Dossier "Cryptologie : l'art des codes secrets"
par Philippe GUILLOT

1. Le chiffrement traditionnel

Le premier procédé qui vient à l'esprit pour rendre obscur un texte écrit dans une langue à alphabet consiste à remplacer chaque lettre par une autre selon une règle convenue entre les correspondants.

Le chiffre de Jules César consiste à décaler l'alphabet. Il est décrit par les historiens Suetone, Dion Cassius et Aulu Gelle.

Les lettres peuvent aussi être remplacées par des symboles ésotériques, ce qui donne l'illusion d'augmenter le mystère qui entoure le cryptogramme.

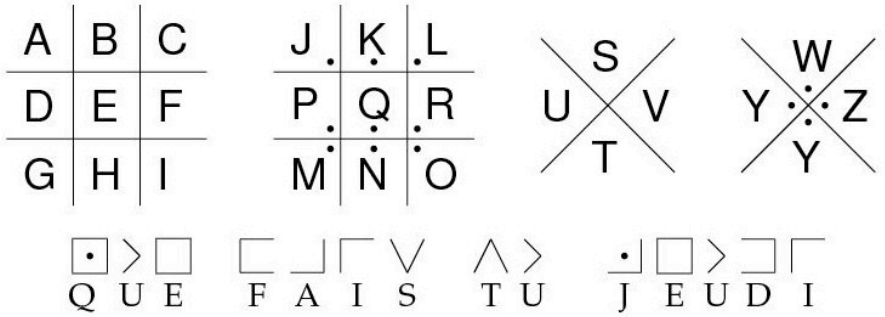


Fig. 1.2 Le parc à cochon, procédé très ancien cité par Vigenère dans son *Traité des chiffres et des secrètes manières d'écrire*, Paris, 1586.

Fig. 1.3 Les hommes dansants. Chaque figurine représente une lettre. Le talent de Sherlok Holmes et l'analyse des fréquences sont aisément venus à bout de ces mystérieux messages.

Un autre procédé consiste à changer l'ordre des lettres sans les altérer, comme par exemple la grille tournante, présentée par le colonel autrichien Édouard Fleissner von Wostrovitz (1825-1888) et décrite dans le roman de Jules Verne *Mathias Sandorf*.

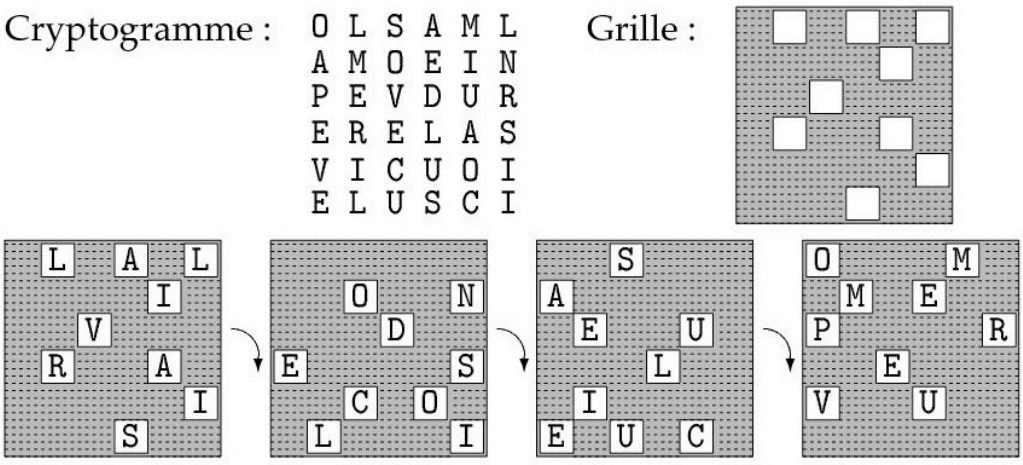


Fig. 1.4 La grille tournante : la grille est placée sur le cryptogramme, puis est tournée quatre fois d'un quart de tour dans le sens des aiguilles d'une montre. Le message en clair apparaît dans les cases ajourées de la grille.

