BULLETIN

DE LA

SOCIÉTÉ D'ANTHROPOLOGIE

DE LYON

TOME TRENTE ET UNIÈME

1912

LYON
H. GEORG, LIBRAIRE
PASSAGE DE L'HÔTEL-DIEU, 36-38

PARIS
MASSON et Cie, LIBRAIRES
120, BOULEVARD SAINT-GERMAIN

1913

thropologie. Citons seulement ceux de ses mémoires ou volumes qui ont été couronnés par l'Institut : *Etude sur la taille considérée suivant l'âge, le sexe et les races*, parue en 1865 ; *Des anomalies du nombre des vertèbres et de la colonne vertébrale chez l'homme* (1877), *et les Eléments d'Anthropologie générale* (1885). En 1901, il faisait paraître un nouveau volume, *l'Anthropologie et les Sciences sociales*, ouvrage très intéressant sur les sociétés animales et sur les premières associations humaines.

Il y a deux ans, il avait été nommé membre d'honneur du nouvel Institut français d'Anthropologie.

Paul Topinard avait conservé jusque dans son âge avancé toute son activité scientifique et même son activité physique, car toujours épris de la nature sauvage au milieu de laquelle il avait passé son enfance et sa jeunesse, il allait parcourir les Alpes et faisait encore, à près de quatre-vingts ans, de vraies excursions de montagne. Son esprit ouvert s'intéressait à toutes les questions scientifiques, et tout homme de science était sûr de trouver auprès du Dr Topinard, plongé au milieu de ses documents, et dans sa riche bibliothèque, l'accueil le plus sympathique et les conseils les plus encourageants.

COMMUNICATION

LA CRYPTOGRAPHIE EN TECHNIQUE POLICIÈRE ÉTUDE SUR L'EMPLOI DES ÉCRITURES CHIFFRÉES PAR LES MALFAITEURS

Par M. E. LOCARD

Il n'y a que les imbéciles qui devinent.....
(M. LEBLANC : *Arsène Lupin contre Herlock Sholmes.*)

L'emploi des écritures secrètes ou chiffrées n'a guère été étudié jusqu'ici qu'au point de vue militaire et diplomatique. C'est seulement pour ceux que leur profession destine

à pénétrer le secret des correspondances échangées entre les ambassadeurs et les ministres, ou entre les attachés militaires et leurs gouvernements, que les traités de cryptographie ont été rédigés. Mais on a attaché trop peu d'attention à l'emploi relativement fréquent de ces méthodes, et parfois des moins simples, par diverses catégories de criminels, et surtout par les détenus. C'est peut-être parce que nombre de policiers, rebutés par la difficulté du déchiffrage, y renoncent d'emblée et détruisent, sans tenter de les lire, les documents cryptographiés qui tombent entre leurs mains. En fait, il y a là une source extrêmement précieuse d'indications, et le soin même qu'apportent les criminels à rendre leur texte d'une intelligence malaisée, marque à quel point les preuves de culpabilité s'y doivent rencontrer fréquemment.

Dans la pratique, deux cas se présentent surtout : tantôt il s'agit de notes prises par un malfaiteur pour son usage personnel, et ce seront des adresses de complices, des indications de coups à faire, des noms de victimes désignées, voire des listes d'objets volés, ou le repérage du lieu où sont recélés les produits du vol ; tantôt, et plus ordinairement, il s'agit de correspondances échangées, soit entre deux détenus, soit entre un détenu et ses amis en liberté. Comment de tels billets s'échangent, ce n'est point ici le lieu de le dire, mais l'étanchéité des cellules et des maisons d'arrêt est une illusion que le plus bref usage fait envoler, et les complicités les plus fâcheusement imprévues s'y rencontrent. Le mal, d'ailleurs, n'est point exclusivement français : Hans Gross, dans sa *Criminalistique*, qui est le point de départ historique de notre technique policière ; Reiss, dans son admirable et tout récent *Manuel*, parlent comme d'une chose peu rare des *kassiber*, c'est-à-dire des billets circulant entre les détenus autrichiens, allemands ou suisses. Et je sais de bonne source que les choses ne se passent pas autrement en Italie. Un juge d'instruction français me disait, il y a peu de jours, qu'il ne lui est pas arrivé une fois, lorsqu'il a affaire à une bande de voleurs qui prétendent ne pas se connaître, d'or-

donner des fouilles dans leurs cellules sans qu'on en rapportât quelque billet, preuve de leur entente. Et c'est là un exemple de la nécessité où l'on est de pouvoir déchiffrer de telles pièces lorsque leurs scripteurs ont eu la précaution de les cryptographier.

