

Fonction de chiffrement : Le Chiffre Roulant

Noam Zeitoun

Soit $P = (P_1, P_2)$ un couple de lettres à chiffrer avec $P_i \in \{A, B, \dots, Z\}$ pour $i \in N$. Soit α la position dans l'alphabet de la lettre A, c'est-à-dire $\alpha = 1$, et soit $\cdot \bmod$ l'opérateur modulo.

Le chiffrement se fait en deux étapes :

On calcule les positions dans l'alphabet des lettres de P :

$$p_1 = P_1 - \alpha + 1$$

$$p_2 = P_2 - \alpha + 1$$

On calcule la position dans l'alphabet de la lettre chiffrée C en effectuant une somme modulo 26 :

$$c = (p_1 + p_2) \bmod 26$$

La lettre chiffrée C est la lettre située à la position c de l'alphabet :

$$C = (c - 1 + \alpha)$$

En résumé, la formule de chiffrement pour un couple de lettres P est :

$$E(P) = (P_1 - \alpha + 1 + P_2 - \alpha + 1) \bmod 26 + \alpha$$

Soit:

$$E(P) = ((P_1 - \alpha + P_2 - \alpha + 2) \bmod 26) + \alpha$$

Ensuite, on utilise la table de correspondance suivante pour convertir chaque chiffre en une lettre :

A_1	B_2	C_3	D_4	E_5
F_6	G_7	H_8	I_9	J_{10}
K_{11}	L_{12}	M_{13}	N_{14}	O_{15}
P_{16}	Q_{17}	R_{18}	S_{19}	T_{20}
U_{21}	V_{22}	W_{23}	X_{24}	Y_{25}
Z_{26}				

Pour obtenir la lettre 'A', il suffit de prendre la paire 'AZ' qui ferait :

$$(1 + 26) \mod 26 = 1$$

Prenons l'exemple de la plaque d'immatriculation 'AB 123 CD'. Nous allons utiliser le Chiffre Roulant pour chiffrer les paires de lettres dans la plaque.

Pour la paire de lettres 'AB', nous avons :

$$P_1 = 1, P_2 = 2, \alpha = 1$$

$$E_{AB} = ((P_1 - \alpha + P_2 - \alpha + 2) \mod 26) + \alpha$$

$$E_{AB} = 3$$

Pour la paire de lettres 'CD', nous avons :

$$P_1 = 3, P_2 = 4, \alpha = 1$$

$$E_{CD} = ((P_1 - \alpha + P_2 - \alpha + 2) \mod 26) + \alpha$$

$$E_{CD} = 7$$

Finalement, nous convertissons chaque chiffre en une lettre en utilisant la table de correspondance fournie :

3 correspond à la lettre 'C'

7 correspond à la lettre 'G'

Ainsi, la plaque d'immatriculation 'AB 123 CD' est chiffrée en 'CG'.