Quelques méthodes de chiffrement

Graham A. Niblo (2008) *

Chiffre de César

La méthode la plus élémentaire pour chiffrer un message est de remplacer chaque lettre par une autre selon une règle fixe. Par exemple, on peut remplacer chaque lettre a par la lettre D, chaque lettre b par la lettre E, etc...

Ici, on remplace chaque lettre par celle qui est trois rang plus loin dans l'alphabet. En appliquant cette méthode au paragraphe précédent, on obtient :

OD PHWKRGH OD SOXV VLPSOH SRXU FKLIIUHU XQ PHVVDJH HVW GH UHPSODFHU FKDTXH OHWWUH SDU XQH DXWUH VHORQ XQH UHJOH ILAH. SDU HAHPSOH, RQ SHXW UHPSODFHU FKDTXH OHWWUH D SDU OD OHWWUH G, FKDTXH OHWWUH E SDU OD OHWWUH H, HWF...

Par convention, on écrira le texte chiffré en majuscules et le texte clair en minuscules, en ignorant les accents.

Cette méthode de chiffrement (ou simplement chiffre) est connue sous le nom de chiffrement par décalage, puisque chaque lettre de l'alphabet est décalée d'un rang fixe, ou de chiffre de César, car Jules César l'utilisait déjà. Pour déchiffrer un tel chiffre, il suffit de trouver le décalage utilisé, ce qui peut se faire en trouvant par quelle lettre du texte chiffré est remplacée une lettre donnée du texte clair. Ici, on peut voir que le mot OD apparaît trois fois, et deviner qu'il s'agit du mot « le »ou « la ». On voit rapidement que si la lettre l est encodée par O, il s'agit du mot « la »et on déduit rapidement le reste du message.

*Traduction française par Auguste Olivry (2015), d'après « On substitution ciphers ».

En fait, il n'y a que 26 chiffres de César possibles dont le chiffre qui ne modifie pas le message (celui où chaque lettre est remplacée par . . . elle-même), donc il est assez facile de déchiffrer le message en essayant chaque décalage possible jusqu'à trouver le bon : on dit qu'on résout par force brute.

Chiffre de substitution par mot-clé

Pour rendre le texte plus difficile à déchiffrer, il nous faut augmenter la taille de notre famille de chiffres. Un bon exemple est le chiffre de substitution. Dans ce procédé, on choisit un mot ou une expression pour générer une permutation de l'alphabet. Pour cela, on écrit le mot ou l'expression, sans accents ni espaces, en omettant tous les caractères répétés. Ainsi, si l'on choisit l'expression « Ornithorynque »cela donnera `ORNITHYQUE`. On complète ensuite avec les lettres de l'alphabet restantes, dans l'ordre, ce qui nous donne `ORNITHYQUEABCDFGJKLMPSVWXZ`. On l'écrit en dessous de l'alphabet standard et on obtient une table de chiffrement :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
O	R	N	I	T	H	Y	Q	U	E	A	B	C	D	F	G	J	K	L	M	P	S	V	W	X	Z

En choisissant comme mot-clé un pangramme, c'est à dire une phrase qui contient toutes les lettres, par exemple « *Portez ce vieux whisky au juge blond qui fume* », on évite de devoir compléter l'alphabet, mais ce n'est pas nécessaire pour avoir un nombre suffisant de permutations possibles. Sous réserve de trouver une expression appropriée, il peut y en avoir jusqu'à $26! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot 26$, qui est de l'ordre de 10^{26}. Malheureusement, on peut casser ce chiffre sans tester toutes les possibilités.

