Réponses TP chiffrement 1 – les principes

Exo. 1 : Le carré de Polybe

GAGNE

POLYBE

Exo. 2 : Code César

MJQQT BTWQI

Exo. 3 : Casser le code César par analyse fréquentielle

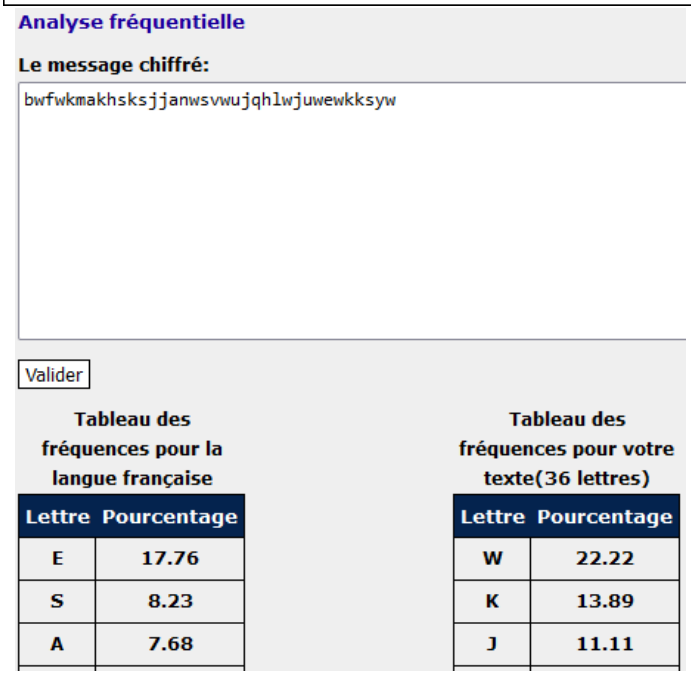
clé : 5

LE E EST TRES FREQUENT

Exo. 4 sur PC : Déchiffrer le code César avec un outil

Clé : 6 - LAVIE ESTBE LLE

Exo. 5 sur PC : Casser un code César par analyse fréquentielle



Résultat :

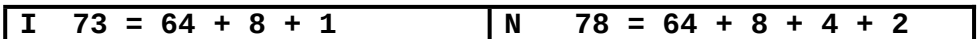
jenesuispasarriveadecryptercemessage

Exo. 6 : Chiffrement avec OU Exclusif

Explication : cet exercice montre de manière très simplifiée la façon dont on chiffre des données avec un algorithme comme AES. Les bits du message clair sont permutés, en quelque sorte « mélangés ». Puis un XOR est effectué avec la clé (en fait une partie de la clé). Ces opérations (qui forment « un tour ») sont répétées de nombreuses fois. Le message chiffré n'a plus rien à voir avec le message original.
Ces opérations sont réversibles et on peut déchiffrer le message si on connaît la clé.

Travail à faire :

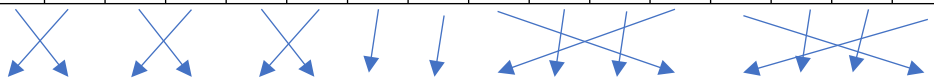
texte clair



texte clair binaire

0	1	0	0	1	0	0	1	0	1	0	0	1	1	1	0

Effectuer des permutations



données mélangées

1	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1

XOR avec la clé

clé

0	1	0	1	0	1	1	0	0	1	0	1	0	1	1	0

texte chiffré

1	1	0	1	0	0	1	1	0	0	0	1	0	0	0	1

Déchiffrement

XOR avec la clé

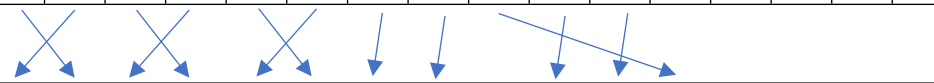
clé

0	1	0	1	0	1	1	0	0	1	0	1	0	1	1	0

données mélangées

1	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1

Faire permutations inverses



texte clair binaire

0	1	0	0	1	0	0	1	0	1	0	0	1	1	1	0

texte clair