

Cryptographie

Chiffrement symétrique

- La cryptographie se base sur des opérations mathématiques généralement (algorithmes)
- Objectif : transmettre de manière sécurisée des messages

Cryptographie

Chiffrement symétrique

- Principe du chiffrement :
 - appliquer un algorithme sur le message en clair
 - qui utilise comme paramètre d'entrée une clé de chiffrement.
- Principe du déchiffrement :
 - appliquer un algorithme sur le message chiffré
 - qui utilise comme paramètre d'entrée une clé de déchiffrement.

- Cryptographie symétrique :



Avantage :

Rapidité des opérations de chiffrement et déchiffrement

Inconvénient :

Transmission de la clé secrète de chiffrement (la procédure doit être sécurisée)

Algorithmes de chiffrement symétrique : AES, DES, Blowfish

Cryptographie

Chiffrement symétrique

- Chiffrement symétrique (à clé secrète)
 - Algorithmes de chiffrement avec opérations mathématiques simples
 - Connaître clé de chiffrement + algorithme de chiffrement utilisé permet de calculer la clé de déchiffrement -> inconvénient majeur
 - clé secrète assimilée à une clé identique pour chiffrer et déchiffrer -> **la clé doit rester secrète**
 - **Procédure sécurisées pour transmettre la clé**

Cryptographie

Chiffrement symétrique

- Chiffrement symétrique (à clé secrète)
 - Avantage : rapidité des opérations cryptographiques rapidement.
 - Algorithme AES, DES / triple DES, Blowfish
 - AES est l'un des plus sûr
 - Robustesse du procédé :
 - Les algorithmes symétriques sont connus
 - Tentative de déchiffrement = découvrir la clé
 - -> importance du choix de la **longueur de la clé**