Crypotagraphie : Partie I

Un peu de vocaublaire :

⋆ **Chiffrement :** procédé suivant lequel un document compréhensible de tous est transformé en un autre, incompréhensible.

⋆ **Déchiffrement :** procédé inverse.

⋆ **Un algorithme cryptographique :** est un procédé mathématique utilisé pour le chiffrement et le déchiffrement. Il décrit pas à pas toutes les étapes nécessaires à la transformation du document

I Le codage César

I.1 Définition et Exemples

Définition 1 *Lors de ses batailles, l'empereur romain JULES CÉSAR cryptait les messages qu'il envoyait à ses généraux. Sa méthode de codage consistait à décaler les lettres de 3 rangs, vers la droite, dans l'alphabet.*

Cette méthode de cryptage est appelée ***chiffrement de César, ou Code César****.*

Le nombre de rangs de décalage des lettres est appelé ***la clé****. (JULES CÉSAR employait donc la clé égale à 3).*

Exemple 1

1. Coder le mot "ENQUETE" avec le code César de clé 3.
2. Décoder le message " ERQ GHEXW" qui a été codé par le code César de clé 3.

I.2 Codage

On peut coder un message à l'aide du code César avec n'importe quelle clé n, où n est un entier naturel. Quelle condition vérifie cependant l'entier n ?

Un exemple : avec la clé 17

1. Crypter la lettre C à l'aide du code César avec clé 17.
2. Crypter la lettre M à l'aide du code César avec clé 17.
3. Proposer une méthode rapide pour coder en code César.
4. Crypter à l'aide de votre méthodeun message et faites le décoder à votre voisin.

I.3 Décodage : la méthode d'Al-Kindi

Les possibilités de codage sont très nombreuses mais le déchiffrement d'un texte chiffré par un code César est possible.

Les savants arabes sont les inventeurs de la cryptanalyse. C'est une méthode permettant de décrypter les méssages codés. Les lettres du texte sont remplacées par d'autres lettres de la façon suivante :

- Deux lettres différentes sont codées de façon différente.
- La même lettre est toujours codée de la même façon.

Le premier traité exposant une procédure pour décrypter un texte codé de cette manière à été écrit par AL-Kindi au neuvième siècle après J.C. Sa théorie repose sur le fait que dans un texte, les lettres ont des fréquences d'apparition différentes. Par exemple, en français, la fréquence de la lettre E, est selon le texte presque toujours supérieure aux fréquences des autres lettres.

Selon sa théorie, il y a donc de fortes chances pour que , dans un texte codé, la lettre qui apparaît le plus fréquemment représente un E. Les lettres les moins fréquentes représentent probablement un W, un K, un Z ...

Le tableau ci-dessous exprime, en pourcentage, les fréquences moyennes, des letrtes utilisées dans les textes écrits en français :

A	B	C	D	E	F	G	H	I	J	K	L	M
7,68	0,8	3,32	3,6	17,76	1,06	1,1	0,64	7,23	0,19	0	5,89	2,72

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7,61	5,34	3,24	1,34	6,81	8,23	7,3	6,05	1,27	0	0,54	0,21	0,07

On considère le message codé suivant dans lequel les espaces ont été supprimés. En utilisant la méthode statistique, trouver la clé et déchiffrer le message suivant :

BWFWKMAKHSKSJJANWSVWUJQHLWJUWEWKKSYW

Quel est donc l'inconvéniement majeur du code César ?

II Codage affine

II.1 Principe

A chaque lettre est associée un nombre entier n selon son rang dans l'alphabet de 0 pour la lettre A à 25 pour la lettre Z.

Deux nombres a et b sont choisis comme clés.

Méthode :

- ⋆ Au nombre n de départ, on associe le nombre $m = an + b$.
- ⋆ Ce nombre m n'étant pas toujours compris entre 0 et 25, il ne permet pas de chiffrer une lettre.
- ⋆ Pour résoudre ce problème, le codage se fait en associant au nombre de départ n le nombre entier p, reste de la division euclidienne de m par 26.
- ⋆ Puis, on retranscrit p en lettres.

Par exemple, si on prend $a = 4$ et $b = 1$.

La lettre Z est remplacée par $n = 25$.

Puis $m = 4 \times 25 + 1 = 101$.

Or 101 n'est pas compris entre 0 et 25, on effectue donc la division euclidienne de 101 par 26 ce qui donne :

$101 = 3 \times 26 + 23$.

Donc $p = 23$ qui correspond à la lettre X. Z est donc codée par X.

II.2 Un exemple

On prend $a = 3$ et $b = 7$, compléter les tableaux suivants :

Lettre décodée	A	B	C	D	E	F	G	H	I
n									
m									
p									
Lettre décodée									

Lettre décodée	J	K	L	M	N	O	P	Q	R
n									
m									
p									
Lettre décodée									

Lettre décodée	S	T	U	V	W	X	Y	Z
n								
m								
p								
Lettre décodée								

1. Coder une phrase de votre choix avec la clé $(3; 7)$.
2. Décrypter la phrase RXF HPJJF avec la clé $(3; 7)$ ainsi que celle de votre voisin.
3. On prend maintenant pour clé le couple $(2; 13)$. Coder alors le mot ENTIER. Quel problème apparaît dans ce codage ?

