CRYPTO

Chiffrements symétriques & PRNGs

Loïc Rouquette

2025-02-16

Rappels du Dernier Cours

Les 5 propriétés de la sécurité

- Disponibilité
- Authentification
- Intégrité
- Non-Répudiation
- Confidentialité

Les fonctions de hashage

Définition

$$H : \{0,1\}^* \rightarrow \{0,1\}^n, H(m) = h$$

Pourquoi faire ?

- Assurer l'intégrité des données ;
- Stocker les mots de passes sans les faire apparaître en clair dans une base de donnée.

Le standard

- SHA-3 (Keccak), standardisé par le NIST en 2015

Les fonctions de hashage(ii)

Les propriétés des fonctions de hashage cryptographique

- Résistance à la **pré-image**
- Résistance à la **seconde pré-image**
- Résistance aux **collisions**

Ce qu'il reste à voir !

- Disponibilité
- Authentification
- ~~Intégrité~~
- Non-Répudiation
- Confidentialité

Ce qu'il reste à voir !(ii)

- Disponibilité
- Authentification
- ~~Intégrité~~
- Non-Répudiation
- **Confidentialité**

Les chiffrements symétriques et les PRNGs

Pourquoi les PRNGs et les chiffrements symétriques ensemble ??

Pas si différent que ça en pratique !

Retour à la case départ

Le chiffrement de César (1er siècle av. J.C.)

$$\mathtt{A} \longrightarrow \mathtt{D}$$

Si on considère une lettre comme un nombre, on peut traduire le chiffrement par :

$$E(lettre) = (lettre + 3)[26]$$

Cryptanalyse par l'analyse fréquentielle.

Retour à la case départ(ii)

Chiffre de Vigenère (1553)

```
def enc_vigenere(K: str, M: str) -> str:
    C = ""
    i = 0
    for letter in M:
        offset = get_key_offset(K[i % len(K)], letter)
        if offset is not None:
            C += enc_letter_caesar(offset, letter)
            i += 1
        else:
            C += letter
    return C
```

Cryptanalyse par le test de Kasiski.

Retour à la case départ(iii)

L'opération effectuée entre le texte clair et le texte chiffré est une **addition modulo** également appelée **congruence**.

Retour à la case départ(iv)

Existe-t-il une opération binaire qui fait la même chose ?

Masque Jetable ou Chiffrement de Vernam (1917)

Il existe un chiffrement prouvé **parfait** : il s'agit du chiffrement de Vernam.

Fonctionnement

Comme Vigenère mais avec un **XOR**.

$$E_K(m) = m \oplus K$$

Masque Jetable ou Chiffrement de Vernam (1917)(ii)

Mais ça fonctionne à quelles conditions ??

Masque Jetable ou Chiffrement de Vernam (1917)(iii)

La clé doit être :

- purement aléatoire ;
- de la taille du texte ;
- utilisée une seule fois.

Masque Jetable ou Chiffrement de Vernam (1917)[iv]

Non réaliste en pratique !

Comment fait-on en pratique !?

On essaie de faire semblant d'avoir une clé aléatoire.

À l'aide de **CSPRNG** ou de **chiffrements symétriques**.

Les générateurs de nombres (pseudo-)aléatoires

Les TRNG (True Random Number Generator)

Figure 1. – Mur de lampes à lave de CloudFlare

Les TRNG (True Random Number Generator)(ii)

Objectif

Obtenir de l'entropie : une source d'aléa complet.

Difficultés

- Très lent (comparé aux autres méthodes) ;
- Non reproductible.

Les PRNG (Psuedorandom Number Generator)

Objectif

Générerer une séquence de nombre qui « semble » aléatoire.

Fonctionnement

- Algorithme prédéfini qui va générer des séquences différentes en fonction de la valeur initiale appelée *seed* ;
- Sortie reproductible (même *seed* = même séquence) ;
- Très rapide mais peu avoir des biais statistique (la séquence générée ne semble pas aléatoire).

Un bon **PRNG** doit passer des tests statistiques.

Les PRNG (Psuedorandom Number Generator)(ii)

Figure 2. – A « really good » PRNG.