Peut-on toujours lire une lettre chiffrée ? Les maîtres de cet art, officiers de l'état-major général, ou fonctionnaires du quai d'Orsay, répondent oui. En technique policière, il faut considérer que les conditions ne sont point absolument semblables. D'une part, nous avons l'avantage de nous trouver en face de scripteurs infiniment moins habiles que les diplomates ou les espions, et les méthodes de cryptographie que nous rencontrerons seront moins abstruses. Mais, d'autre part, l'expert policier, contrairement au déchiffreur des Affaires étrangères, n'aura en général à traduire que des textes très courts. Or, plus un texte est long, plus la lecture en est facile. Et il nous arrivera de nous heurter à des difficultés insurmontables si le billet a seulement quelques syllabes, alors qu'il eût été déchiffrable, avec une simplicité enfantine, s'il avait eu cinq ou six mots de plus.

Un autre facteur dont il convient de faire état dans la difficulté du déchiffrement, c'est la vitesse avec laquelle il est nécessaire de procéder. Il n'est pas rare que les circonstances enlèvent toute utilité à la lecture d'un cryptogramme, quand elle n'est pas achevée à une date, voire à une heure donnée. Il peut s'agir, par exemple, d'une lettre indiquant un crime à accomplir pour le soir même, et la police veut soit l'empêcher, soit profiter du flagrant délit. Ou bien un chiffre est la seule preuve dont un chef de sûreté dispose pour maintenir en état d'arrestation un individu soupçonné : en pareil cas, le délai imparti au cryptographe ne peut excéder quelques heures.

Trois conditions peuvent donc se présenter, ensemble ou séparément, qui rendent délicate la tâche du policier appelé au déchiffrement d'un texte : complexité de la méthode de chiffrage, brièveté de la lettre, urgence de la solution. C'est

pourquoi un tel travail ne s'improvise point. Et si l'on ne peut exiger d'un chef de sûreté ou d'un commissaire, pas plus que d'un juge d'instruction, qu'ils soient préparés et entraînés à une opération aussi spéciale, du moins est-il nécessaire que, dans les villes munies d'un laboratoire de police, le chef de ce service ait étudié et soit à même de pratiquer constamment l'art du déchiffrage. La cryptographie devient ainsi une branche de cet art déjà si varié et si polymorphe qu'est la technique policière.

Je ne prétends pas écrire ici un traité des écritures secrètes : la matière est d'une ampleur à fournir un lourd volume, même sans excéder le domaine purement criminalistique : je voudrais seulement montrer par quelques exemples, tirés de la pratique du laboratoire de Lyon, la façon dont le problème du déchiffrage se présente, et les solutions qu'il peut comporter. Mais, avant d'aller plus outre, je tiens à mettre en garde ceux que la question intéresse contre l'absurdité d'une vieille croyance. En matière de cryptographie, la pire des politiques est de tâcher à deviner. Certes, je ne nie pas l'admirable utilité, je dirai plus, la nécessité du flair en police. Mais, ici, on n'en a que faire : la cryptographie n'est pas l'art de deviner des charades ou d'interpréter des rébus, c'est une technique, on va le voir, à base mathématique, où il faut calculer et résoudre, et non supposer et tâtonner. L'imagination la plus féconde ne saurait ici suppléer à la science, et le goût des devinettes à l'étude des théorèmes.