III Codage à l'aide d'une table de Vignère

Même si l'on connaissait depuis fort longtemps les faiblesses de la cryptographie par substitution, il n'y eut pas entre César et le XVI ème siècle de véritable nouveau procédé cryptographique, à la fois sûr et facile à utiliser. Blaise de Vigenère, né en 1523, fut l'initiateur d'une nouvelle façon de chiffrer les messages qui domina 3 siècles durant.

Vigenère était quelqu'un de très hétéroclite, tantôt alchimiste, écrivain, historien, il était aussi diplomate au service des ducs de Nevers et des rois de France. C'est en 1586 qu'il publie son *Traité des chiffres ou Secrètes manières d'écrire*, qui explique son nouveau chiffre (le texte intégral est disponible sur le site de la Bibliothèque Nationale de France).

L'idée de Vigenère est d'utiliser un chiffre de César, mais où le décalage utilisé change de lettres en lettres. Pour cela, on utilise une table composée de 26 alphabets, écrits dans l'ordre, mais décalés de ligne en ligne d'un caractère. On écrit encore en haut un alphabet complet, pour le texte à coder, et à gauche, verticalement, un dernier alphabet, pour la clé .

Il s'agit de la table de Vigenère 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
A	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
B	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	A
C	C	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
D	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
E	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	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	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
X	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	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

III.1 Principe de chiffrement avec la table :

A chaque lettre en clair, on sélectionne la colonne correspondante tandis que la lettre de la clé se sélectionne par ligne, au croisement de la ligne et de la colonne on trouve la lettre chiffrée.

Texte en clair : **D**ECODER C EST GENIAL
Clé répétée : **C**LE

La première lettre vaut : Colonne **D**, ligne **C** : on obtient la lettre **F**.

La deuxième lettre vaut : Colonne **E**, ligne **L** : on obtient la lettre **P**.

La troisième lettre vaut : Colonne **C**, ligne **E** : on obtient la lettre **G**.

La quatrième lettre vaut : Colonne **O**, ligne **C** : on obtient la lettre **Q**.

.....

Poursuiver cette méthode pour coder le texte.

III.2 Principe de déchiffrement avec la table :

On regarde pour chaque lettre de la clé répétée, la ligne correspondante sur laquelle on cherche la lettre chiffrée. Le nom de la colonne donne la lettre déchiffrée.

Texte chiffré : FPGQOIT N IUE KGYMCW
Clé répétée : CLE

La première lettre vaut : Colonne **C**, on cherche **F** : on trouve la colonne **D**.

La deuxième lettre vaut : Colonne **L**, on cherche **P** : on trouve la colonne **E**.

La troisième lettre vaut : Colonne **E**, on cherche **G** : on trouve la colonne **C**.

La quatrième lettre vaut : Colonne **C**, on cherche **Q** : on trouve la colonne **O**.

.....

III.3 Application

Décoder le texte suivant (la clé est FONCTION)

QSF OTBVRROGKJCSF H SFV MZCC GWRP

IV Annexe

IV.1 Retour sur l'enquête

Dans l'ordinateur de Rémi MOLETTE les enquêteurs ont retrouvé un mail suspect qui contenait le message suivant :

FETWTDPGTRPYPCPLGPNWLNWPXZWPEEPPEEFNZXACPYOCLD
EWEYFTFMBOSGGIEQPPTMIOCFXXKENWPRIEYEQSIK

Saurez-vous le déchiffrer ?

IV.2 Pour aller plus loin

Voici un texte codé par la méthode de chiffrement de Vigenère :

TMFASAYKBWVJELRIYLNMOMGROTRBOYHOZIEBSMAJBINJOKBJOZPKW
MFYKORYKVFJSACUCMEJOTNIVMRYDCAHYAFHBIIUXMNTWWVTCAVRZIEBS
MAZKARYPQAYMMFZACRPOTHOKCEGSAOOOVRDZTVWEMERKURZRWQK

On ne dispose pas de clé de codage. En combinant deux techniques, il est possible de trouver la longueur de la clé et des clés possibles :

- Repérer des groupes de lettres identiques dans le message, en pratique on cherche des groupes de 3 lettres. On évalue l'écart de position entre le groupe de lettres. Il est probablement un multiple de la longueur de la clé :
- Par le codage de Vigenère, la fréquence des lettres dans la langue française n'est pas modifiée ; comme l'on dispose d'une valeur possible de la longueur de la clé, on découpe le message codé en blocs de cette longueur. On fabrique ainsi en prenant les lettres en même position dans ces blocs des nouveaux textes dont le décalage avec le texte en clair est constant (chiffrement de César).

Essayer d'appliquer cette méthode au texte ci-dessus.