Les CSPRNG (Cryptographically Secure PRNG)

Objectif

Générerer une séquence de nombre qui « semble » aléatoire et **qui peut être utilisé en cryptographie**.

Fonctionnement

- Idem que pour le **PRNG**
- Mais avec des contraintes supplémentaires :
  - Les **CSPRNGs** doivent passer le *next-bit test*.
  - Ils doivent résister « attaques d'extension de la compromission de l'État ».

Les chiffrements symétriques

Création d'un canal confidentiel

Utiliser un chiffrement à clé **secrète** (symmétrique)

- Un canal public pour transmettre les messages chiffrés ;
- Un canal authentifié **et** confidentiel pour transmettre la clé secrète.

Chiffrement à clé secrète

Un chiffrement à clé secrète E est un algorithme paramétré par une chaîne binaire **secrète** K partagée entre **deux entités** qui transforme un **message clair** M en un **message chiffré** C. Le déchiffrement associé D utilise le même paramètre K.

Canal confidentiel contre les attaques passives

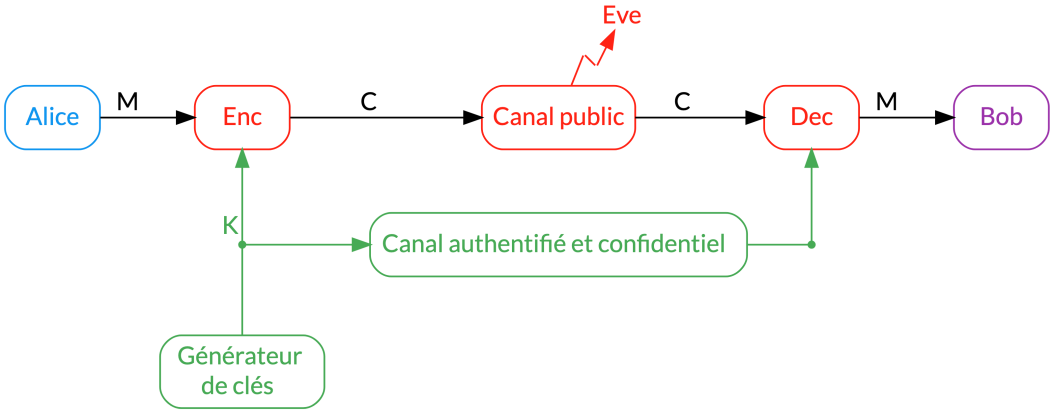

Figure 3. – Une communication utilisant un chiffrement symétrique. On a besoin du canal authentifié et confidentiel **une fois** au préalable de l'envoi d'un **nombre élevé de messages**.

Deux familles de chiffrements

Chiffrement par flux

Fonctionnement : *simuler* une clé aléatoire et faire un XOR avec le message (principe du masque jetable).

Soit $\oplus$ l'opérateur booléen XOR et $G_m : \{0,1\}^n \to \{0,1\}^m$ un générateur pseudo aléatoire.

Chiffrement par flux

$$E_K(M) = E(K, M) : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^m, C = M \oplus G_m(K)$$

Deux familles de chiffrements(ii)

Les chiffrements par bloc

Fonctionnement : chiffrer le message bloc par bloc.

Chiffrement par bloc

$$E_K(M) = E(K, M) : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n, C = E_K(M)$$

Fonction de déchiffrement associée à un chiffrement par bloc

$$D_K(C) = D(K, C) = E_K^{-1}(C) : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$$

$$\text{avec } M = D_K(C) \quad \text{et } \forall K, D_K(E_K(M)) = M$$

Construction des chiffrements par bloc

Les propriétés de Shannon (*Communication Theory of Secrecy Systems*, 1949)

Confusion

Volonté de rendre la relation entre la **clé de chiffrement** et le **texte chiffré** la plus complexe possible.

Diffusion

La diffusion est une propriété où la redondance statistique dans un texte en clair est dissipée dans les statistiques du texte chiffré. En d'autres termes, un biais en entrée ne doit pas se retrouver en sortie et les statistiques de la sortie doivent donner le moins possible d'informations sur l'entrée.

