1. Le code de César

César, pour ses communications importantes à son armée, cryptait ses messages.

Figure 1 : Jules César

Le code de César est la méthode de cryptographie la plus ancienne communément admise par l'histoire. Il consiste en une substitution mono-alphabétique : chaque lettre est remplacée ("substitution") par une seule autre ("mono-alphabétique"), selon un certain décalage (appelé clé en cryptologie) dans l'alphabet.

1.1. Chiffrement

Ce que l'on appelle le chiffrement de César est un décalage des lettres.

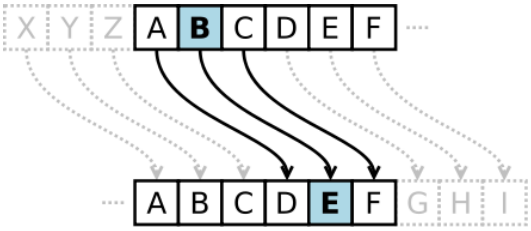

Figure 2 : méthode du chiffrement de César

Par exemple, pour chiffrer le mot NUMERIQUE avec un décalage de 3, le **N** devient **Q**, le **U** devient **X** pour ainsi obtenir le mot QXPHULTXH.

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
-> décalage = 3																										
CODE	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

Figure 3 : chiffrement par décalage de 3

1.2. Déchiffrement

Pour déchiffrer un code César, il suffit de décaler les lettres dans l'autre sens avec le même décalage qui a servi au chiffrement.

Par exemple, pour déchiffrer le mot LQIRUPDWLTXH avec un décalage de 3, le L devient I, le Q devient N pour ainsi former le mot INFORMATIQUE.

1.3. Sécurité du code

Niveau sécurité, le chiffre de César n'est pas fiable du tout, et ce pour deux raisons :

- Il n'existe que 26 façons différentes de crypter un message : puisqu'on ne dispose que de 26 lettres, il n'y a que 26 décalages possibles. Dès lors, des **attaques exhaustives** (attaque par **force brute** : tester tous les décalages un à un) ne demande que très peu de temps.

- Le chiffre de César est aussi très vulnérable à l'analyse des fréquences des lettres (par exemple, pour un texte écrit en français, il y a de fortes chances que la lettre qui apparaît le plus souvent corresponde à la lettre E).

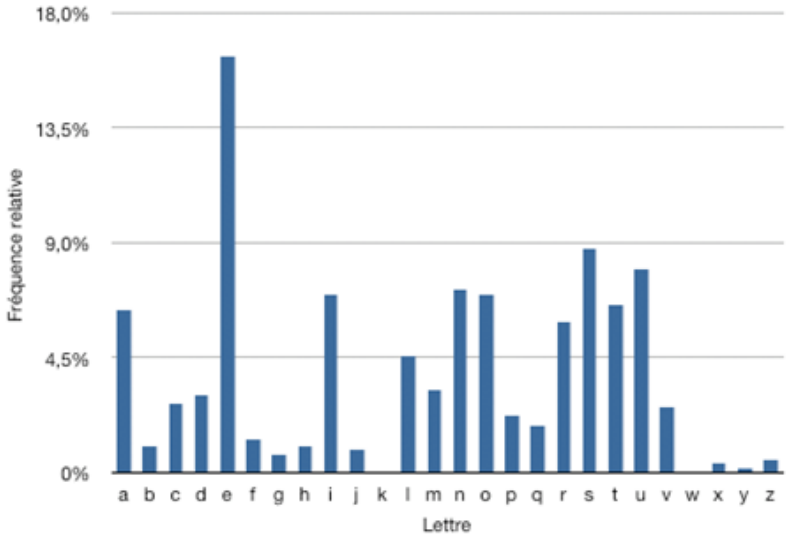

Fig 4 : fréquence d'apparition des lettres d'un texte français non chiffré

1.4. Exemples

✍ Chiffrer le mot **CESAR** avec un décalage (clé) de 3.

✍ Déchiffrer le code **MXOHV** qui utilise un décalage (clé) de 3.

✍ Chiffrer le mot **ROMAIN** avec un décalage (clé) de 10.

Alice a reçu le message « **RKXKTJKFBUAYKYZGJODNKAXKY** » de Bob. Elle sait que la clé est le chiffre 6.
✍ Aide Alice à déchiffrer le message de Bob.

Alice a envoyé le message suivant à Bob, mais il ne connaît pas la clé de chiffrement.
✍ Aide Bob à déchiffrer le message reçu : « **PIGSJJVIIWXHERWPIKEVEKI** » et retrouve la clé.

Bob a envoyé le message suivant à Alice, mais elle ne connaît pas la clé de chiffrement.
✍ Aide Alice à déchiffrer le message reçu : « **TIKTMMABLIVATMXWB** » et retrouve la clé.