Jusqu'à la première guerre mondiale, les chiffres militaires reposaient souvent sur une combinaison

de ces deux procédés : substitution alphabétique et transposition des lettres. Ainsi, les services d'écoute français ont-ils interceptés le 1er juin 1918, dans les environs de Compiègne, le message suivant :

```
FGAXA XAXFF FAFFA AVDFA GAXFX FAAAG DXGGX AGXFD XGAGX GAXGX
AGXVF VXXAG XFDAX GDAAF DGGAF FXGGX XDFAX GXAXV AGXGG DFAGD
GXVAX VFXGV FFGGA XDGAX ADVGG A
```

Ce message fut immédiatement transmis à la section du chiffre qui réussit à trouver la clé de transposition, puis la clé de substitution pour finalement reconstituer le message en clair :

Munitioneirung beschleunigen punkt soweit nicht eingesehen auch bei tag (hâter l'approvisionnement en munitions, le faire même de jour tant qu'on n'est pas vu)

Ce texte, transmis au général Pétain, puis au général Foch, chef d'état-major interallié, a confirmé que l'offensive allemande allait se concentrer à cet endroit. Elle se produisit le 10 juin 1918, mais l'information avait permis de prendre toutes dispositions pour la parer. Elle fut stoppée, ce qui fut décisif. Pour cette raison, le texte intercepté porte aujourd'hui le nom de *radiogramme de la victoire*.

6	16	7	5	17	2	14	10	15	9	13	1	21	12	4	8	19	3	11	20	18
D	A	G	X	F	A	G	F	X	G	G	F	A	D	F	A	G	F	X	A	V
X	G	X	F	A	X	X	V	G	X	A	G	D	A	A	G	V	F	F	X	A
G	X	F	A	G	F	X	X	X	A	F	A	V	A	G	X	F	A	D	D	X
G	G	D	A	D	F	D	X	A	G	F	X	G	F	A	G	F	A	A	G	V
X	G	X	A	G	F	F	A	X	X	X	A	G	D	X	A	G	V	X	A	F
A	D	G	G	X	A	A	G	V	V	G	X	A	G	F	X	G	D	G	X	X

Fig. 1.5 Radiogramme de la victoire : application de la transposition. La clé de transposition est une numérotation des colonnes. Le radiogramme intercepté est écrit verticalement dans les colonnes numérotées 1, 2, ... jusqu'à 21. La lecture horizontale dans le tableau donnera le clair après application de la substitution.

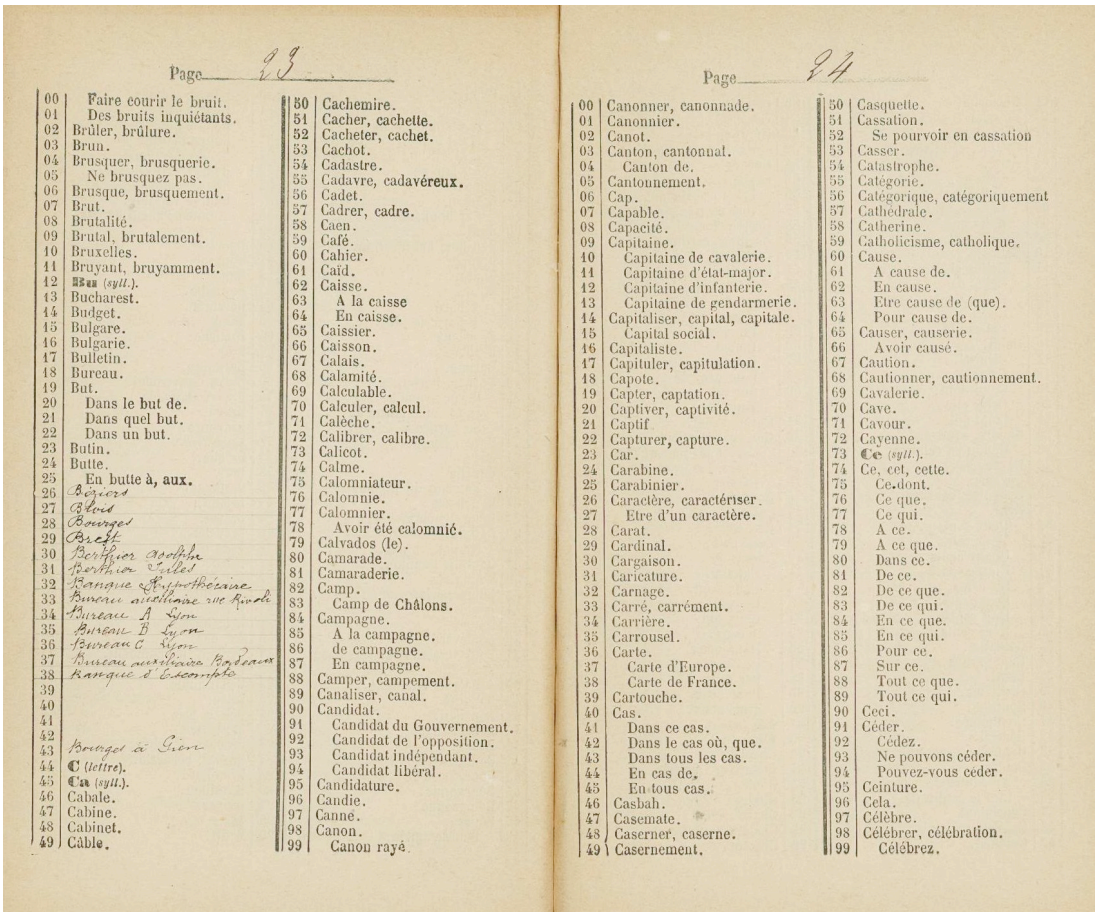
	A	D	F	G	V	X
A	c	o	8	x	f	4
D	m	k	3	a	z	9
F	n	w	l	0	j	d
G	5	s	i	y	h	u
V	p	1	v	b	6	r
X	e	q	7	t	2	g

