IUT ANNECY
UNIVERSITÉ SAVOIE MONT BLANC

Cryptographie et sécurité

Cours 2: cryptographie symétrique

Mickaël Bettinelli
(mickael.bettinelli@univ-smb.fr)

Prérequis et objectifs

Connaissances nécessaire pour ce cours:

- Comprendre le fonctionnement des méthodes de chiffrement symétrique

Connaissances et compétences à acquérir à la fin du cours

- Connaître le fonctionnement de certaines méthodes modernes

Sommaire

1. Vue d’ensemble: chiffrements par blocs et par flot
2. Chiffrement par bloc
   a. Vue générale
   b. Présentation de AES
3. Chiffrement par flot
   a. Vue générale
4. Synthèse

Les services de la cryptographie

- Confidentialité: le message n’est pas lisible par tout le monde
- Intégrité: le message n’est pas modifiable par un tier
- Authentification: l’émetteur et le récepteur sont clairement identifiés
- Non-répudiation: l’émetteur ne peut réfuter avoir envoyé le message

Les services de la cryptographie symétrique

- Confidentialité: le message n’est pas lisible par tout le monde
- ~~Intégrité: le message n’est pas modifiable par un tier~~
- ~~Authentification: l’émetteur et le récepteur sont clairement identifiés~~
- ~~Non-répudiation: l’émetteur ne peut réfuter avoir envoyé le message~~

Les services de la cryptographie symétrique

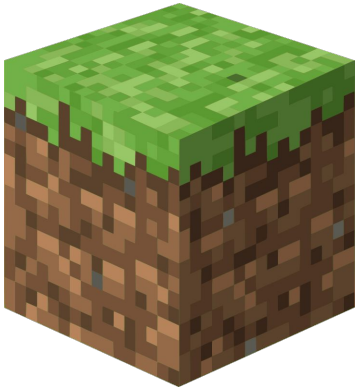
- Confidentialité: le message n’est pas lisible par tout le monde

Comment assurer la confidentialité ?

→ en chiffrant la donnée de façon à ce qu’elle ressemble le plus possible à une chaîne aléatoire.

Types de chiffrements

Par bloc

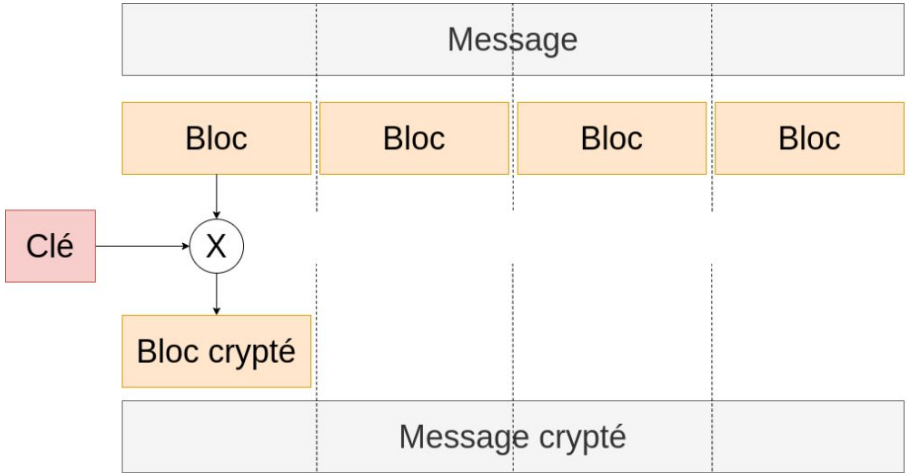


Par flot

Chiffrement par bloc

Fonctionnement:

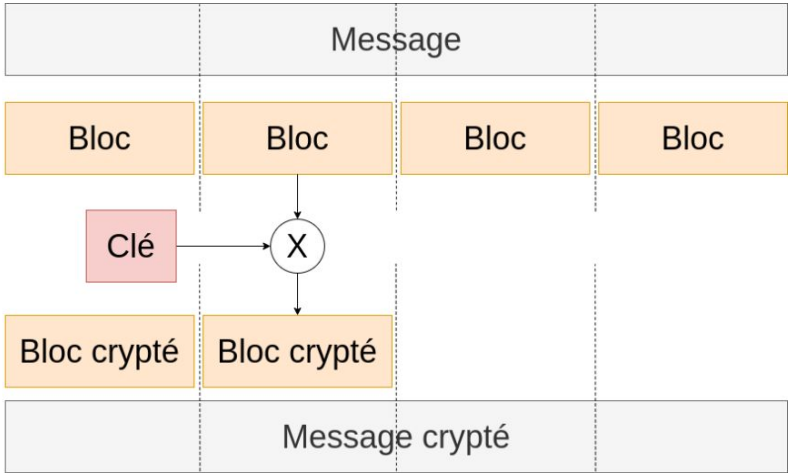
- Création d'une clé de taille fixe
- Division du message en blocs de la taille de la clé
- Chiffrement de chaque bloc avec la clé (par exemple avec un XOR)