> Wikipédia

Construction des chiffrements par bloc(ii)

Les chiffrement itératifs

$$E_K(M) = E(K, M) = \left(E^r_{K_r}\left(E^r_{K_{r-1}} \ldots \left(E^r_{K_2}\left(E^r_{K_1}(M)\right)\right)\ldots\right)\right)$$

Construction des chiffrements par bloc(iii)

Les SPN (Substitution Permutation Network)

Dans les **SPN** chaque tout est composé de :

- une couche de **substitution** et de l'ajout d'une partie de la clé.
  - Cette couche est responsable de la *confusion*.
- une couche de permutation[1].
  - Cette couche est responsable de la *diffusion*.

La répétition de la fonction tour est utilisé pour mettre en place l'**effet avalanche**.

[1] dans certain cas la couche de permutation est enlevée du dernier tout étant donné qu'elle n'apporte aucun gain de sécurité et qu'elle demande des ressources inutiles en calcul.

Construction des chiffrements par bloc(iv)

Example AES (Advanced Encryption Standard)

Chiffrement symétrique standardisé par le NIST, succésseur du **DES**.

Construction du chiffrement

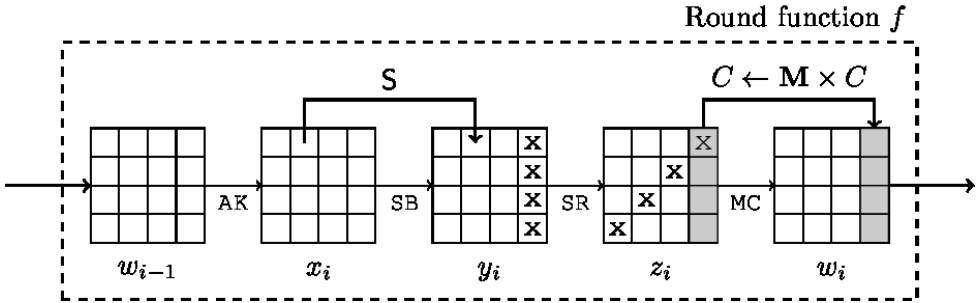

Figure 4. – Schéma de la fonction tour de l'**AES** (source Tikz for Cryptographer).

Construction des chiffrements par bloc(v)

Les réseaux de Feistel

$$L_0, \quad R_0 = M$$

$$L_i, \quad R_i = f_{K_i}(L_{i-1}) \oplus R_{i-1}, \quad L_{i-1}$$

$$C = L_r, \quad R_r$$

Le déchiffrement s'écrie alors :

$$L_r, \quad R_r = C$$

$$L_i, \quad R_i = R_{i+1}, \quad f_{K_i}(R_{i+1}) \oplus L_{i+1}$$

$$M = L_0, \quad R_0$$

Avantage : on est capable d'utiliser n'importe quelle fonction pour f, même des fonctions qui ne sont pas inversibles.

Construction des chiffrements par bloc(vi)

Example DES (Data Encryption Standard)

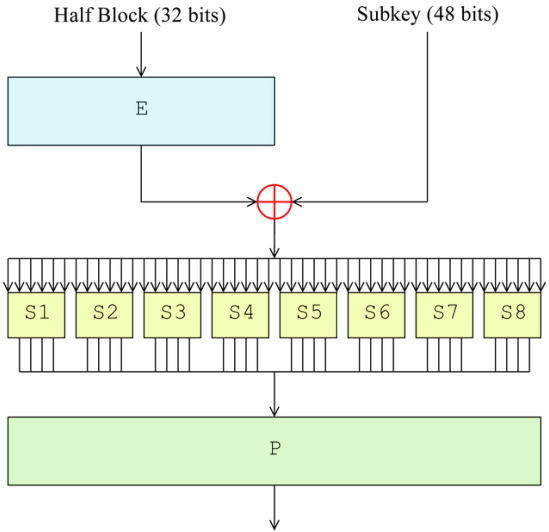

Figure 5. – Schéma du chiffrement **DES** (source Wikipedia).

Les modes d’opérations

Objectif

Transformer des chiffrements par **bloc** en chiffrements par **flux**.

Comment faire ?