I. — Systèmes d'interversion monoalphabétique.

On appelle systèmes d'interversion, ceux qui modifient le rang des lettres dans l'alphabet. C'est ce qui se produit, par exemple, quand on décide que chaque lettre du texte clair sera remplacée par la lettre placée 2 rangs, 10 rangs, 20 rangs plus loin dans l'alphabet. Ainsi, le clair :

Je suis détenu à Saint-Paul,

si l'on baisse chaque lettre de 4 rangs, devient :

Ni wymw hixiry e wemrx teyp

La lecture d'un tel document est d'une extrême simplicité ; il suffit de lui appliquer la méthode de déchiffrement dite de Jules César. Soit le chiffre :

e v d x v x c z g z n j w z e o n q j g z n

Si nous écrivons en colonne verticale sous chaque lettre la suite naturelle de l'alphabet, nous produisons bientôt une ligne qui se trouve être un texte clair :

e v d x v x c z g z n j w e z o n q j g z n
f w e y w y d a h a o k x f a p o r k h a o
g x f z x z e b i b p l y g b q p s l i b p
h y g a y a f c j c q m z h c r q t m j c q
i z h b z b g d k d r n a i d s r u n k d r
j a i c a c h e l e s o b j e t s v o l e s

soit : *j'ai caché les objets volés.* Chaque lettre du clair avait été baissée de 21 rangs.

Ce procédé de chiffrage, extrêmement primitif, est relativement rare. Bien plus fréquemment, les détenus brouillent l'ordre des caractères alphabétiques, soit en conservant les formes ordinaires des lettres, soit en les remplaçant par des chiffres arabes. C'est ce qu'on appelle l'interversion irrégulière. Reiss en cite divers cas dans son *Manuel.*

J'ai eu, par exemple, à déchiffrer le cryptogramme suivant, trouvé dans la poche d'un cambrioleur :

2 g t 8 9 4 14 B 2 4 3 4 14 14 3
H 8 t 14 15 d 14 9 2 9 t 14
1 4 7 3 u 14 10 2 3 c 2 d 14 t
1 2 9 u 14 t 2 15 4 c 14
16 2 v 4 16 16 14 3 8 10 2 3 4 9 18

Admettons que le système soit monoalphabétique, c'est-à-dire que chaque caractère garde constamment la même valeur. Il est probable que les groupes de chiffres soulignés représentent une seule lettre. Or, le nombre *14* figure onze fois, c'est-à-dire avec une fréquence nettement prééminente. Il doit donc représenter la lettre *e*.

D'autre part, le dernier mot de la première ligne se termine par *14 14 3*. Or, il n'y a en français que les mots *créer* et *récréer* (éliminés par le nombre de leurs lettres) et les féminins pluriels en *ées* qui présentent des terminaisons par deux *é* suivis d'une finale. Celle-ci étant un *s*, nous avons *3* = *s*.

Mais, d'autre part, nous trouvons à la troisième ligne le groupement *3u14*. En admettant que *u* garde sa valeur alphabétique, on peut penser au mot *rue*, le mot *sue* ne paraissant guère vraisemblable. Mais si *3* = *r*, la finale en *14 14 3* va être en *eer* et le texte sera, non en français, mais en anglais, en flamand ou en hollandais. Seulement, il faut penser qu'en cryptographie policière on est constamment en présence de textes orthographiés d'une façon fantaisiste ou de fautes de chiffrage. Gardons donc comme plus naturelle l'hypothèse et que le clair est en français et que, malgré la présence d'une finale, probablement fautive, en *eer*, *3* = *r*.

Si l'on examine alors le dernier mot de la troisième ligne, et en admettant toujours que les lettres gardent leur valeur alphabétique, nous trouvons d'une part une finale *d14t*, qui sera *det*, d'autre part un groupement *23c2*, où *3* valant *r*, 2 précédant et suivant le bigramme *rc* ne peut être qu'une voyelle. Si cette voyelle est *a*, nous avons un mot formé d'une initiale et de *arcadet*. Le bottin signalant l'existence d'une rue Marcadet, nous en concluons que *10* vaut *m*.

Si, maintenant, dans le mot *3 8 10 2 3 4 9* de la dernière ligne, nous substituons leurs valeurs aux signes connus, nous avons *r.mar..*, qui évoque aussitôt l'idée de Romarin, nom de rue. Ce mot nous fournit : *8* = *o*, *4* = *i* et *9* = *n*.

