CRYPYOGRAPHIE

Une permutation des lettres de l'alphabet permet de coder un texte :

- **On chiffre les lettres de l'alphabet : A ↦ 0, B ↦ 1, …….. , Z ↦ 25**
- On applique une "**fonction de codage**" **modulo 26**, de {0, 1, …, 25} sur lui-même, **bijective :** **X en clair ↦ Y codé**
- En appliquant une "**fonction de décodage**" **modulo 26**, de {0, 1, …, 25} sur lui-même, **bijective, on retrouve le message en clair : Y codé ↦ X en clair**

Méthode de César ou codage par translation

(feuille de calcul)

On choisit une lettre-clé chiffrée C

CODAGE

Une lettre étant chiffrée X en clair, il lui correspond la lettre chiffrée par Y tel que

$Y \equiv X + C$ modulo 26, $Y \in \{0, 1, 2, …., 25\}$.

DECODAGE (*lorsque la lettre clé est connue*)

$X \equiv Y - C$ modulo 26, $X \in \{0, 1, 2, …., 25\}$.

DECRYPTAGE (*lorsque la lettre clé est inconnue*)

On peut comparer la distribution des fréquences des lettres du message à la distribution « théorique » des fréquences des lettres d'un texte en clair.

Clé ≡ Chiffre le plus fréquent – 4 (mod 26)

(Cette analyse est suffisante lorsque le texte à décoder est assez long et sans particularité linguistique ou sans lettres ajoutées).

CODE DE VIGENERE OU CODAGE MULTI-ALPHABETIQUE

(feuille de calcul)

Comment rendre le travail de décryptage plus difficile ?

En utilisant plusieurs alphabets dans un même texte codé grâce à l'introduction d'**un mot-clé chiffré C_1 C_2 C_3 …, de longueur l.**

CODAGE

texte en clair: $X_1\ X_2\ X_3\ X_4\ X_5\ldots$
mot-clé $C_1\ C_2\ C_3\ C_1\ C_2\ldots..$
texte codé $Y_1\ Y_2\ Y_3\ Y_4\ Y_5\ldots$

pour tout i tel que $i \equiv r \pmod{l}$, $Y_i \equiv X_i + C_r \pmod{26}$

On code en utilisant l alphabets, l étant la longueur du mot-clé.

DECODAGE (lorsque le mot-clé est connu)

texte codé $Y_1\ Y_2\ Y_3\ Y_4\ Y_5\ldots$
texte en clair: $X_1\ X_2\ X_3\ X_4\ X_5\ldots$
mot-clé $C_1\ C_2\ C_3\ C_1\ C_2\ldots..$
texte en clair: $X_1\ X_2\ X_3\ X_4\ X_5\ldots$

pour tout i tel que $i \equiv r \pmod{l}$, $X_i \equiv Y_i - C_r \pmod{26}$

DECRYPTAGE

Dans ce système de codage, une même lettre peut-être codée de différentes façons, selon la lettre du mot - clé auquel elle est associée. La simple analyse des fréquences des lettres ne peut plus suffire.
Une suite de lettres répétée dans le texte en clair ne sera codée par la même suite de lettres dans le message codé que si la distance séparant ces deux suites est multiple de la longueur du mot- clé.
La longueur l du mot-clé est donc diviseur commun des distances séparant les différentes répétitions de séquences.

En regroupant les lettres de même rang modulo l, on retrouve des lettres codées par la même lettre du mot clé, donc issues du même alphabet. On pourra donc procéder par analyse des fréquences pour retrouver les lettres du mot clé.

CODAGE PAR UNE FONCTION AFFINE
f: X ↦ AX + B, A et B dans {0, 1, …., 25}, A ≠ 0.
(feuille de calcul)

CODAGE

lettre en clair: X
lettre codée: Y ≡ A.X + B modulo 26.