Prenons le texte suivant :

E'MKMSZMHU WU XDSVZIJRIU JS MEFAMOUZ WU XARCCIUHUSZ WU XUZZU HMSRUIU UVZ GJ'RE UVZ ZIUV CMXREU WU HUHDIRVUI EU HDZ DJ E'UNFIUVVRDS JZRERVU, UZ WDSX E'MEFAMOUZ WU XARCCIUHUSZ. X'UVZ ZIUV RHFDIZMSZ, XMI VR E'UHUZZUJI WJ HUVVMHU WDRZ UXIRIU E'MEFAMOUZ WU XARCCIUHUSZ VJI JS ODJZ WU FMFRUI, XUEJR-XR FUJZ ZDHOUI USZIU EUV HMRSV WU E'USSUHR, GJR XDSSMRZ MEDIV EM XEU WU XARCCIUHUSZ UZ FUJZ WUXARCCIUI ZDJZU XDHHJSRXMZRDS GJR M UZU USXDWUU MKUX. MJ XDSZIMRIU, VR EM XEU UVZ JSRGJUHUSZ HUHDIRVUU, EUV XAMSXUV GJU E'USSUHR EM WUXDJKIU VDSZ FEJV CMROEUV.

On peut commencer par utiliser la ponctuation : on remarque que la

séquence E' apparaît régulièrement, et devant des mots très différents, ce qui indique que c'est probablement le chiffré de l'article l' . On remarque ensuite les mots EU et EM , qui sont donc probablement les chiffrés des mots le et la . Pour savoir à quoi correspond quelle lettre, on peut observer que la lettre M apparaît seule, ce qui fait pencher en faveur de la lettre a. De plus on peut vérifier que la lettre U est de loin la plus fréquente dans ce texte, tout comme la lettre e est la plus fréquente en français. On commence ainsi à déchiffrer le texte, en remplaçant E, U et M par l, e et a respectivement :

l'aKaSZaHe We XDSVZIJRIe JS alFAaOeZ We XARCCIeHeSZ We XeZZe HaSReIe
eVZ GJ'Rl eVZ ZIeV CaXRle We HeHDIRVeI le HDZ DJ l'eNFIeVVRDS JZRlRVe,
eZ WDSX l'alFAaOeZ We XARCCIeHeSZ. X'eVZ ZIeV RHFDIZaSZ, XaI VR l'eHeZZeJI
WJ HeVVaHe WDRZ eXIRIe l'alFAaOeZ We XARCCIeHeSZ VJI JS ODJZ We FaFReI,
XelJR-XR FeJZ ZDHOeI eSZIe leV HaRSV We l'eSSeHR, GJR XDSSaRZ alDIV la Xle
We XARCCIeHeSZ eZ FeJZ WeXARCCIeI ZDJZe XDHHJSRXaZRDS GJR a eZe eSXDWee
aKeX. aJ XDSZIaRIe, VR la Xle eVZ JSRGJeHeSZ HeHDIRVee, leV XAaSXeV GJe
l'eSSeHR la WeXDJKIe VDSZ FlJV CaROleV.

On peut continuer en remarquant que la séquence « leV »apparaît deux fois, et que la lettre V est souvent en fin de mot, et on la remplace par la lettre s :

l'aKaSZaHe We XDSsZIJRIe JS alFAaOeZ We XARCCIeHeSZ We XeZZe HaSReIe
esZ GJ'Rl esZ ZIes CaXRle We HeHDIRseI le HDZ DJ l'eNFIessRDS JZRlRse,
eZ WDSX l'alFAaOeZ We XARCCIeHeSZ. X'esZ ZIes RHFDIZaSZ, XaI sR l'eHeZZeJI
WJ HessaHe WDRZ eXIRIe l'alFAaOeZ We XARCCIeHeSZ sJI JS ODJZ We FaFReI,
XelJR-XR FeJZ ZDHOeI eSZIe les HaRSs We l'eSSeHR, GJR XDSSaRZ alDIs la Xle
We XARCCIeHeSZ eZ FeJZ WeXARCCIeI ZDJZe XDHHJSRXaZRDS GJR a eZe eSXDWee
aKeX. aJ XDSZIaRIe, sR la Xle esZ JSRGJeHeSZ HeHDIRsee, les XAaSXes GJe
l'eSSeHR la WeXDJKIe sDSZ FlJs CaROles.

