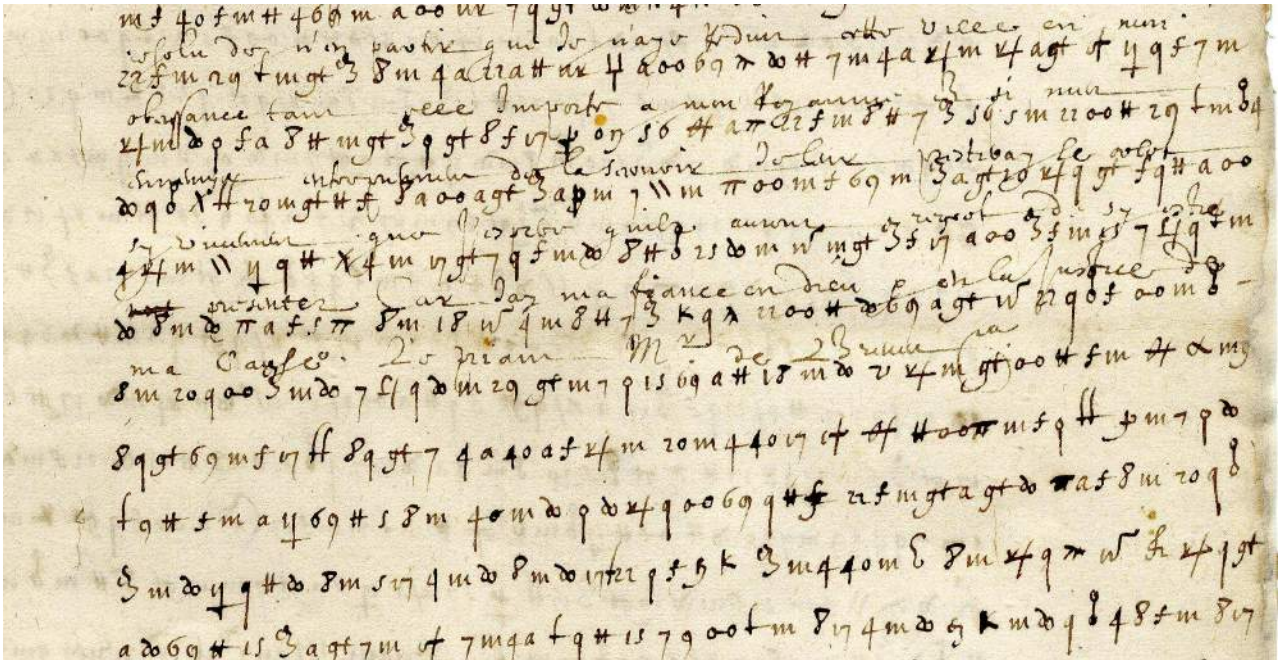
Dans la nomenclature verticale ci-contre, chaque lettre de m à t peut être remplacée par une lettre prise dans un groupe de trois ou quatre lettres ou signes chacune. Le codage et décodage sont tout aussi simples, mais la fréquence des lettres est cassée, ce qui augmente la difficulté pour les décrypteurs.

De nombreux livres et sites internet diffusent des cours de cryptographie destinés à ceux qui voudraient se perfectionner.

L'archiviste peut trouver différents documents dans ses fonds. Bien souvent sont conservés les messages reçus par le destinataire qui a écrit directement sur le message reçu la correspondance en clair.

Dans l'exemple ci-après, une partie du message a été décodée et l'on peut se demander pourquoi le destinataire n'a pas poursuivi son travail.





Cependant il faut remarquer que chaque lettre a été codée, ce qui est une précaution supplémentaire négligée par certains. En effet, plus par facilité que par coutume il arrivait parfois que seuls les noms propres ou les noms géographiques soient cryptés.

Dans l'exemple ci-contre reproduit par ordinateur, la ligne du bas représente le message tel qu'il a été chiffré, et la ligne du haut sa transcription en clair. Des phrases complètes sont lisibles sans code et laissent deviner le sujet du courrier.

A Rome le 1er Juillet 1721

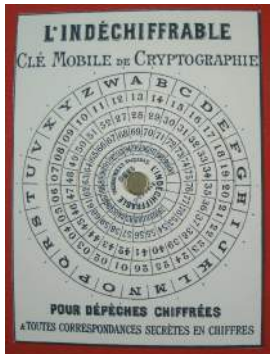
L'abbé vivant écrivit à M. Le Cardinal de Noailles par le dernier courrier. Je n'ay point encore

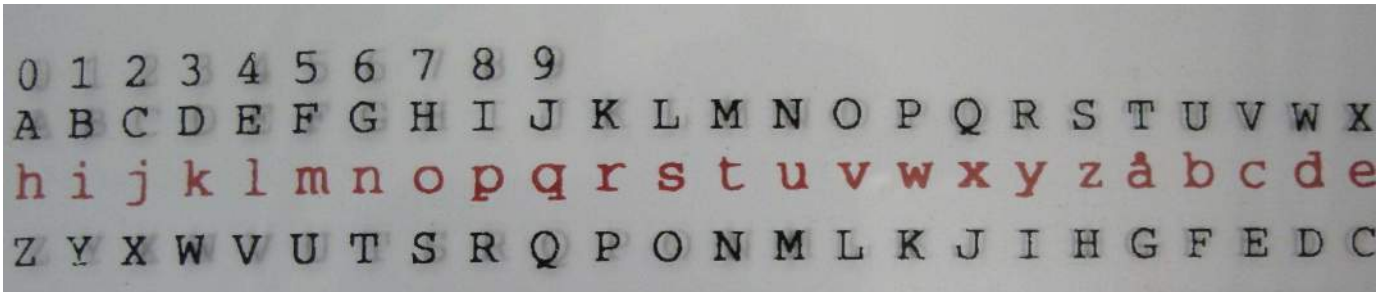
l'honneur de luy écrire aujourdhuy. Je m'addresse a vous, Monsieur, je compte que c'est la même

