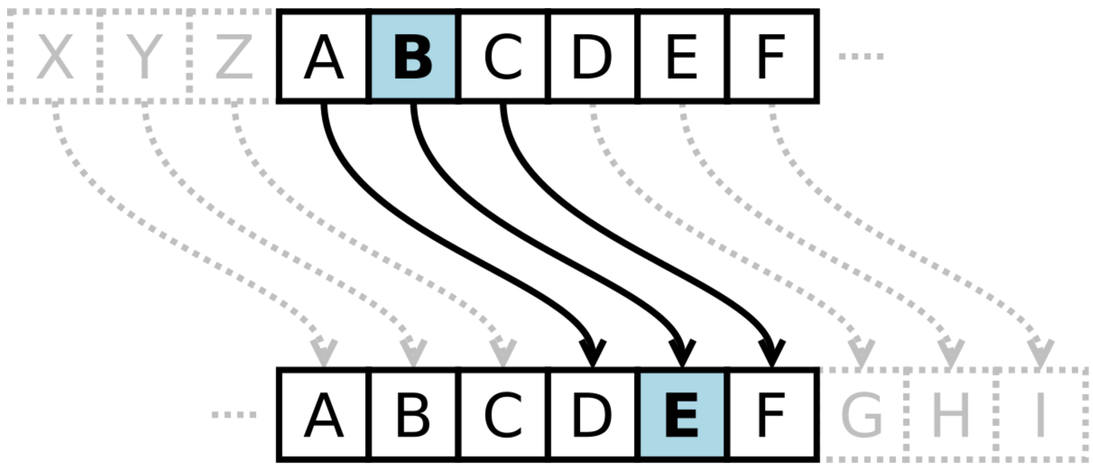
ACTIVITÉ 1 - CHIFFREMENT

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

Activité 1.1



Le 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 suivante :

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

On trouve alors *DEULFRW* : on dit que *DEULFRW* est le **chiffré** de César du message **clair** *ABRICOT* pour une **clé** valant 3.

Remarques :
Si l'addition donne un nombre plus grand que 26, on retourne alors au début de l'alphabet ainsi 27 donnera la lettre A et ainsi de suite.
La clé peut également être une lettre, dans ce cas là, la deuxième étape sera de trouver la position de la lettre avant d'additionner cette valeur.

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. *LKZK JK RG YIOKTIK* pour une clé valant *F*.
3. *ECGP* pour une petite clé.

Activité 1.2

Le chiffrement de Vigenère

Vigenère est un mathématicien français qui a détourné les codes de César pour chiffrer des messages en utilisant une technique similaire. Cependant, 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 de chaque lettre du mot *CLE* : $3 - 12 - 5$, et on regarde les 3 tables de décalage :

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. *QTBTW YMY HOA* pour une clé valant *NOISETTE*.
3. *FZIXSJQ GBZD HSFTJ* pour une clé valant *SUPER CLE*.

Activité 1.3

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

Le 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** ?