Nous pouvons, dès à présent, tenter de reconstituer la clef,

c'est-à-dire l'ordre dans lequel les lettres de l'alphabet normal ont été brouillées pour prendre les valeurs chiffrées, maintenant partiellement connues. Nous avons, dans l'ordre, et en remplaçant par des points les chiffres de valeur inconnue :

$$.\,a\,r\,i\,\ldots\,o\,n\,m\,\ldots\,e$$

Une brève réflexion fait découvrir la clef :

$$P\,a\,r\,i\,s\,L\,y\,o\,n\,M\,a\,r\,s\,e\,i\,l\,l\,e$$

où, en effet, la lettre *c* n'apparaît pas avant le quatorzième rang. Les transcriptions seront donc :

$1 = p$	$5 = s$	$9 = n$
$2 = a$	$6 = l$	$10 = m$
$3 = r$	$7 = y$	$14 = e$
$4 = i$	$8 = o$	$16 = l$

On voit que *11* doublerait *2*, que *13* doublerait *3*, que *15* doublerait *4*, et que les lettres *b*, *c*, *d*, *h*, *t*, *u*, *v*, entre autres, font défaut, ce qui explique leur présence dans le cryptogramme sous la forme alphabétique.

Le texte chiffré se lit alors ainsi qu'il suit :

Antonie Baurieer
Hôtel de Nante.
147 rue Marcadet
Panuet Alice
Laville Romarin 18

En résumé, cryptogramme des plus faciles, et rédigé à l'aide d'une clef extrêmement défectueuse et primitive. On peut dire que cet exemple est typique (1), et que la plupart des

(1) Le cryptogramme célèbre qui est décrit dans le conte d'Edgar Poe, *The gold Bog*, est de même sorte : il est également chif-

kassiber courants n'en diffèrent que par les détails. Au contraire, les systèmes qui vont suivre, et dont le maniement est beaucoup plus délicat, indiquent à coup sûr des malfaiteurs habiles et dangereux.

II. — Interversion polyalphabétique.

Lorsque chaque signe du cryptogramme ne garde pas une valeur fixe, mais, suivant sa position, prend des significations diverses ; quand, par exemple, *a* vaut tantôt *c*, tantôt *e*, tantôt *q*, le système est dit polyalphabétique. Tantôt le scripteur s'est servi d'un chiffre ou nombre-clef, ainsi :

J'ai	*été*	*interrogé*
2 3 4	*2 3 4*	*2 3 4 2 3 4 2 3 4*
L d m	*g w i*	*k q x g u v q j i*

Tantôt il emploie un mot-clef dont chaque lettre représente un chiffre égal à son rang dans l'alphabet ; ainsi :

N'avouez	*jamais*
A r t h u r a	*r t h u r a*
n r p v p v z	*b l t u a s*

où le mot-clef *arthur* correspond à un chiffre *1 + 18 + 20 + 8 + 21 + 18*. On voit donc que le mot-clef a sur le chiffre simple l'avantage de varier entre *1* et *26* au lieu de *1* à *9* seulement. Son emploi, un peu plus laborieux, est facilité par l'usage de la table de Vigenère, ainsi que je le montrerai plus loin.

Voici d'abord un exemple de cryptogramme chiffré à l'aide d'un nombre-clef. J'ai eu à lire le texte suivant :

fré par inversion monoalphabétique, partie en chiffres et partie en caractères conventionnels.

M g w q g l f w w q s v f w i e f e i g w f f p t o e e f x
f s v k s e j s e n j u p x w w s g q l i t w g r x i n s p
e h g q z z s l v c j p f q p f a c o w p c y g o u i c i g
v a t c x c h d y e n g e h p c u q s w i f s p u u i g n n
t v s p y g o i i i t r g t g e p u w o h g c x u f w x g k g
s p i g f x f f y p h c e g r c x c m h x v w g t g s p y n
f p s v j u u s e t q g j o w f j x o r r v j v s h t c w v
b j i u j o v l x c g n f p i p y g o w v g y q v v i p y g
o d r v h q n s x g i g n h y t a e n h y t n p e l u w j g
t x v n f p p w i s z g m r r v w q v y i t e c v i s p i f
f o e e f n t h x v j u f x p e j a v l e s z k k d n e t p
g l i n i e i l j h w g e h z t f r s h r f w g d h u w n c
f w i o n u b o e t y f b q w n e d p l x g i g n h x c q r
m o g g j c e u s k y g f w e w k q o g

