
📘 Cours : Chiffrement Symétrique (AES, DES)

🔐 1. Définition du chiffrement symétrique

Le **chiffrement symétrique** est un type de cryptographie où **la même clé** est utilisée à la fois pour **chiffrer** et **déchiffrer** les données.

🔁 Exemple simple :

- Clé : `1234`
- Message : `Bonjour`
- Message chiffré → (illisible sans la clé)
- Même clé utilisée pour retrouver `Bonjour`

🎯 2. Avantages et limites

Avantages	Inconvénients
Rapide et efficace	Partage sécurisé de la clé nécessaire
Peu gourmand en ressources	Non adapté à l'échange public sans canal sécurisé
Très utilisé pour le chiffrement de données locales	Clé unique = point de faiblesse

---

🔐 3. Algorithme DES (Data Encryption Standard)

a. Historique

- Créé par IBM dans les années 1970, adopté comme standard en 1977.
- Clé de **56 bits**, bloc de données de **64 bits**.
- Jugé **obsolète aujourd'hui** à cause de sa faible longueur de clé.

b. Fonctionnement

- Basé sur 16 **rounds** (étapes de transformation).
- Utilise la **substitution et permutation** pour brouiller les données.

- Forme de **chiffrement par blocs**.

c. Vulnérabilités

- Sensible au **brute-force**.
- Aujourd'hui remplacé par **3DES** (Triple DES) puis par **AES**.

🛡 4. Algorithme AES (Advanced Encryption Standard)

a. Historique

- Sélectionné par le NIST en 2001.
- Remplace DES.
- Utilisé dans la plupart des systèmes modernes (VPN, HTTPS, Wi-Fi...).

b. Caractéristiques

- Taille de clé : **128, 192 ou 256 bits**.
- Taille de bloc : **128 bits**.
- Nombre de **rounds** :
  - 10 (AES-128)
  - 12 (AES-192)
  - 14 (AES-256)

c. Fonctionnement

AES utilise une série d'opérations sur une **matrice 4x4** de bits :

1. **SubBytes** : Substitution non linéaire de chaque octet.
2. **ShiftRows** : Décalage des lignes.
3. **MixColumns** : Mélange des colonnes.
4. **AddRoundKey** : Ajout de la clé de round via un XOR.

d. Points forts

- Très **rapide** et **sûr**.
- Résiste aux attaques connues.
- Largement implémenté dans les logiciels et matériels.

🔄 5. Comparaison : AES vs DES

Critère	DES	AES
Taille de clé	56 bits	128/192/256 bits
Taille de bloc	64 bits	128 bits
Sécurité	Faible aujourd'hui	Très élevée
Vitesse	Moyenne	Élevée
Standard actuel	Non	Oui

⚙ 6. Exemple de chiffrement AES (simplifié)

- Message : `HELLO12345678AB`
- Clé AES-128 : `1234567890ABCDEF1234567890ABCDEF`
- Sortie (hex) : `A1 B2 C3 D4 E5 F6 ...`
  → Le message devient un **bloc chiffré illisible** sans la clé.

📌 7. Cas d’usage

- Chiffrement de fichiers (ZIP, PDF, disques durs)
- Communication sécurisée (HTTPS, VPN, SSL/TLS)
- Messagerie chiffrée (Signal, WhatsApp)
- Stockage chiffré (bases de données, clouds)

---

8. Conclusion

Le **chiffrement symétrique** reste incontournable pour la sécurité informatique, notamment grâce à **AES**, aujourd’hui **le standard mondial**. Bien que **DES ait marqué l’histoire**, il est désormais obsolète face aux puissances de calcul actuelles.
