

CM2 - Cryptographie : Des Chiffres à la Sécurité Computationnelle

Introduction à la sécurité informatique

Mohamed Said M'Bareck

SUPNUM

`ms.mbareck@supnum.mr`

2025-2026

1 Fondements du Secret

- Introduction à la Cryptographie
- Cryptographie Classique et Théorique
- Outils Mathématiques pour la Crypto Moderne
- Sécurité Computationnelle

2 La Révolution de la Clé Publique et Application

- Principes de la Clé Publique (PKC)
- Protocoles Asymétriques
- Implémentations et Pièges Pratiques

3 Conclusion

- **Définition** : La cryptographie étudie les **techniques mathématiques** pour sécuriser l'information numérique contre les adversaires.
- **Objectifs Principaux** :
 - ① **Confidentialité (Chiffrement)** : Protéger les données du regard non autorisé.
 - ② **Signatures Numériques** : Assurer l'intégrité et l'authenticité des données.
- **Principes Modernes** : Passage d'approches *ad hoc* à des systèmes basés sur des définitions formelles et des preuves de sécurité.

Le Processus de Chiffrement de Base

$$E_K(P) = C \text{ et } D_K(C) = P.$$

- **Chiffrement Symétrique (Clé Secrète) :**

- Utilise la **même clé** (K) pour chiffrer et déchiffrer.
- **Avantage** : Rapide.
- **Exemple** : AES.

- **Chiffrement Asymétrique (Clé Publique) :**

- Utilise une **paire de clés** : publique (K_{pub}) pour chiffrer, privée (K_{priv}) pour déchiffrer.
- **Avantage** : Pas besoin d'échange de clé secret préalable.
- **Exemples** : RSA, Diffie-Hellman.

- **Chiffres Classiques :**

- **Chiffre de César :** Substitution simple avec décalage fixe. Facile à casser avec l'analyse de fréquence.
- **Chiffre de Vigenère :** Substitution polyalphabétique utilisant une clé. Résiste à l'analyse de fréquence simple, mais reste vulnérable aux analyses statistiques plus avancées.

- **Secret Parfait : Le One-Time Pad (OTP)**

- **Opération :** $C = M \oplus K$ (XOR).
- **Conditions (strictes) :** La clé K doit être parfaitement aléatoire, aussi longue que le message et **utilisée une seule fois**.
- **Danger de la réutilisation de clé :** Si K est réutilisée ($K_1 = K_2 = K$), un attaquant obtient $C_1 \oplus C_2 = M_1 \oplus M_2$, ce qui compromet la confidentialité.

La cryptographie moderne repose sur des problèmes mathématiques difficiles à résoudre.

- **Arithmétique Modulaire** : Calculs sur des nombres qui "s'enroulent" après avoir atteint une certaine valeur (le modulo). Ex : $15 \equiv 3 \pmod{12}$. C'est le fondement de la PKC.
- **Algorithme d'Euclide** : Méthode efficace pour trouver le Plus Grand Commun Diviseur (PGCD) de deux nombres. Essentiel pour les opérations en arithmétique modulaire, comme le calcul des clés RSA.
- **Exponentiation Rapide (Square-and-Multiply)** :
 - Permet de calculer très rapidement $x^e \pmod{n}$ même avec des exposants e très grands.
 - Sans cet algorithme, la plupart des cryptosystèmes à clé publique seraient trop lents pour être utilisables.

- **Le Changement de Paradigme** : La sécurité n'est pas absolue (parfaite), mais repose sur l'idée que casser le système est **computationnellement infaisable** pour un attaquant avec des ressources limitées.
- **Adversaires PPT** : Les attaquants sont modélisés comme ayant un temps de calcul **polynomial probabiliste** (PPT). Ils ne peuvent pas essayer toutes les clés.
- **Modèles d'Attaque (Niveaux de puissance de l'attaquant)** :
 - **Attaque à Texte Clair Choisi (CPA)** : L'attaquant peut obtenir le chiffré de n'importe quel message de son choix. C'est le standard de sécurité minimum pour les chiffrements modernes.
 - **Attaque à Texte Chiffré Choisi (CCA)** : L'attaquant a en plus accès à un "oracle de déchiffrement" pour des messages (sauf celui qu'il cherche à casser). C'est un modèle plus fort et plus réaliste.