On peut encore remarquer les nombreux « We », qui indiquent que la lettre W encode probablement la lettre « d », ainsi que les « eZ »et « esZ », qui indiquent que la lettre Z est probablement la lettre t. On obtient :

l'aKaStaHe de XDSstIJRIe JS alFAaOet de XARCCIeHeSt de Xette HaSReIe
est GJ'Rl est tIes CaXRle de HeHDIRseI le HDt DJ l'eNFIessRDS JtRlRse,
et dDSX l'alFAaOet de XARCCIeHeSt. X'est tIes RHFDItaSt, XaI sR l'eHetteJI
dJ HessaHe dDRt eXIRIe l'alFAaOet de XARCCIeHeSt sJI JS ODJt de FaFReI,
XelJR-XR FeJt tDHOeI eStIe les HaRSs de l'eSSeHR, GJR XDSSaRt alDIs la Xle
de XARCCIeHeSt et FeJt deXARCCIeI tDJte XDHHJSRXatRDS GJR a ete eSXDdee

aKeX. aJ XDStIaRIe, sR la Xle est JSRGJeHeSt HeHDIRsee, les XAaSXes GJe l'eSSeHR la deXDJKIe sDSt FlJs CaROles.

On peut continuer avec « Xette »et « X'est »qui donnent la lettre *c*, « sR »qui donne « si », puis on commence à reconnaître des mots plus longs, comme « alFAaOet »qui est probablement « alphabet », etc... On obtient finalement cet extrait de l'excellent ouvrage de Simon Singh *Histoire des codes secrets : De l'Égypte des pharaons à l'ordinateur quantique* (*The Code Book* en anglais) :

« L'avantage de construire un alphabet de chiffrement de cette manière est qu'il est très facile de mémoriser le mot ou l'expression utilisé, et donc l'alphabet de chiffrement. C'est très important, car si l'émetteur du message doit écrire l'alphabet de chiffrement sur un bout de papier, celui-ci peut tomber entre les mains de l'ennemi, qui connaît alors la clé de chiffrement et peut déchiffrer toute communication qui a été encodée avec. Au contraire, si la clé est uniquement mémorisée, les chances que l'ennemi la découvre sont plus faibles. »

Analyse fréquentielle

Une manière plus systématique d'attaquer le chiffrement par substitution est l'analyse fréquentielle. On compare la fréquence de chaque caractère dans le texte chiffré et on la compare avec la fréquence moyenne des lettres dans la langue française. Voici la fréquence en pourcentage des lettres dans le texte chiffré précédent :

A	B	C	D	E	F	G	H	I	J	K	L	M
2,0	0,0	2,7	4,5	5,7	2,3	1,1	5,0	6,4	5,2	0,7	0,0	6,4
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0,2	1,4	0,0	0,0	7,5	6,4	0,0	18,9	5,7	3,4	5,7	0,0	8,9

Comparons la avec les fréquences moyennes de chaque lettre en français :

a	b	c	d	e	f	g	h	i	j	k	l	m
9,4	1,0	2,6	3,4	15,9	0,9	1,0	0,8	8,4	0,9	0,0	5,3	3,2
n	o	p	q	r	s	t	u	v	w	x	y	z
7,1	5,1	2,9	1,1	6,5	7,9	7,3	6,2	2,1	0,0	0,3	0,2	0,3

En utilisant cela, ainsi que des informations sur les mot courants de une, deux ou trois lettres, nous avons assez d'éléments pour commencer a attaquer ce chiffre.

Déguiser la structure des mots

Pour l'instant, la faiblesse de nos chiffres résidait dans la préservation de la structure des mots et de la ponctuation (souvenez-vous du « l' »), car cela permet d'identifier les mots fréquents. Pour éviter cela, les cryptologues suppriment en général la ponctuation et les espaces et regroupent les caractères par blocs de quatre ou cinq. Ainsi le chiffré précédent ressemble à ceci :

```
EMKMS ZMHUW UXDSV ZIJRI UJSME FAMOU ZWUXA RCCIU HUSZW UXUZZ UHMSR
UIUUV ZGJRE UVZZI UVCMX REUWU HUHDI RVUIE UHDZD JEUNF IUVVR DSJZR
ERVUU ZWDSX EMEFA MOUZW UXARC CIUHU SZXUV ZZIUV RHFDI ZMSZX MIVRE
UHUZZ UJIWJ HUVVM HUWDR ZUXIR IUEME FAMOU ZWUXA RCCIU HUSZV JIJSO
DJZWU FMFRU IXUEJ RXRFU JZZDH OUIUS ZIUEU VHMRS VWUEU SSUHR GJRXD
SSMRZ MEDIV EMXEU WUXAR CCIUH USZUZ FUJZW UXARC CIUIZ DJZUX DHHJS
RXMZR DSGJR MUZUU SXDWU UMKUX MJXDS ZIMRI UVREM XEUUV ZJSRG JUHUS
ZHUHD IRVUU EUVXA MSXUV GJUEU SSUHR EMWUX DJKIU VDSZF EJVCM ROEUV
```