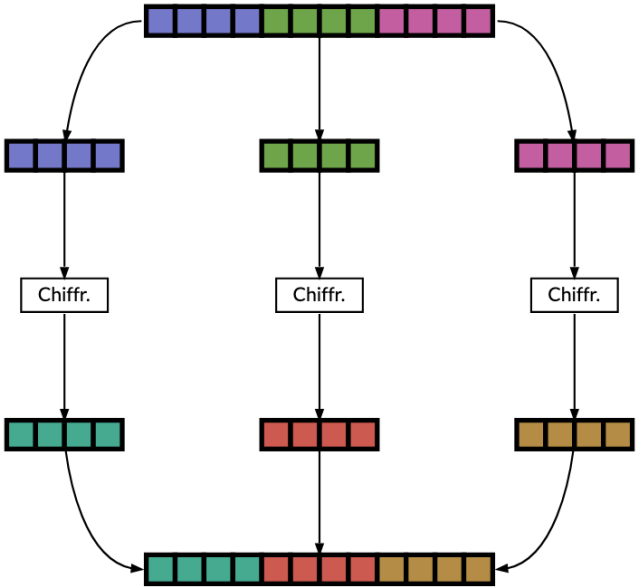

Figure 6. – Réprésentation du mode d'opération **ECB** (**E**lectronic **C**ode**b**ook).

Attention !

Les modes peuvent engendrer des faiblesses cryptographiques !

Figure 7. – Text clair (image bitmap) (gauche). Image chiffrée avec AES et le mode d'opération **ECB** (centre). Image chiffrée avec AES et le mode d'opération **CBC** (droite).

Les modes d'opérations

Cipher Block Chaining

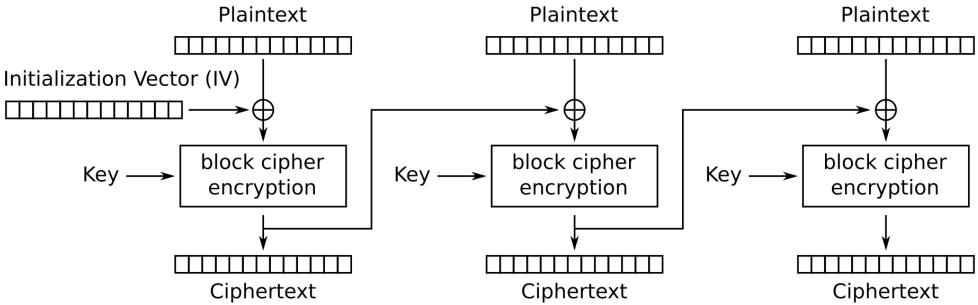

Figure 8. – Cipher Block Chaining Mode of Operation (source Wikipedia)

Problématiques :

- le chiffrement ne peut pas se faire en parallèle ;
- la taille du texte doit être un multiple de la taille du bloc.

Les modes d'opérations(ii)

Cipher Feeback

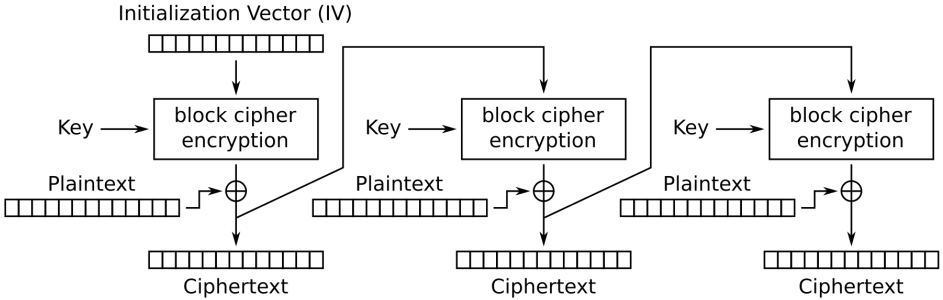

Figure 9. – Cipher Feedback Mode of Operation (source Wikipedia)

Problématiques :

- Le chiffrement ne prend pas en charge les pertes de blocs ni le chiffrement simultané de plusieurs blocs. Le décryptage, en revanche, est parallélisable et tolère les pertes.

Questions ?