Ce cryptogramme est polyalphabétique, car les diverses lettres y sont en nombre beaucoup plus sensiblement égal qu'il n'arriverait dans le cas d'une simple interversion monoalphabétique. Il s'agit avant tout de déterminer le nombre des alphabets. Pour cela, on applique les théorèmes suivants :

I. DÉFINITION. — On appelle polygrammes semblables des groupements semblables de deux ou plusieurs signes : ainsi *mg* et *mg* sont deux polygrammes semblables.

II. THÉORÈME DE KERCKHOFFS. — Deux polygrammes semblables du texte chiffré sont le produit de deux polygrammes semblables du clair par deux polygrammes semblables de la clef.

Exemple : Dans le chiffrement :

A s s a s s i n a t
2 4 2 2 4 2 2 4 2 2
c w u c w u k r c v

les polygrammes semblables *cwu* du texte chiffré sont tous deux le produit d'un même polygramme *ass* du clair par un même polygramme *242* de la clef.

III. Théorème de Kasiski (rédaction nouvelle). — Dans les systèmes de chiffrage par interversion polyalphabétique, le nombre des alphabets est égal au produit des facteurs premiers les plus fréquents des nombres représentant l'écartement des polygrammes semblables. Soit le chiffrement :

D o u z e	*j o u r s*	*d*	*o u b l i*
1 2 4 3 2	*1 2 4 3 2*	*1*	*2 4 3 2 1*
e q y c g	*k q y n u*	*e*	*q y e d j*

Le polygramme *eqy* se retrouve à 10 caractères d'intervalle ; en outre, *qy* se trouve (1er et 2e mots) à 5 caractères d'intervalle. Réduisons ces chiffres à leurs facteurs premiers : $5 = 5$ et $10 = 2 \times 5$. Le chiffre 5 étant le multiple commun le plus grand, il y aura probablement 5 alphabets, ce qui est vrai en l'espèce, la clef étant *12432*. (Je dis probablement, car il peut y avoir de simples coïncidences, surtout avec des textes courts et des clefs longues.)

Appliquons ces deux théorèmes au cryptogramme reproduit plus haut. Nous trouvons des polygrammes semblables, ainsi qu'il suit :

1 pentagramme	*ipygo*	*distant de*	$12 = 2^2 \times 3$
1 tétragramme	*occf*	—	$276 = 2^2 \times 3 \times 23$
6 trigrammes	*fwi*	—	$348 = 2^2 \times 3 \times 29$
—	*fxf*	—	$126 = 2 \times 3 \times 31$
—	*gch*	—	$240 = 2^4 \times 3 \times 5$
—	*ygo*	—	$114 = 2 \times 3 \times 19$
—	*cxc*	—	$72 = 2^3 \times 3^2$
—	*set*	—	$180 = 2^2 \times 3^2 \times 5$

et de nombreux bigrammes, comme :

mg	$100 = 2^2 \times 5^2$	*ig*	$72 = 2^3 \times 3^2$
wq	$6 = 2 \times 3$	*ig*	$64 = 2^6$
qg	$187 = 187$	*ig*	$98 = 2 \times 7^2$
fw	$6 = 2 \times 3$	*ei*	$318 = 2 \times 3 \times 53$
fw	$132 = 2^2 \times 3 \times 11$	*ig*	$364 = 2^4 \times 91$
fw	$207 = 3^2 \times 23$	*gw*	$18 = 2 \times 3^2$
fw	$42 = 2 \times 3 \times 7$	*ff*	$135 = 3^3 \times 5$
ef	$12 = 2^2 \times 3$	*fp*	$158 = 2 \times 79$
wi	$96 = 2^5 \times 3$	*wf*	$174 = 2 \times 3 \times 29$

etc., etc.

