INTRODUCTION À LA CRYPTOGRAPHIE

Antoine Douteau[1]
[1]Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, FRANCE
[1]en thèse dirigée par Adeline Roux-Langlois
antoine.douteau@unicaen.fr

GREYC
Laboratoire de recherche en sciences du numérique

Mais qu'est ce que la cryptographie ?

D'où ça vient ? : la **cryptographie** vient des mots en grec ancien *kruptos* signifiant "caché" et *graphein* signifiant "écrire". C'est l'art de **cacher des messages** pour qu'ils ne soient compréhensibles que par les personnes sensées pouvoir les comprendre.

A quoi ça sert ? :

- Pour communiquer de manière secrète,
- Pour **sécuriser** les paiements par carte bancaire et en ligne,
- Pour **protéger** des informations importantes des pirates.

Vocabulaire

Comme tout domaine scientifique, la cryptographie a son vocabulaire :

- **clair** : un (message) **clair** est un message à transmettre,
- **chiffré** : un message **chiffré** est inintelligible et dissimule un clair,
- **chiffrement** : modification d'un clair en un chiffré avec une clé,
- **déchiffrement** : restitution d'un chiffré en son clair initial,
- **clé secrète** : la clé secrète permet de chiffrer/déchiffrer correctement de manière à restituer le bon clair associé à un chiffré.

Activité 1.1

Correspondance lettre/position dans l'alphabet latin

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Figure 1: *Ordre des lettres et positions dans l'alphabet latin*

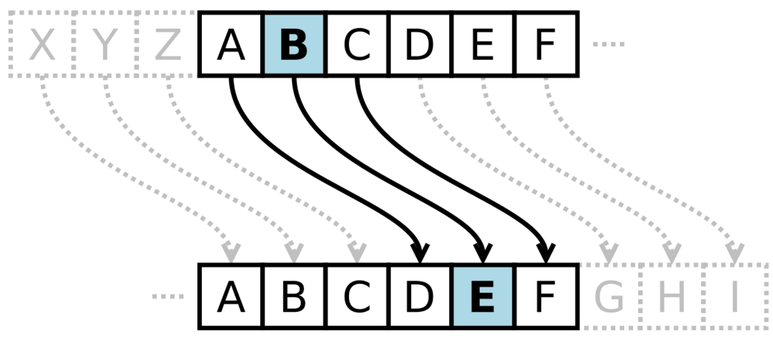

Figure 2: *Exemple visuel du décalage de César avec une clé valant 3*

Code de César

Jules César utilisait un code particulier pour chiffrer ses messages. Comment procédait-il ?
Premièrement, il identifiait les lettres comme des nombres correspondants à leur position dans l'alphabet $A = 1; B = 2; \ldots; Z = 26$.
Il utilisait une clé qui était un nombre qu'il additionnait à la position de chaque lettre de son message clair, puis il identifiait le nouveau mot en regardant les nouvelles lettres aux nouvelles positions.
Exemple : Si la clé est le nombre 3, et le clair est le mot *ABRICOT* : il regarde la table de décalage de 3 lettres suivantes :

clair / clé	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	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 trouve alors *DEULFRW* : on dit que *DEULFRW* est le **chiffré** de César du message **clair** *ABRICOT* pour une **clé** valant 3.
Le **déchiffrement** se passera de la même manière sauf qu'on soustrait la valeur de la clé à la position de chaque lettre du message chiffré.

A vous de jouer : De tête ou utilisant les outils à disposition, déchiffrez les différents messages ci-dessous :

1. *GBDJMF MB DSZQUPHSBQIJF* pour une clé valant 1,
2. *H'YG AMKNPGQ* pour une clé valant -2,
3. *LKZK JK RG YIOKTIK* pour une clé valant *F* (quand la clé est une lettre, on cherche la position de la lettre avant d'additionner cette valeur).

Analyse de fréquence

Si l'on utilise un même décalage, alors chaque lettre sera toujours chiffrée par une même autre lettre. Or, dans la langue française, certaines lettres sont plus fréquentes que d'autres. Par exemple, le *E* est plus utilisé que le *W*.
De même, on peut répérer des structures bien connues du langage dans un texte (les verbes finissant en *-er*, les pronoms, le pluriel, etc).

Lettre	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
Fréquence en %	7.6	0.9	3.3	3.7	14.7	1	0.9	0.7	7.5	0.6	0.1	5.5	3.0	7.0	5.8	2.5	1.4	6.7	7.9	7.2	6.3	1.8	0.1	0.4	0.1	0.3

Figure 4: *Fréquence moyenne de chaque lettre en langue française(dans un corpus de texte compilée par Thomas Tempé)*

A vous de jouer : De tête ou utilisant les outils à disposition, déchiffrez le message ci-dessous :

VK MEBSYCSDO OCD EX FSVKSX NOPKED WKSC EXO ZOBCYXXO WKV SXDOXDSYXXOO X'K AEO NOC NOPKEDC.

.

Chiffrement de Vigenère

Vigenère est un mathématicien français qui a détourné les codes de César pour chiffrer des messages en utilisant une technique similaire. Au lieu de chiffrer lettre par lettre avec la même clé, il utilisait un mot entier, qu'il répétait jusqu'à ce que le clair soit totalement chiffré.
Exemple : Si la clé est le mot *CLE*, et le clair est le mot *POMME* : On cherche les positions des lettres du mot *CLE* : $3 - 12 - 5$ puis on décale :

clé \ clair	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	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
+12	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
+5	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

On décale lettre par lettre en commençant par le décalage **+3**, puis **+12** puis **+5** puis on recommence jusqu'à chiffrer le mot entier.
On trouve alors *SARPQ* : on dit que *SARPQ* est le **chiffré** de Vigenère du message **clair** *POMME* pour la **clé** *CLE*.

A vous de jouer : De tête ou utilisant les outils à disposition, déchiffrez les différents messages ci-dessous :

1. *LBFRXJ* pour une clé valant *FACILE*,
2. *FZIXSJQ GBZD HSFTJ* pour une clé valant *SUPER CLE*,
3. Faites vos propres exemples entre vous.

Activité 1.2

Les chiffrements précédents étaient visuels et facilement réalisables avec une table de décalage.
Passons maintenant à des chiffrements nécessitant du calcul.

Chiffrement affine

Un autre exemple de chiffrement plus complexe est le chiffrement affine, lié à la fonction **affine** $f(x) = a \times x + b$. La clé sera ici le couple (a, b) et la sortie chiffrée sera l'opération $a \times x + b$ pour x valant la position de chaque lettre.
Exemple : Si la clé est $(3, 2)$, et le clair est le mot *BANANE* :

- Il cherche les positions de chaque lettre du mot *BANANE* : $2 - 1 - 14 - 1 - 14 - 5$,
- Il effectue le calcul $3 \times x + 2$ pour chaque position, ce qui donne : $8 - 5 - 44 - 5 - 44 - 17$,
- Il identifie les nouvelles lettres : *HERERQ*,
- On dit que *HERERQ* est le **chiffré** affine du message **clair** *BANANE* pour la **clé** $(3, 2)$.

A vous de jouer : De tête ou utilisant une calculatrice :

- Déchiffrez le message *TVQFS EJGGJDJMF* pour une clé valant $(1, 1)$.
- Chiffrez le message *BAOBAB* pour une clé valant $(5, 6)$. Donnez un autre couple (**clair, clé**) donnant le même **chiffré** ?