La Révolution de la Clé Publique et Application

Principes de la Clé Publique (PKC)

- **Le Concept** : Permet une communication sécurisée sans échange préalable de clé secrète.
- **Mécanisme Fondamental** : Utilise des **Fonctions à Sens Unique à Trappe**.
 - **Sens unique** : Facile à calculer dans un sens (ex : multiplier deux grands nombres premiers).
 - **Difficile à inverser** : (ex : factoriser le résultat) ...
 - **... Sauf avec la trappe** : Une information secrète (la clé privée) qui rend l'inversion facile.
- **Chiffrement Hybride** : En pratique, les PKC sont lents. On combine les deux mondes :
 - ① On utilise un PKC (ex : RSA) pour échanger de manière sécurisée une petite clé symétrique.
 - ② On utilise cette clé symétrique avec un algorithme rapide (ex : AES) pour chiffrer le reste des données.

La sécurité des PKC repose sur la difficulté supposée de ces problèmes :

- **Problème de Factorisation Entière (IFP - Integer Factorization Problem) :**
 - Étant donné un grand nombre N , trouver ses facteurs premiers p et q .
 - C'est le problème sur lequel repose la sécurité de **RSA**.
- **Problème du Logarithme Discret (DLP - Discrete Logarithm Problem) :**
 - Étant donné g , p , et $h = g^x \pmod{p}$, trouver x .
 - C'est le problème sur lequel repose la sécurité de **Diffie-Hellman**.

La Révolution de la Clé Publique et Application

Échange de clés Diffie-Hellman (DH)

But : Établir une clé secrète partagée (K) sur un canal public non sécurisé.

Alice (Privé : a)

- 1 Calcule $A \equiv g^a \pmod{p}$
- 2 Envoie A à Bob.
- 3 Reçoit B . Calcule $K \equiv B^a \equiv (g^b)^a \pmod{p}$.

Bob (Privé : b)

- 1 Calcule $B \equiv g^b \pmod{p}$
- 2 Envoie B à Alice.
- 3 Reçoit A . Calcule $K \equiv A^b \equiv (g^a)^b \pmod{p}$.

Vulnérabilité

Le protocole DH standard est vulnérable aux **attaques de l'homme du milieu (Man-in-the-Middle)** car il n'y a pas d'authentification des participants.

- **Chiffres par Blocs (Block Ciphers) :**

- Ex : **AES**. Traite les données par blocs de taille fixe (128 bits).
- **Mode d'Opération ECB (Electronic Code Book) :** Le mode le plus simple, mais **totalemtent insécurisé** car des blocs de texte clair identiques donnent des blocs chiffrés identiques. **À ne jamais utiliser.**
- **Modes sécurisés (CTR, GCM) :** Utilisent un mécanisme (compteur, nonce) pour s'assurer que des blocs de texte clair identiques produisent des blocs chiffrés différents. Ils offrent une sécurité CPA.

- **Fonctions de Hachage (Hash Functions) :**

- Ex : **SHA-256**. Produisent une empreinte (digest) de taille fixe.
- Propriétés : résistance à la préimage, à la seconde préimage et aux collisions.
- **Attaque par extension de longueur :** Une faiblesse de l'ancienne construction Merkle–Damgård (MD5, SHA-1) qui peut être problématique dans certains cas d'usage (ex : MACs).

La Révolution de la Clé Publique et Application

Pièges d'Implémentation Courants

La théorie ne suffit pas

Des algorithmes solides peuvent être cassés par des erreurs d'implémentation.

- **Génération de nombres aléatoires faible** : Si les clés ou les nonces ne sont pas vraiment aléatoires, le système peut être prédictible.
- **Réutilisation de Keystream/Nonce** : Pour les modes de chiffrement de flux (comme CTR), réutiliser une paire (Clé, Nonce) est catastrophique et casse la confidentialité.
- **Attaques par canal auxiliaire (Side-channel)** : L'attaquant exploite des fuites d'information non intentionnelles comme le temps de calcul, la consommation électrique ou les messages d'erreur (ex : Oracle de Padding) pour deviner des secrets.

- **Synthèse** : La sécurité moderne repose sur des chiffrements rapides (AES) pour les données, et des chiffrements lents (RSA) pour l'échange de clés, le tout basé sur des problèmes mathématiques difficiles.
- **Randomisation** : La qualité des nombres aléatoires est un pilier fondamental de toute la cryptographie. Un mauvais générateur de nombres aléatoires (PRNG) peut tout compromettre.
- **Le Défi Quantique** : Les futurs ordinateurs quantiques, avec l'algorithme de Shor, pourront résoudre les problèmes IFP et DLP, brisant ainsi RSA et DH.
- **Cryptographie Post-Quantique (PQC)** : La communauté de recherche développe activement de nouveaux algorithmes (basés sur les réseaux, les codes, etc.) qui résisteraient aux attaques quantiques.
- **Leçon Finale** : Une sécurité fiable nécessite des algorithmes solides ET une implémentation sans faille.