En général, la taille des blocs a peu d'importance, sauf éventuellement dans l'analyse du chiffre de Vigenère (voir plus loin), où une taille de bloc bien choisie peut permettre de faire ressortir la longueur de la clé, en rendant les répétitions plus évidentes.

Pour attaquer un chiffré qui a été regroupé de cette manière, il nous faut travailler directement sur les lettres et non plus sur les mots. Pour cela, on utilise l'analyse fréquentielle décrite plus haut, agrémentée d'un peu de jugement (ou de chance). Cela peut être long et difficile, mais l'issue de certaines guerres a dépendu de tels procédés.

« C'était laborieux, mais cela ne dérangeait pas Jericho. Il faisait quelque chose, c'était le principal. C'était comme l'attaque de codes secrets. La règle était de toujours faire quelque chose, même en situation désespérée. Comme le disait Alan Turing :"aucun cryptogramme n'a jamais été résolu en le regardant bêtement." »Enigma, Robert Harris

Chiffre affine

Malgré les avantages de l'utilisation d'un chiffre par mot-clé pour un agent, la plupart des chiffres modernes sont automatisés et reposent sur des algorithmes de chiffrement mathématiques. Le chiffre de César peut par exemple être vu comme tel :

On commence par coder chaque lettre par sa position dans l'alphabet (en partant de 0) :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	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

Puis on décale l'alphabet en ajoutant 3 à chaque position :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2

Les additions sont faites ici modulo 26, c'est à dire que lorsqu'on atteint 25 on repart de 0.

Enfin, on remplace les chiffres par les lettres qu'ils représentent :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

On retrouve la table de chiffrement du chiffre de César avec un décalage de 3 du début de ce cours.

On peut représenter le chiffre de César avec un décalage de n par la transformation $x \mapsto x+n$. Ici x représente la position d'une lettre (entre 0 et 25), et n le décalage (également entre 0 et 25). Clairement, puisque le chiffre est défini uniquement par n il y a exactement 26 chiffres de César.

Il existe une classe plus vaste de chiffres pouvant s'exprimer comme des transformations arithmétiques, appelés chiffres affines. Ils utilisent le fait qu'on peut également multiplier dans l'arithmétique modulo 26. Plutôt que de les introduire formellement directement, ce qui serait un peu lourd, nous allons l'illustrer par un exemple

Le chiffre affine $x \mapsto 3x + 5$

Comme précédemment, on part du tableau des positions, mais au lieu de remplacer la position x par $x + 3$, on la remplace cette fois-ci par le nombre $3x + 5$, toujours pris modulo 26. Autrement dit, si deux nombrent diffèrent par un multiple de 26 on dit qu'il sont congruents modulo 26. Par exemple $101 \equiv 23 \pmod{26}$ (est congruent à 23 modulo 26) car 23 est le reste à la division de 101 par 26. Ainsi,

$$\begin{aligned} 2 &\mapsto 3 \cdot 2 + 5 = 11, \\ 8 &\mapsto 3 \cdot 8 + 5 = 29 \equiv 3 \pmod{26}. \end{aligned}$$

On obtient la table suivante :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
5	8	11	14	17	20	23	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2

On peut également écrire les chiffres affines sous la forme $x \mapsto ax + b$, et les chiffres de César sont simplement les cas où $a = 1$.

