📚 Cours : Introduction à la Cryptographie

🔐 1. Définition de la Cryptographie

La cryptographie est la **science du secret**. Elle permet de **protéger l'information** contre l'accès non autorisé en la **transformant** de manière à ce qu'elle soit **illisible** sans autorisation.
Elle est utilisée pour assurer la **confidentialité**, l'**intégrité**, l'**authenticité** et la **non-répudiation** des données.

🎯 2. Objectifs de la Cryptographie

1. **Confidentialité** : empêcher toute personne non autorisée de lire les données.
2. **Intégrité** : garantir que les données n'ont pas été modifiées.
3. **Authenticité** : assurer que le message provient de la bonne source.
4. **Non-répudiation** : empêcher l'émetteur de nier avoir envoyé le message.

🔑 3. Types de Cryptographie

a. Cryptographie symétrique

- Même clé pour le chiffrement et le déchiffrement.
- Rapide, mais nécessite un **partage sécurisé** de la clé.
- Exemples : **AES, DES, RC4**

b. Cryptographie asymétrique

- Clé publique pour chiffrer, clé privée pour déchiffrer.
- Plus lente, mais idéale pour l'échange sécurisé.
- Exemples : **RSA, ECC, ElGamal**

c. Fonctions de hachage

- Prise d'un message et retour d'un résumé (empreinte) fixe.
- Impossible de revenir en arrière.
- Utilisé pour l'intégrité et les mots de passe.
- Exemples : **SHA-256, MD5, SHA-1**

🔐 4. Chiffrement et Déchiffrement

Exemple symétrique (AES) :

- Message : `HELLO`
- Clé : `XYZ123`
- Message chiffré : `8F 7D 1B ...`
- Le même algorithme + la même clé permettent de retrouver le message original.

Exemple asymétrique (RSA) :

- Alice utilise la **clé publique de Bob** pour chiffrer un message.
- Seule la **clé privée de Bob** peut le déchiffrer.

📎 5. Signatures numériques

- L'émetteur signe un message avec sa **clé privée**.
- Le destinataire vérifie l'authenticité avec la **clé publique** de l'émetteur.
- Garantit l'**authenticité** et la **non-répudiation**.

🏛 6. Certificats numériques et PKI

- Les certificats X.509 lient une **identité** à une **clé publique**.
- La **PKI** (Infrastructure à Clé Publique) gère les certificats, leur délivrance, et leur révocation.

⚠ 7. Attaques courantes en cryptographie

- **Brute-force** : tester toutes les clés possibles.
- **Cryptoanalyse** : exploiter des faiblesses dans l'algorithme.
- **Attaque par dictionnaire** : pour casser des mots de passe hachés.
- **Man-in-the-middle** : intercepter une communication chiffrée.

🌐 8. Applications réelles

- Sécurisation des sites web (**HTTPS**)
- Chiffrement des emails (**PGP, S/MIME**)
- Signature de documents numériques
- Stockage sécurisé (disques chiffrés, bases de données)

📌 9. Résumé

Concept	Description
Chiffrement	Transformer un message en données illisibles
Clé	Information utilisée pour chiffrer/déchiffrer
Symétrique	Même clé pour chiffrer et déchiffrer
Asymétrique	Deux clés différentes (publique/privée)
Hachage	Résumé unique d’un message
Signature numérique	Preuve d’authenticité et d’intégrité