Fig. 1.6 Radiogramme de la victoire : application de la substitution. La clé de substitution est la façon de remplir le tableau avec les lettres et les chiffres. Les lettres ordonnées du radiogramme sont groupées par deux. La première est l'indice de ligne, la seconde est l'indice de colonne du tableau. DA=m, GX=u, FA=n, GF=i, XG=t, *etc.*

La faiblesse des substitutions alphabétiques a rapidement été mise en évidence. Elles n'apporte qu'un semblant de sécurité. A la renaissance, plusieurs acteurs : l'architecte Léon Battista Alberti, l'abbé Johannes Heidenbert, dit Jean Trithème, le physicien Giovani Battista Porta, le mathématicien Girolamo Cardano et le magistrat Blaise de Vigenère développent le chiffre

polyalphabétique. Il s'agit d'un procédé où l'alphabet de substitution change au cours du message, rendant extrêmement difficile le travail de décryptement. Cette méthode gardera très longtemps la réputation d'être indéchiffrable. Il ne sera cependant que très peu utilisé pour les dépêches officielles et son usage restera confiné à des échanges entre acteurs privés, comme par exemple entre la reine Marie-Antoinette et le comte Axel de Fersen dans les années 1791 e 1792. La raison à cela est l'extrême difficulté de le mettre en œuvre à la main et les inévitables erreurs qui en résultent. Il ne sera réellement pratiqué dans un cadre institutionnel qu'après l'invention de machines qui en automatisent la mise en œuvre, comme la fameuse machine ENIGMA.

La cryptologie gouvernementale et diplomatique a longtemps utilisé les nomenclateurs qui consistent en un alphabet de substitution, avec plusieurs choix possibles pour les lettres les plus courantes pour tromper l'analyse des fréquences, associée à un répertoire de codage des mots courants. Ces répertoires ont été populaires au début du télégraphe tant à des fins de confidentialité que de compression, les télégrammes étant facturés au nombre de caractères. Le plus célèbre d'entre eux est sans doute le dictionnaire abréviatif chiffré de F.-J. Sittler qui comprend cent pages contenant chacune une liste de cent mots ou portion de phrase courante. Chaque mot est codé par deux nombres indiquant la page et la place dans la page. Ces codes perdureront jusqu'aux années 1970, date où le développement du calcul électronique les a définitivement rendu obsolètes.