On peut remarquer que les chiffres $x \mapsto x+3$ et $x \mapsto 3x+5$ chiffrent tous deux la lettre y par la lettre B, puisque $24+3 = 27 = 26+1 \equiv 1 \pmod{26}$ et $3 \cdot 24+5 = 80 = 3 \cdot 26+1 \equiv 1 \pmod{26}$. Ainsi deux chiffres affines différents peuvent chiffrer une même lettre de la même façon, et il ne suffit plus de déterminer le chiffré d'une unique lettre pour déchiffrer le message. Puisqu'il y a deux degrés de liberté (a et b) dans notre choix de chiffre affine, on peut espérer que connaître le chiffré de deux lettres est suffisant. Il l'est en effet, car si l'on connaît deux valeur de l'expression $ax + b$, on peut résoudre le système à deux équations correspondant pour trouver a et b.

Vous avez probablement l'habitude de résoudre ce type de systèmes pour des nombres réels, mais la même méthode marche pour l'arithmétique modulaire, avec la différence qu'on ne peut pas toujours diviser. Cette différence a une interprétation simple : pour que la règle $x \mapsto ax + b$ définisse un chiffre, il faut que tous les nombres entre 0 et 25 apparaissent une et une seule fois dans la liste de nombres $ax + b$ pour x variant de 0 à 25. Si l'on ne fait pas attention il se peut que ça ne soit pas le cas (c'est à dire qu'on ne peut pas diviser par a modulo 26).

Par exemple la règle $x \mapsto 2x$ chiffre a la fois la lettre c et la lettre p par la lettre E, car $2 \cdot 2 = 4$ et $2 \cdot 15 = 30 = 4 \pmod{26}$. Ce n'est donc pas un bon chiffre car différents messages clairs sont chiffrés de la même manière :

les mots « cas »et « pas »sont tous deux chiffrés par EAK.

Formellement, un système de chiffrement définit une fonction de l'alphabet sur lui-même, et il faut que cette fonction soit inversible pour que le chiffre soit déchiffrable de manière unique. En arithmétique, cela se traduit par le fait que a doit être premier avec 26, c'est à dire que $\text{pgcd}(a, 26) = 1$. Il y a 12 nombres inférieurs à 26 qui ont cette propriété : les nombres impairs différents de 13. Pour chaque valeur de a on a 26 choix possibles pour b, ce qui donne 312 chiffres affines possibles. Ainsi l'attaque par force brute sans analyse de fréquence est plus laborieuse que pour le chiffre de César.

Chiffres polyalphabétiques

La principale faiblesse des chiffres de substitution vient du fait que les lettres sont distribuées très irrégulièrement dans un texte français (ou dans n'importe quelle autre langue).

Pour pallier cela, il faut donc cacher les fréquences des lettres du texte clair, et une manière de faire est d'utiliser un chiffre polyalphabétique. Avec ce type de chiffres, une même lettre du texte clair peut être encodée de plusieurs manières dans le texte chiffré. La lettre e, par exemple, pourra être encodée une fois par X, et une autre fois par G. Cependant on ne peut pas choisir la lettre au hasard si l'on veut être capable de décoder le texte par la suite. La méthode connue sous le nom de chiffre de Vigenère donne une solution élégante.

Dans un texte chiffré par le chiffre de Vigenère, chaque lettre est encodée par un chiffre de César, mais la valeur du décalage change à chaque lettre. Pour que le message soit déchiffrable, il faut que les deux parties (l'émetteur et le destinataire) choisissent une séquence de décalages connue d'eux seuls. Par exemples, elles peuvent se mettre d'accord sur la séquence 21, 8, 6, 4, 13, 4 17, 4, qui sera ensuite répétée pour encoder tout le texte : 21, 8, 6, 4, 13, 4 17, 4, 21, 8, 6, 4, 13, 4 17, 4,...

Pour déchiffrer, le destinataire décale la première lettre de 21 rangs en arrière, la seconde de 8, etc. jusqu'à retrouver le texte original. Comme une séquence de chiffres n'est pas facile à retenir, on réutilise l'idée du chiffre par mot-clé qui consiste à faire correspondre les lettres et les chiffres de 0 à 15. Ici la séquence 21, 8, 6, 4, 13, 4 17, 4 donne le mot *vigenere*. Ainsi les deux

parties ont simplement à choisir un mot ou une expression pour définir un chiffre de Vigenère.

