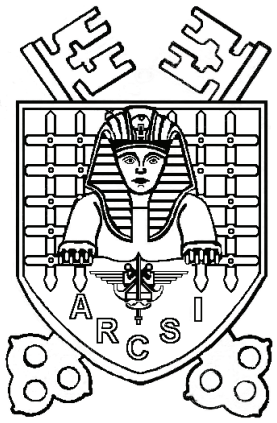

ASSOCIATION des RESERVISTES du CHIFFRE et de la SECURITE de L'INFORMATION

Nouvelle série
n° 28 - 2000

Document interne à l'Association
Réservé aux adhérents

11 . Décryptement

Le décryptement des substitutions polyalphabétiques par la méthode de KASISKI.

Dans l'article qui suit nous nous intéresserons au décryptement de substitutions qui doit beaucoup à Blaise de VIGENERE et à F.W. KASISKI.Le premier est tenu pour l'inventeur des « double-clés » le second pour leur décrypteur. Entre le traité de VIGENERE et le recueil de KASISKI il s'est écoulé 277 ans. Presque trois siècles pendant lesquels on ne connut pas de méthode globale de décryptement. Pourtant le VIGENERE fut relativement peu utilisé car sa difficulté de mise en œuvre rebuta les chiffreurs. ROSSIGNOL lui-même préféra les nomenclateurs.

Après avoir tenté de décrire le travail du décrypteur, celui de VIGENERE étant supposé connu, nous essayerons de comprendre l'évolution normale de cette technique.

Tout d'abord une précision en matière de substitutions. Si l'on fait abstraction des investigations basées sur les mots probables ou les essais systématiques, les décrypteurs ne savent et n'ont jamais su décrypter que des substitutions simples à représentation unique (SSRU) et leur recherche se cantonne donc à deux axes :

- Le premier, simple survivance du passé, consistait à maîtriser le décryptement des SSRU (Substitutions Simples à Représentation Unique). Je conjugue cette recherche fondamentale au passé car il y a belle lurette que tout est dit, que tout est fait en la matière. Déjà dans ma jeunesse le manuel des castors juniors donnait les clés de ce mystère et plus récemment l'informatique a automatisé le processus au point de le rendre trivial. Seuls les fanatiques se livrent encore aux joies des relevés manuels de fréquences et des séparations voyelles-consonnes. Toutefois je rappelle à tous les membres de l'association que ces exercices sont formateurs aux plans de la rigueur et de l'invention intellectuelles.
- Le second, puissant moteur de la recherche cryptologique, a pour but de réduire un cryptogramme à une SSRU ou à un ensemble de SSRU. C'est ce que d'aucuns appellent se ramener à un problème connu. Pour les substitutions simples à représentations multiples les recherches ont porté leurs fruits dès le moyen-âge. Citons Jérome CARDAN et Léon-Baptiste ALBERTI au passage. Pour les substitutions à double-clé c'est le major silésien F. W. KASISKI qui le premier publia la solution dans son ouvrage « Die Geheimschriften und die Dechiffrierkunst » édité à Berlin en 1863. Cette antériorité ne signifie pas qu'avant lui personne n'avait su décrypter des textes chiffrés en double-clé mais elle est la preuve irréfutable que personne avant lui n'a publié une méthode de décryptement de ces cryptogrammes. De même il y eut vraisemblablement des chiffres méritant l'appellation contrôlée de substitutions polyalphabétiques avant VIGENERE mais qui avant lui a pensé à combiner les avancées de TRITHEME et de PORTA ? N'oublions pas que dans notre domaine la chape de plomb du secret rend parfois délicate l'attribution des prix. Mais pour revenir à la méthode préconisée par KASISKI il nous faut avant tout en définir les limites.

De quoi s'agit-il ? interrogeait le maréchal FOCH.

Considérons un cryptogramme chiffré à l'aide d'un carré de VIGENERE. La clé est courte et utilisée selon la variante de PORTA. Un exemple vous évitera un long discours ésotérique. Soit le mot clé « MESSAGERIE » que nous allons utiliser répétitivement pour chiffrer le début d'un poème d'Alfred de VIGNY :

```
J a i m e l e s o n d u c o r l e s o i r a …
M e s s a g e r i e m e s s a g e r i e m e …
```

Pour faciliter les opérations de chiffrement et limiter les écritures il est possible de présenter le travail sous forme de tableau :

```
M e s s a g e r i e
------------------
j a i m e l e s o n
V E A F E R I L W R
d u c o r l e s o i
P Y U H R R I L W M
r a u f o n d d e s
D E N Y O T H W M W
b o i s s o i t q u
N S A L S U M M Y Y
i l c h a n t e l e
U P V A A T X X T I
```

Nous voyons alors que chaque colonne correspond à une SSRU commandée par la lettre clé située en haut de colonne. Dans notre exemple il y a 10 SSRU dont 7 différentes. Ajoutons que chaque SSRU ne constitue pas un texte clair mais est composée de lettres distantes d'une longueur de clé. Le décryptement de chaque SSRU ne portera donc que sur la fréquence des lettres et non sur les séparations consonnes-voyelles ou l'étude des poly grammes fréquents. Mais comme les différents alphabets ne sont que des « Jules CESAR » de l'alphabet clair, la connaissance d'une seule lettre claire, par exemple une des plus fréquentes, entraîne la connaissance de toute la colonne.