Page 23

00 Faire courir le bruit.
01 Des bruits inquiétants.
02 Brûler, brûlure.
03 Brun.
04 Brusquer, brusquerie.
05 Ne brusquez pas.
06 Brusque, brusquement.
07 Brut.
08 Brutalité.
09 Brutal, brutalement.
10 Bruxelles.
11 Bruyant, bruyamment.
12 Bue (*syll.*).
13 Bucharest.
14 Budget.
15 Bulgare.
16 Bulgarie.
17 Bulletin.
18 Bureau.
19 But.
20 Dans le but de.
21 Dans quel but.
22 Dans un but.
23 Butin.
24 Butte.
25 En butte à, aux.
26 Béziers
27 Blois
28 Bourges
29 Brest
30 Berthier Apolphe
31 Berthier Talleyrand
32 Banque Hypothécaire
33 Bureau auxiliaire rue Rivoli
34 Bureau A Lyon
35 Bureau B Lyon
36 Bureau C Lyon
37 Bureau auxiliaire Bordeaux
38 Banque d'Escompte
39
40
41
42
43 Bourget à Gien
44 C (*lettre*).
45 Ca (*syll.*).
46 Cabale.
47 Cabine.
48 Cabinet.
49 Câble.
50 Cachemire.
51 Cacher, cachette.
52 Cacheter, cachet.
53 Cachot.
54 Cadastre.
55 Cadavre, cadavéreux.
56 Cadet.
57 Cadrer, cadre.
58 Caen.
59 Café.
60 Cahier.
61 Caïd.
62 Caisse.
63 A la caisse
64 En caisse.
65 Caissier.
66 Caisson.
67 Calais.
68 Calamité.
69 Calculable.
70 Calculer, calcul.
71 Calèche.
72 Calibrer, calibre.
73 Calicot.
74 Calme.
75 Calomniateur.
76 Calomnie.
77 Calomnier.
78 Avoir été calomnié.
79 Calvados (le).
80 Camarade.
81 Camaraderie.
82 Camp.
83 Camp de Châlons.
84 Campagne.
85 A la campagne.
86 de campagne.
87 En campagne.
88 Camper, campement.
89 Canaliser, canal.
90 Candidat.
91 Candidat du Gouvernement.
92 Candidat de l'opposition.
93 Candidat indépendant.
94 Candidat libéral.
95 Candidature.
96 Candie.
97 Canne.
98 Canon.
99 Canon rayé.

Page 24

00 Canonner, canonnade.
01 Canonnier.
02 Canot.
03 Canton, cantonnal.
04 Canton de.
05 Cantonnement.
06 Cap.
07 Capable.
08 Capacité.
09 Capitaine.
10 Capitaine de cavalerie.
11 Capitaine d'état-major.
12 Capitaine d'infanterie.
13 Capitaine de gendarmerie.
14 Capitaliser, capital, capitale.
15 Capital social.
16 Capitaliste.
17 Capituler, capitulation.
18 Capote.
19 Capter, captation.
20 Captiver, captivité.
21 Captif.
22 Capturer, capture.
23 Car.
24 Carabine.
25 Carabinier.
26 Caractère, caractériser.
27 Etre d'un caractère.
28 Carat.
29 Cardinal.
30 Cargaison.
31 Caricature.
32 Carnage.
33 Carré, carrément.
34 Carrière.
35 Carrousel.
36 Carte.
37 Carte d'Europe.
38 Carte de France.
39 Cartouche.
40 Cas.
41 Dans ce cas.
42 Dans le cas où, que.
43 Dans tous les cas.
44 En cas de.
45 En tous cas.
46 Casbah.
47 Casemate.
48 Caserner, caserne.
49 Casernement.
50 Casquette.
51 Cassation.
52 Se pourvoir en cassation
53 Casser.
54 Catastrophe.
55 Catégorie.
56 Catégorique, catégoriquement
57 Cathédrale.
58 Catherine.
59 Catholicisme, catholique.
60 Cause.
61 A cause de.
62 En cause.
63 Etre cause de (que).
64 Pour cause de.
65 Causer, causerie.
66 Avoir causé.
67 Caution.
68 Cautionner, cautionnement.
69 Cavalerie.
70 Cave.
71 Cavour.
72 Cayenne.
73 Ce (*syll.*).
74 Ce, cet, cette.
75 Ce dont.
76 Ce que.
77 Ce qui.
78 A ce.
79 A ce que.
80 Dans ce.
81 De ce.
82 De ce que.
83 De ce qui.
84 En ce que.
85 En ce qui.
86 Pour ce.
87 Sur ce.
88 Tout ce que.
89 Tout ce qui.
90 Ceci.
91 Céder.
92 Cédez.
93 Ne pouvons céder.
94 Pouvez-vous céder.
95 Ceinture.
96 Cela.
97 Célèbre.
98 Célébrer, célébration.
99 Célébrez.

Deux pages du fameux code Sittler. http://www.fredandre.fr/images/codebooks/sittler/sittler4.jpg