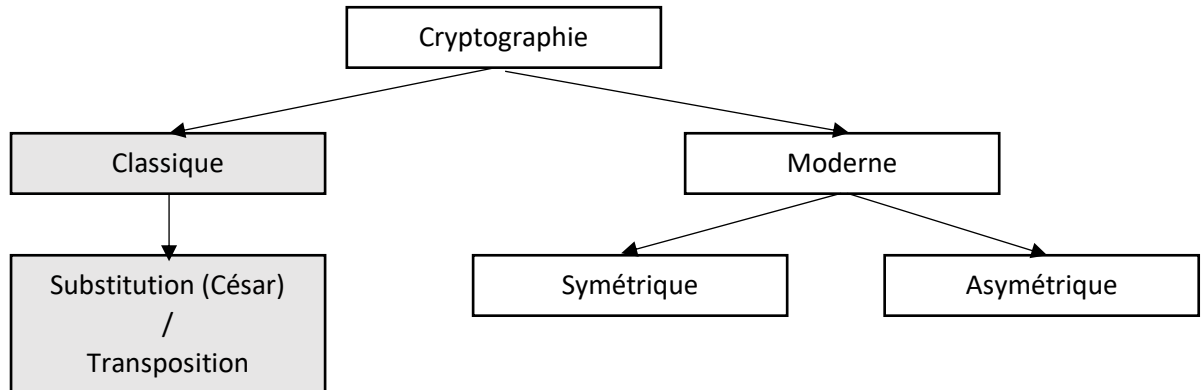


TD Sécurité Informatique

Série TD 3.1 : Cryptographie Symétrique (S-DES)

Rappel :

- ❖ Série 1 : Service, Menaces, Mécanismes, ISO 27002
- ❖ Série 2 : Cryptographie classique (César, Transposition)



Cryptographie Symétrique (S-DES) :

1. Quelle est la différence entre la cryptographie symétrique et asymétrique ?
2. Comment les deux parties communicantes s'échangent-elles la clé secrète dans le contexte de la cryptographie symétrique afin de garantir la confidentialité des données échangées ?
3. Liste des algorithmes de chiffrement symétrique les plus connus :
 - ❖ AES (Advanced Encryption Standard)
 - ❖ ~~DES (Data Encryption Standard)~~
 - ❖ 3DES (Triple Data Encryption Standard)
4. Quelle est la différence fondamentale entre l'algorithme **S-DES** (Simplified Data Encryption Standard) et le **DES** (Data Encryption Standard) complet ?

S-DES or Simplified Data Encryption Standard

1. S-DES chiffre des blocs de **8 bits**.
2. La **clé** de chiffrement est de **10 bits**.
3. Deux tours de chiffrement.

Exemple :

Trouvez les valeurs de K1, K2, et le texte chiffré en utilisant l'algorithme S-DES avec les paramètres suivants :

- ❖ Clé: 10111 00111 -> K1: 1011 1110 / K2: 1101 1011
- ❖ Plain text: 0110 1100

Exercise 01:

Trouvez les valeurs de K1, K2, et le texte chiffré en utilisant l'algorithme S-DES avec les paramètres suivants :

- ❖ Clé : 10100 00010
- ❖ Texte Clair (r): 0111 0010

Indiquez clairement vos calculs pour chaque étape.