Le problème est donc résolu si nous connaissons la longueur de la clé. Merci major KASISKI puisque c'est cela sa découverte. Il a remarqué que les lettres et polygrammes clairs identiques répétés à des distances égales à la longueur de la clé ou multiples de cette longueur sont chiffrés identiquement. C'est le cas par exemple des quadrigrammes RILW correspondants aux clairs "leso" dans notre crypto. Les répétions dues au hasard sont séparées par des intervalles quelconques, c'est le cas des bigrammes WM. Le plus grand diviseur commun aux intervalles entre lettres mais surtout polygrammes répétés sera donc la longueur de la clé.

Dans la pratique le calcul entre lettres seules n'est effectué que si le calcul des distances entre polygrammes ne donne pas de résultat probant. A noter que si une lettre apparaît n fois dans un crypto il faut calculer $\underline{n(n-1)}$ distances.

Dans notre crypto:
Le quadrigramme RILW apparaît 1 fois distance: 10
Le bigramme WM apparaît 1 fois distance : 8
Le bigramme YU apparaît 1 fois distance : 28

On considère pour le calcul qu'un trigramme vaut trois bigrammes, qu'un quadrigramme vaut quatre trigrammes. Nous admettrons donc que la longueur de la clé est de 10. Le reste relève du décryptement des SSRU. A noter que si la clé avait été de 5 le décryptement aurait été possible, la longueur de chaque colonne étant simplement divisée par 2. Par contre essayer de décrypter avec une clé supposée de 5 un crypto dont la véritable clé est de 10 est très hasardeux car chaque colonne dépend de deux lettres clés.

Vous avez remarqué que la méthode s'applique que la clé soit claire ou aléatoire, il suffit qu'elle soit répétitive (variante de PORTA).

Les chiffreurs proposèrent diverses solutions pour contrer la méthode KASISKI. Il s'agit évidemment de rendre la clé apériodique. Citons en quelques unes :

Apériodisation de la clé par lettre d'arrêt. Chaque fois qu'une lettre choisie apparaît dans le clair on recommence la clé à sa première lettre. Si le o est la lettre d'arrêt cela donne :

J a i m e l e s o n d u c o r l e s o i r a u f o n …
M e s s a g e r m e s s a m e s s a m e s s a g m e …

Clé texte. On utilise une clé apériodique par exemple un texte issu d'un livre quelconque convenu à l'avance. La clé est alors aussi longue que le clair et le décryptement fait appel à d'autres outils : les mots probables entre autres. Mais les décrypteurs s'aperçurent que si une clé toujours la même était utilisée pour un ensemble de messages il suffisait de « caler » ces messages pour trouver à nouveau des SSRU en considérant les lettres de rang n de chaque message, puis celles de rang n+1 et ainsi de suite.

Clé une fois aléatoire. Les décrypteurs se cassent les dents sur ce type de chiffrement lorsque le problème de la distribution de clés est résolu. Mais ça c'est une autre histoire.

Il serait inopportun de terminer cet article sans répéter que le chiffre n'est pas une fin en soi. Il contribue à la sécurité de l'information et en constitue le plus souvent le maillon le plus solide. Malheureusement l'élaboration de procédés de chiffrement de haute qualité n'a jamais suffi et ne suffira jamais à assurer la sécurité d'une information. On conçoit alors que le décryptement est une arme redoutablement efficace mais qu'il en existe bien d'autres souvent moins sophistiquées, moins onéreuses mais à la limite moins incertaines.

Enfin pour ceux que le décryptement intéresse voici un cryptogramme chiffré en VIGENERE avec une clé utilisée en variante de PORTA. Bonne chance.

```
BOATZ  EQGVC  UKABN  RUGHS  XMHGE  CTXCX  NXSRV  WKLBH
NTPGP  KCLXL  MNELY  HMLVR  LRXEN  MEXGE  CTXCY  NXSEG
RTXML  HRZCM  INAXL  CBOTB  YFXEE  GTELU  QEWEF  FIULG
IMEHT  WXXXX
```

Jean-Paul FABREGETTES