				mander	*a*	*M. le C. de N*		*certains*	*es*	*ci*	*r*	*co*
chose, et je ne pourrois				475	10	817		391	193	192	26	201
ns	*tant*	*ces*	*je*	*puis*	*vous*	*ecrire*	*a*	*vous*		*qui*	*j'ai*	*un*	*c*	*hi*
216	309	182	118	424	537	519	223	10	519		128	414	489	12	344
f		*re.*					*qu'il*	*y*	*a*	*icy*	*un*	*petit*	*no*	*m*
16.39		198. Vous scaurez donc Monsieur,					128	31	10	504	489	217	196	21
b	*re*	*de*	*personne*	*s*					*M.le C. de N.*					
11	198	282	247	50	qui sont celles sur lesquelles					817		compte le plus, et		
						bien	*ou*	*mal*	*ent*	*en*	*du*	*s*		*le*
qui veritablement sont dans ses interets						101	416	455	173	173	312	50. Je veux dire		205

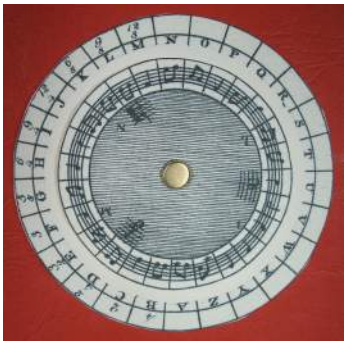
Le cardinal de Rohan, auteur de cette lettre, a eu le tort de négliger les capacités des cabinets noirs. Son chiffre était trop simple, ce qui a causé sa perte.

L'archiviste peut trouver dans ses fonds des codes sous forme de listes, mais aussi des grilles, de règles ou des disques. Le premier disque ci-contre a été utilisé pendant la guerre de sécession. Il a été réalisé en carton pour être brûlé facilement en cas de capture de son porteur par l'ennemi.

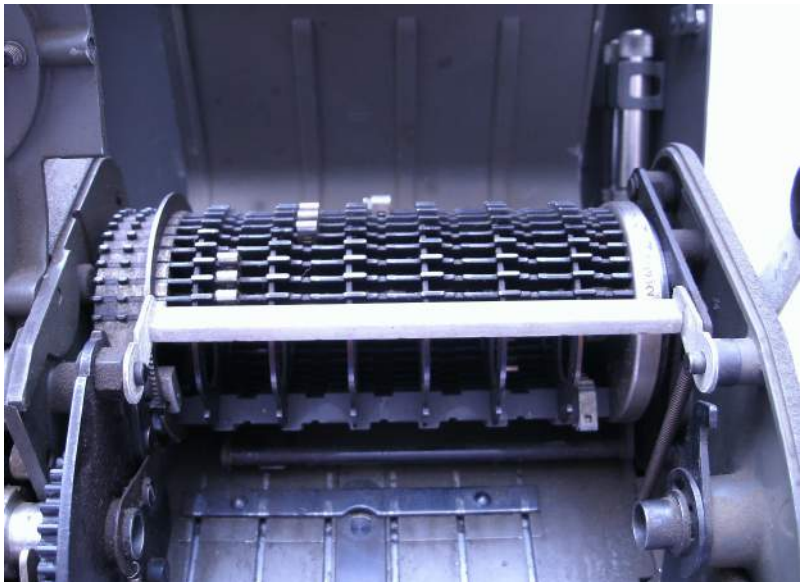




Les possibilités cryptographiques sont vastes. L'encyclopédie Brittanica a publié vers 1800 le dessin d'un disque pour transposer les lettres de l'alphabet en…notes de musique !



L'apparition de la mécanique d'abord puis de l'informatique limite depuis le début du vingtième siècle les possibilités de décryptement pour l'historien. Désormais il faut détenir la machine adéquate, connaître la position de ses rotors et éventuellement des cavaliers de « la cage à écureuil », ainsi que la clé de départ ou le logiciel. Il est donc peu probable de déchiffrer des messages parus après 1920.



Ci-dessus, certaines machines de chiffrement comme la CX52, possèdent en plus de rotors mécaniques une « cage à écureuil » visible ici au fond, dont la position des cavaliers influe sur le codage des messages.

Ci-dessous, la CX52 complète avec ses rotors.

De façon générale tout document découvert dans les archives dont les termes sont incohérents, mélangeant lettres, signes ou chiffres, peut-être considéré comme étant cryptographié.

Un travail d'inventaire s'impose, mais à l'échelon international car les guerres provoquent l'arrivée de documents chiffrés provenant de l'envahisseur. Sans doute avons nous en France, par exemple, des documents chiffrés par la machine « Enigma » allemande, et leur déchiffrement présenterait un intérêt aux historiens des deux cotés de la frontière. De même, des lettres chiffrées par le « cabinet noir » de Napoléon doivent figurer dans de nombreux services d'archives en Europe.

L'idéal serait la publication de ces documents transcrits totalement sur ordinateur après vérification paléographique, ce qui permettrait de faciliter le travail de chacun et sans déplacement.

N'oublions pas qu'une lettre décodée peut donner une nomenclature car il arrivait que le même code soit employé pour plusieurs lettres.

Il arrive aussi qu'un message connaisse un surchiffrement. Le texte une fois décodé laisse apparaître un autre texte qu'il faut lui-aussi décoder. Ainsi la lettre chiffrée de Chalons en Champagne, traiterait d'une vente de vignes, événement anodin qui ne mérite pas de chiffrement.