Un tel chiffre est beaucoup plus difficile à casser que les précédents. Ils existe cependant des méthodes, et nous recommandons celle de Babbage et Kasiski, qui l'ont découverte indépendamment et qui est basée sur la régularité de la répétition du mot-clé. On utilise l'analyse des séquences de lettres répétées pour deviner la longueur de la clé, et une fois la longueur choisie on utilise une analyse fréquentielle sur chaque partie du texte chiffrée par le même décalage.

Chiffres de transposition

Parfois, en étudiant la fréquence des lettres d'un texte chiffré, vous observerez que chaque lettre apparaît individuellement avec une fréquence proche de celle qui serait attendue dans un texte en français (ou la langue du texte original). Cela signifie que le texte n'a pas été chiffré par un chiffre de substitution, mais plutôt par un chiffre de transposition, ou chiffre par anagramme. Dans un tel chiffre, au lieu de remplacer les lettres, celles-ci sont permutées en utilisant une règle qui permet de les réordonner pour retrouver le message original.

Par exemple, nous allons chiffrer le texte suivant : *Portez ce vieux whisky au juge blond qui fume.* On commence par choisir un mot-clé, par exemple *OUI.* On l'écrit en haut d'un tableau à trois colonnes puis on inscrit le texte chiffré en-dessous.

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

Les deux dernières cases sont complétées pas des « x ».

On réordonne ensuite les colonnes de sorte que les lettres du mot-clé soient dans l'ordre alphabétique :

I	O	U
R	P	O
Z	T	E
V	C	E
U	I	E
H	X	W
K	I	S
U	Y	A
G	J	U
L	E	B
D	O	N
I	Q	U
M	F	U
X	E	X

Ce qui nous donne alors comme chiffré :

```
RPOZTEVCEUIEHXWKISUYAGJULEBDONIQUMFUXEX
```

Si le mot-clé contient des lettres répétées, on les supprime comme pour le

mot-clé d'un chiffre de substitution. Ainsi, si on avait choisi comme mot-clé *ANNEE*, on aurait utilisé une grille à trois colonnes avec en tête *ANE*, puis on aurait réordonné les colonnes pour obtenir *AEN*.

Comment attaquer un tel chiffre ?

Il est assez clair que la longueur du mot-clé est un point essentiel. Il est possible de la deviner par la longueur du texte chiffré, qui en sera un multiple. Dans notre exemple, le chiffré est de longueur 39 donc la clé pourrait être de taille 3 ou 13. On commence par essayer une clé de longueur 3, donc on écrit le texte en 3 colonnes et on obtient le deuxième tableau ci-dessus. Notre meilleure chance de trouver la solution rapidement est de trouver un mot de texte. Si vous connaissez un mot qui a de grandes chances de se trouver dans le texte, il faut chercher des anagrammes de ce mot. Ce n'est pas toujours facile à cause de la division du texte en blocs, car si le mot ne prend pas toute la ligne, il sera mélangé avec les autres lettres. Au contraire, s'il est trop long, il risque de s'étaler sur plusieurs lignes et il faut alors chercher des anagrammes de parties du mot.

Dans notre exemple le mot « qui »est idéal : il est transformé sur la douzième ligne en « IQU ». En déplaçant la dernière colonne à la fin, nous avons déchiffré le message.

Bien sûr, pour une clé de 3 caractères il est très rapide de tester les 5 permutations possibles (en excluant la permutation qui ne change pas le texte) mais ces méthodes permettent de résoudre à la main ce type de chiffres pour des mot-clés un peu plus longs.

C'est évidemment plus difficile si le texte est dans une langue que vous ne maîtrisez pas puisque vous aurez plus de mal à déterminer ce qui a du sens. Si seule une partie du message est dans votre langue, il est possible de déchiffrer cette partie puis d'utiliser l'information sur la clé pour déchiffrer l'intégralité du message.

D'autres indices plus subtils peuvent être utiles : par exemple en français la lettre q est presque systématiquement suivie d'un u.