La solution est évidente, en tenant compte surtout de l'énorme prévalence d'un pentagramme ou d'un tétragramme sur des bigrammes, même en grande quantité : le nombre des alphabets est égal à $2 \times 3 = 6$. Coupons alors par tranche de six le texte donné : [*mgwqge* [*fwwqsv* [etc., et comptons pour chaque rang la fréquence des lettres. Nous établirons ainsi le tableau suivant, dans lequel chaque colonne représente un des six alphabets (p. 18).

Un tel tableau permet de fixer immédiatement la valeur des caractères pour chacun des six alphabets, dans le cas au moins où ceux-ci sont ordonnés normalement. En effet, pour une langue donnée, la fréquence de chaque lettre est un chiffre connu. L'alphabet français présente, pour un texte suffisamment long, les valeurs pour dix mille suivantes :

A 72.6	*H* 5.3	*O* 66.0	*U* 66.6
B 9.3	*I* 68.6	*P* 28.0	*V* 18.0
C 35.3	*J* 3.3	*Q* 7.3	*W* 0.0
D 46.0	*K* 0.0	*R* 68.6	*X* 5.3
E 170.0	*L* 48.6	*S* 68.6	*Y* 3.3
F 12.6	*M* 30.6	*T* 67.3	*Z* 2.7
G 7.3	*N* 87.3		

Un alphabet se présente donc avec un maximum corres-

pondant à *E* précédé de 3 groupes forts *(A, C, D,* avec l'intervalle du *B* faible), suivi de 3 groupes faibles *(F, G, H),* puis d'un relèvement *(I),* puis d'une chute à zéro *(J, K) ;* vient

Caractères du Cryptogramme	Alphabets					
	I	II	III	IV	V	VI
a	»	1	»	»	2	»
b	3	»	»	»	»	»
c	»	»	1	9	»	8
d	1	4	»	»	»	1
e	6	»	8	6	2	3
f	12	1	»	5	7	2
g	1	6	3	7	2	19
h	2	11	»	1	2	»
i	2	2	15	»	5	»
j	2	1	1	»	11	»
k	1	»	»	2	2	1
l	»	8	»	»	»	1
m	6	»	1	»	2	»
n	2	»	»	5	3	4
o	6	3	»	1	»	»
p	3	4	3	7	»	7
q	1	2	»	3	2	5
r	1	2	5	»	1	2
s	7	5	5	2	4	1
t	6	»	2	8	1	»
u	2	3	2	1	1	6
v	6	2	4	6	»	3
w	»	9	6	4	6	1
x	»	4	7	»	4	3
y	»	1	4	»	8	»
z	»	»	1	»	3	1

ensuite un plateau de quatre *(L. M. N. O.)* fortement relevé en *N*, puis une dépression de *2*, suivie d'un plateau égal de quatre *(R. S. T. U.)* descendant en *V* pour arriver à une zone nulle *(W, X, Y, Z)* avant la forte réascension de l'*A*.

Appliquons ces principes, d'autant plus exacts que le document fournit des tableaux de classement plus riches, aux six alphabets du cryptogramme étudié. Nous voyons de suite que, pour l'alphabet I, $F = e$. En effet, le vide *W-X-Y-Z-A* correspond ainsi au groupe nul *w-z*, le plateau *M-P* correspond au groupe *l-o*, le nul *L* correspond à *x*. En opérant de même, nous trouverons dans le second alphabet $H = e$, dans le troisième $I = e$, dans le quatrième $G = e$ (moins certain, mais contrôlé par la concordance générale avec le 6e alphabet, dont, certainement, la clef est la même), dans le cinquième $Z = e$, et dans le sixième $G = e$. Il n'y a plus alors qu'à dresser une table de correspondance, ainsi qu'il suit (p. 20).

Il ne reste qu'à substituer les valeurs aux signes du cryptogramme, dont le nombre-clef était, on le voit, *134252*.

M g w q g l f w w q s v f w i e f e i g w
1 3 4 2 5 2 1 3 4 2 5 2 1 3 4 2 5 2 1 3 4
L e s o b j e t s o n t é t é c a c h é s

et ainsi de suite.

