Cryptographie Symétrique

Introduction à la Cryptographie Symétrique

La cryptographie symétrique utilise la même clé pour chiffrer et déchiffrer les données.
Elle est rapide et efficace pour le chiffrement de grandes quantités de données.

AVANTAGES:

Rapidité d'exécution

Simplicité d'implémentation

Efficace pour le chiffrement en masse

INCONVÉNIENTS:

Problème de distribution sécurisée des clés

Gestion difficile des clés dans un environnement multi-utilisateurs

Algorithmes Symétriques Courants

1. AES (Advanced Encryption Standard) - Le plus utilisé aujourd'hui
2. DES (Data Encryption Standard) - Obsolète, remplacé par AES
3. 3DES (Triple DES) - Version plus sécurisée de DES
4. Blowfish - Alternative à DES
5. RC4 - Algorithm de flux (désormais considéré comme non sécurisé)

Chiffrement/Déchiffrement avec AES-256-CBC

Chiffrement d'un fichier:

openssl enc -aes-256-cbc -salt -in fichier_original.txt -out fichier_chiffre.enc -k "maCleSecrete"

- enc : commande de chiffrement

-aes-256-cbc : algorithme utilisé

-salt : ajoute un sel pour renforcer la sécurité

-in : fichier d'entrée

-out : fichier de sortie chiffré

-k : mot de passe/clé

Génération d'une clé de 32 octets (256 bits) pour AES-256

openssl rand -hex 32 > cle_aes.key

Puis l'utiliser pour chiffrer:

openssl enc -aes-256-cbc -salt -in fichier_original.txt -out fichier_chiffre.enc -pass file:cle_aes.key

Domaines d'Utilisation des Clés Symétriques & Algorithmes Courants

1. Contexte d'Utilisation des Clés Symétriques

La cryptographie symétrique est largement utilisée dans les domaines où la vitesse et l'efficacité sont cruciales. Voici les principaux contextes :

1.1 Chiffrement des Données en Transit

- SSL/TLS (pour les sessions sécurisées après l'échange de clés asymétriques)
- VPN (IPSec, OpenVPN)
- Wi-Fi (WPA2/WPA3 utilise AES-CCMP)

.2 Chiffrement des Données au Repos

- Disques chiffrés** (BitLocker, VeraCrypt)
- Bases de données (chiffrement transparent TDE)
- Fichiers & Archives (ZIP, 7z avec chiffrement)

1.3 Communications Sécurisées

- Messagerie instantanée (Signal, WhatsApp utilisent AES pour le chiffrement de bout en bout)
- VoIP sécurisé (ZRTP avec AES)

1.4 Applications Embarquées

- Cartes à puce (banque, SIM)
- IoT (protocoles légers comme ChaCha20)

2. Algorithmes Symétriques les Plus Utilisés

2.1 AES (Advanced Encryption Standard)

- Standard depuis 2001 (remplace DES)
- Taille de clé : 128, 192 ou 256 bits
- Bloc de 128 bits
- Modes d'opération courants :
  - CBC (Cipher Block Chaining) – nécessite un IV
  - GCM (Galois/Counter Mode) – avec authentification
  - CTR (Counter Mode) – évite le padding