

Sécurité informatique

Série 2 : Initiation à la cryptographie (César / Transposition)

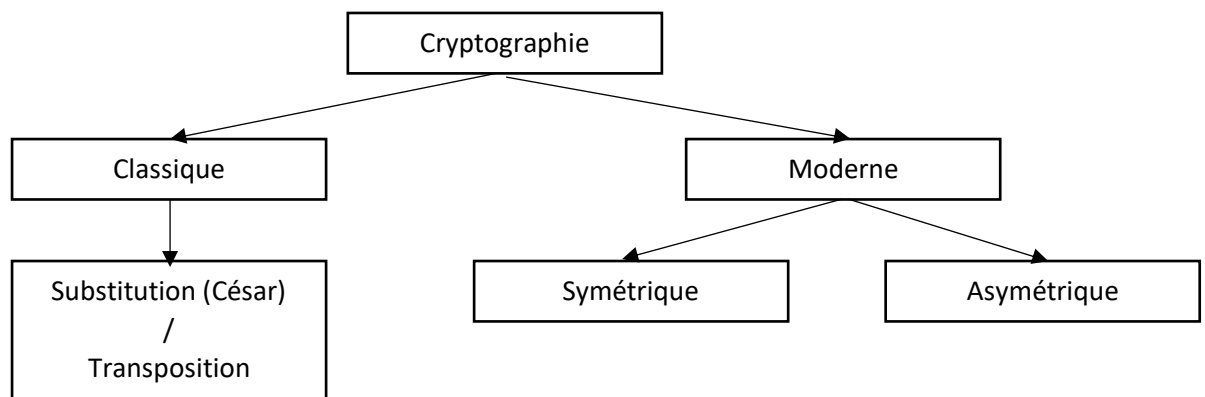
« La cryptographie est l'art et la science de sécuriser les communications en transformant des informations en un format illisible pour toute personne non autorisée, puis en les rendant lisibles uniquement pour ceux qui possèdent la clé de déchiffrement appropriée. »

1. Objectifs de la Cryptographie ?

2. Principaux Concepts :

- ❖ Chiffrement
- ❖ Déchiffrement
- ❖ Clé
- ❖ Algorithme
- ❖ Cryptanalyse

3. Types de Cryptographie :



Exercice 1 : (Algorithme de César)

1.1. Chiffrement avec l'algorithme de César

Chiffrez le message suivant en utilisant l'algorithme de César avec un décalage de 3 lettres :
Message clair : "BONJOUR"

1.2. Déchiffrement avec l'algorithme de César

Déchiffrez le message suivant qui a été chiffré avec l'algorithme de César avec un décalage de 5 lettres :
Message chiffré : "GFION RTPMYFW"

1.3. Déchiffrement sans clé avec l'algorithme de César

Déchiffrez le message suivant qui a été chiffré avec l'algorithme de César sans connaître le décalage :
Message chiffré : "HUUHIH"

Exercice 2 : (Algorithme de chiffrement par transposition)

Par exemple, en utilisant la clé $k = 164325$

Le message clair $M = \text{« MESSAGE SECRET A CHIFFRER PAR TRANSPOSITION »}$,

Nous obtenant le cryptogramme $C = \text{« METFRPO ARIPNT SCHRAI SECERS GEFASI ESARTON »}$

Chiffrement	Déchiffrement
1. Calculer le nombre de caractères du message clair M.	1. Calculer le nombre de caractères du message Chiffré C.
2. Préparation de la matrice :	2. Préparation de la matrice :
a. Colonnes (selon la clé)	a. Colonnes (selon la clé) -6-
b. Lignes (Nb.M / Nb.Cle)	b. Lignes (Nb.M / Nb.Cle) 6+6+ ... + 2
3. Remplissage par Lignes	3. Remplir le message C par Colonnes selon la clé
4. Écrire le message par Colonnes selon la clé	4. Écrire le message M Par lignes

2.1. Quel est le cryptogramme C correspondant au texte clair $M = \text{« MATHEMATIQUES ET INFORMATIQUE »}$ et la clé $k = \text{« 356124 »}$?

2.2. Quel est le texte clair M correspondant au cryptogramme C $\text{« USCCLSETFEIESTCSEAD EXCENA »}$ et la clé $k = \text{« 356124 »}$?