*
* *

Dans les cas analogues au précédent, le déchiffrement est donc une opération purement mathématique. Mais il est assez ordinaire que les textes soient trop courts et que l'application des théorèmes susénoncés ne fournisse que des résultats incomplets et obscurs, dont l'interprétation n'est pas aisée, tant s'en faut. On en trouvera un bon exemple dans le cryptogramme suivant, que j'ai eu récemment à lire dans une importante affaire de vol :

o i m p â a l c y q j v v p s a y b n p p p q a r i n ā h h
e d q à g z x c y v h c v r i d h k i r n i t p i j e m j ā
n g m l s g m g i z m d ā o a g n b n v j a y a v v m b c
i r a z i j k g y v z m n i t n y i z m â n b ā a h m m z
d g j k r t h v v m z f o a i f y x h g z o x j n q n a a y j i b

J'étais averti, par une note saisie sur le détenu auteur du cryptogramme, que la lettre *a* accentuée n'était pas chiffrée

Texte du Cryptogramme	Transcription en clair					
	I	II	III	IV	V	VI
a	*z*	*x*	*w*	*y*	*v*	*y*
b	*a*	*y*	*x*	*z*	*w*	*z*
c	*b*	*z*	*y*	*a*	*x*	*a*
d	*c*	*a*	*z*	*b*	*y*	*b*
e	*d*	*b*	*a*	*c*	*z*	*c*
f	*e*	*c*	*b*	*d*	*a*	*d*
g	*f*	*d*	*c*	*e*	*b*	*e*
h	*g*	*e*	*d*	*f*	*c*	*f*
i	*h*	*f*	*e*	*g*	*d*	*g*
j	*i*	*g*	*f*	*h*	*e*	*h*
k	*j*	*h*	*g*	*i*	*f*	*i*
l	*k*	*i*	*h*	*j*	*g*	*j*
m	*l*	*j*	*i*	*k*	*h*	*k*
n	*m*	*k*	*j*	*l*	*i*	*l*
o	*n*	*l*	*k*	*m*	*j*	*m*
p	*o*	*m*	*l*	*n*	*k*	*n*
q	*p*	*n*	*m*	*o*	*l*	*o*
r	*q*	*o*	*n*	*p*	*m*	*p*
s	*r*	*p*	*o*	*q*	*n*	*q*
t	*s*	*q*	*p*	*r*	*o*	*r*
u	*t*	*r*	*q*	*s*	*p*	*s*
v	*u*	*s*	*r*	*t*	*q*	*t*
w	*v*	*t*	*s*	*u*	*r*	*u*
x	*w*	*u*	*t*	*v*	*s*	*v*
y	*x*	*v*	*u*	*w*	*t*	*w*
z	*y*	*w*	*v*	*x*	*u*	*y*

et gardait sa valeur. Cette élimination faite, le calcul de l'écartement des polygrammes donne :

$cy \quad 30 = 2 \times 3 \times 5$

$vv \quad 73 = 73$

$vw \quad 116 = 2^2 \times 29$

$ay \quad 66 = 2 \times 3 \times 11$

$gz \quad 105 = 3 \times 5 \times 7$

$yv \quad 60 = 2^2 \times 3 \times 5$

kir	$42 = 2 \times 3 \times 7$	*nb*	$35 = 5 \times 7$
nit	$53 = 53$	*wm*	$43 = 43$
ij	$40 = 2^3 \times 5$	*jk*	$50 = 2 \times 5^2$
ng	$84 = 2^2 \times 3 \times 7$	*zm*	$8 = 2^3$
yizm	$40 = 2^3 \times 5$	*mz*	$11 = 11$
oa	$59 = 59$		

Aucun résultat n'est évident, sauf celui-ci, que l'extrême divergence des possibilités indique une clef longue pour un texte court. En tenant compte de la prévalence énorme qui doit être attribuée à un tétragramme *(yizm = $2^3 \times 5$)* sur les groupements inférieurs, la vraisemblance est qu'il y a $2 \times 5 = 10$ alphabets, hypothèse confirmée par les bigrammes *cy (30), yv (60), ij (40), jk (50).*

En répartissant le texte par tranche de dix chiffres, nous obtenons un tableau alphabétique relativement très pauvre où nous discernons cependant une interprétation très probable pour les 1er *(z = e)*, 5e *(i = e)*, 9e *(y = e)*. En substituant des valeurs aux signes dans le texte chiffré, on obtient ainsi un cadre, où rapidement les mots viennent se compléter. C'est ainsi que le groupement *yizm*, déjà utilisé pour le calcul des écartements, et qui nous donne « *.o.r.* », interprété par *pour*, fournira la transcription des huitième et dixième alphabets. La lecture du cryptogramme n'offre plus désormais aucune difficulté. On a :

o i m p à a l c y q j v v
t u é t a i s t é m o i n etc.