Pour A = 13 ou A pair , A et 26 non premiers entre eux ont un diviseur commun k tel que 2 ≤ k ≤ 13

$A = k \times A_1$ et $26 = k \times k'$, A_1 et k' entiers entre 2 et 13

$f(X + k') - f(X) = A \times k' = A_1 \times k \times k' = 26\ k'$

$f(X) - f(X + k') \equiv 0 \pmod{26}$

donc $\underline{f(X + k') \equiv f(X) \pmod{26}.}$

k' étant compris entre 2 et 13, les chiffres X + k' et X correspondent à deux lettres distinctes (car X + k' – X non ≡ 0 (mod 26)).
La relation **Y ≡ A.X + B (mod 26) leur associe le même chiffre modulo 26**.

Pour A = 13 ou A pair la relation de l'ensemble {0, 1, 2 … , 25} dans lui-même définie par X ↦ Y n'est pas injective donc elle n'est pas bijective et ne permet pas de coder.

Pour A impair, distinct de 13, **A est premier avec 26**.

f(X) – f(Y) ≡ A.(X–Y) modulo 26.

$\underline{f(X) - f(Y) \equiv 0 \pmod{26} \Leftrightarrow X - Y \text{ multiple de } 26.}$

Or X et Y sont compris entre 0 et 25 donc,
$f(X) - f(Y) \equiv 0 \pmod{26} \Leftrightarrow X - Y = 0 \Leftrightarrow X = Y$.
L'application X ↦ Y est une injection d'un ensemble fini dans lui-même. Elle est bijective.

Il y a donc **12×26 – 1 = 311 codages de ce type**.

DECODAGE

A et 26 sont premiers entre eux donc il existe deux entiers A' et tels que
A.A' + 26.v = 1 (théorème de Bachet-Bezout)

donc il existe A' tel que **A.A' ≡ 1 (mod 26)**.

Or par codage, Y ≡ A.X + B (mod 26) donc par compatibilité avec la multiplication,

A'.Y ≡ **A'.A**.X + A'.B (mod 26) ≡ X + A'.B (mod 26)

X ≡ A'Y – A'.B modulo 26
Le décodage procède encore par fonction affine.

EXEMPLE DE DECRYPTAGE

Codage mono-alphabétique donc analyse des fréquences

Chiffres les plus fréquents dans le message codé : **23 et 5**
Lettres les plus fréquentes de l'alphabet en clair: **e chiffrée 4 et a chiffrée 0**

23 ≡ 4A + B (mod 26)
5 ≡ 0A + B (mod 26)

Donc B ≡ 5 (mod 26) et 4A ≡ 23 – 5 (mod 26) (par compatibilité avec la soustraction) c'est-à-dire 4A ≡ 18 (mod 26)

Il existe un entier k tel que 4A = 18 + 26.k donc tel que 2A = 9 + k.13

2A ≡ 9 (mod 13) donc 14 A ≡ 63 (mod 13) (compatibilité avec la multiplication)

Or 14 ≡ 1 (mod 13) et 63 ≡ 11 (mod 13) donc A ≡ 11 (mod 13)

donc il existe p entier tel que A = 11 + 13p

Soit p pair, A ≡ 11 (mod 26) donc A est impair
Soit p impair, A ≡ 11 + 13 (mod 26) ≡ 24 (mod 26) donc A est pair

Or A nécessairement impair donc
A ≡ 11 (mod 26) et B ≡ 5 (mod 26)

Conclusion :
La fonction affine de CODAGE est donc :
X ↦ Y, Y ≡ 11.X + 5 (mod26), 0 ≤ Y ≤ 25

La fonction affine de DECODAGE est donc:

19×11 = 209 = 8× 26 + 1.
19×11 ≡ 1 (mod 26) donc A' ≡ 19 (mod 26)
Y ↦ X, X ≡ 19.X – 5×19 (mod26), 0 ≤ X ≤ 25

Exemples d’utilisation du tableur.

Avec le code de César, coder, décoder, observer les fréquences des lettres.

Avec le code de Vigenère, coder un même texte en utilisant des mots-clés de longueurs différentes et observer les éventuelles répétitions.

Avec la fonction affine, dans une feuille automatisée, calculer les restes modulo 26 de AX + B, pour différentes valeurs de A et b et pour X de 0 à 25 et constater que A doit être impair et différent de 13.
Pour retrouver la fonction de décodage, calculer le reste modulo 26 de A.N pour N entier de 0 à 26 et retrouver A’ tel que $A.A' \equiv 1$ modulo 26