Le travail est d'ailleurs facilité par la présence des *a* non modifiés, comme il a été dit plus haut.

*
* *

Mais parfois, aussi, le texte est tellement court que les théorèmes ne donnent aucune indication utile. Il faut alors tenter de reconstituer la clef, travail généralement très dé-

licat et qui peut être impossible. J'ai eu à traduire le texte suivant :

HCV YLVK NLâITQJ
NâKACAZ QM Hâ NBBCYZ QD IIUXKCR
ZH RA AAXVM HâDYNIPVAY PZPPAG
VM CâYD â CNIFMM DSPFB ZI
EBCâVZ â JEIFMXN QâFKAP

La méthode de chiffrage, s'il s'agissait d'une interversion, était certainement polyalphabétique, puisque deux mots, *aaxvm* et *iiuxkcr*, commencent par deux initiales semblables, ce qui ne se peut pas en français. D'autre part, on ne pouvait guère songer à un système de transposition ou de grille. Au surplus, la découverte, dans les papiers de l'auteur, qui est un bandit des plus redoutables et extrêmement intelligent, d'une table carrée de Vigenère, reproduite ci-contre, levait tous les doutes.

Le calcul de l'écartement des polygrammes ne donnait que des chiffres absolument discordants. On en pouvait seulement conclure à la longueur du mot-clef, qu'il s'agissait donc de reconstituer. Les essais portèrent sur les bigrammes, tels que *qm*, *hâ*, *qd*, etc. Sachant que, comme dans le cas précédent, l'*a* accentué gardait sa valeur, le groupe *qm hâ* ne pouvait avoir que l'un des sens suivants : « *de ma, de ta, de sa, de la, si ma, si ta, si sa, si la* ». Avec le sens *de la*, la table de Vigenère donnait (la première colonne verticale étant l'alphabet clair, la première horizontale est celui de la clef ; en cherchant comme dans une table de Pythagore, on trouve dans le tableau le produit du clair par la clef) :

Clair :	*d e*	*l ā*
Clef :	*n i*	*v .*
Chiffré :	*q m*	*h ā*

Le son *niv* étant possible en français, il fallait chercher la liste des mots qui le contiennent : *Ninive, enivrer, univers*, etc. Avec *université*, on obtenait :

H C V X L V K N L á I T Q J etc.
u n i v e r s i t (é) u n i v
m o n c h e r f r a m g i n

Le reste n'offrait plus aucune difficulté. Mais, si le scripteur n'avait pas séparé les mots et n'avait pas eu l'impru-

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*
b	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*
c	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*
d	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*
e	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*
f	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*
g	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*
h	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*
i	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*
j	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*
k	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*
l	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*
m	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*
n	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*
o	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*
p	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*
q	*r*	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*
r	*s*	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*
s	*t*	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*p*	*r*
t	*u*	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*
u	*v*	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*p*	*r*	*s*	*t*
v	*x*	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*
x	*y*	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*
y	*z*	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*
z	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*x*	*y*

Table carrée de Vigenère.

dence de commencer par *Mon cher* et de finir par son prénom comme signature, il est certain que ce cryptogramme eût été sinon indéchiffrable, du moins d'une difficulté extrême.

*
* *

Je ne veux pas m'étendre davantage ni exposer, même dans

leurs principes, les autres méthodes de cryptographie : clefs variables, transposition, grille, dictionnaires chiffrés, d'une lecture bien plus difficile. Le policier expert doit cependant les connaître, car il peut les rencontrer dans les affaires d'escroquerie ou de vol par des bandes fortement et savamment organisées, et dans les affaires d'espionnage. J'ai voulu montrer seulement par quelques exemples qu'il y a là une branche de la technique policière d'une utilité courante et beaucoup trop peu connue.