Chiffrement par bloc

Fonctionnement:

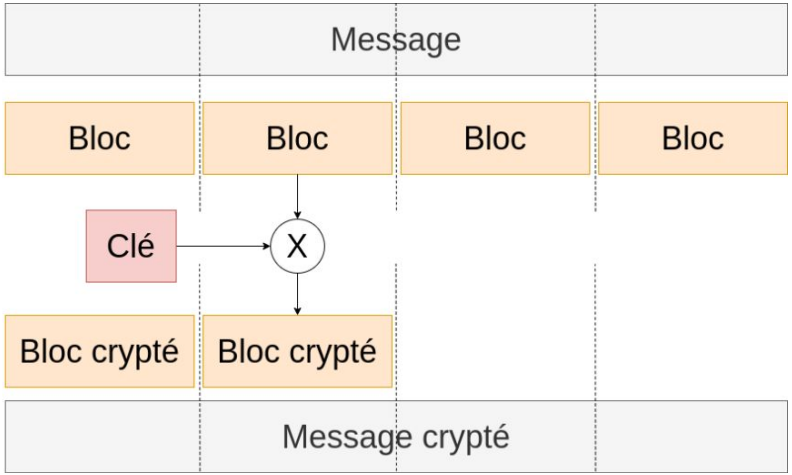
- Création d'une clé de taille fixe
- Division du message en blocs de la taille de la clé
- Chiffrement de chaque bloc avec la clé (par exemple avec un XOR)



Chiffrement par bloc

Inconvénient:

- Il existe des méthodes pour décrypter les chiffrements XOR (à cause des motifs)
- Computationnellement coûteux, peut être un peu lent



Chiffrement par flot

- Chiffrement à la volée sans attendre d’avoir tout le message
- Pas de découpage du message
- Chiffrement rapide
- Bien adapté aux applications temps réel

Chiffrement par flot

Fonctionnement:

- Utilisation d'un générateur de nombres pseudo-aléatoires
- Un XOR est opéré sur chaque bit du nombre généré avec un bit du message

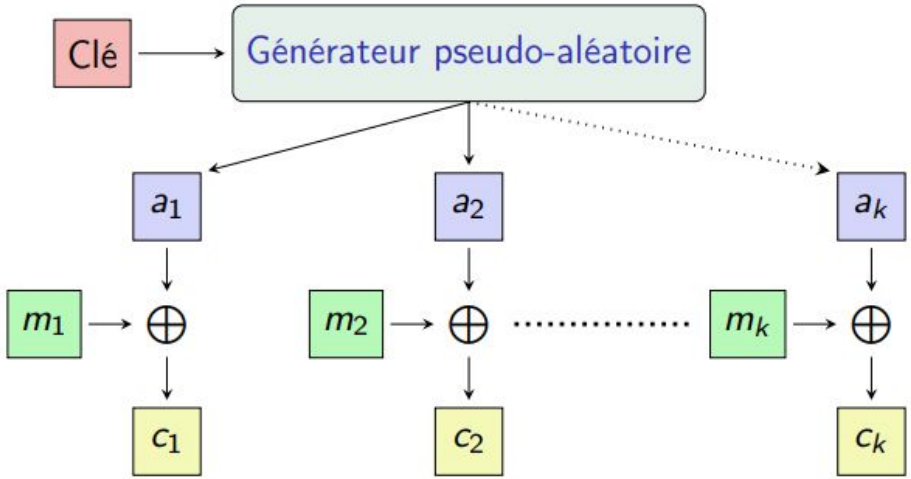


Image par Yves Legrandgérard, IRIF, Université Paris Diderot
https://www.irif.fr/_media/users/ylg/crypto.pdf

Chiffrement par flot

Inconvénient: pour une même clé, le générateur créera les mêmes nombres pseudo aléatoires.

Peu pratique pour éviter les motifs dans le message crypté.

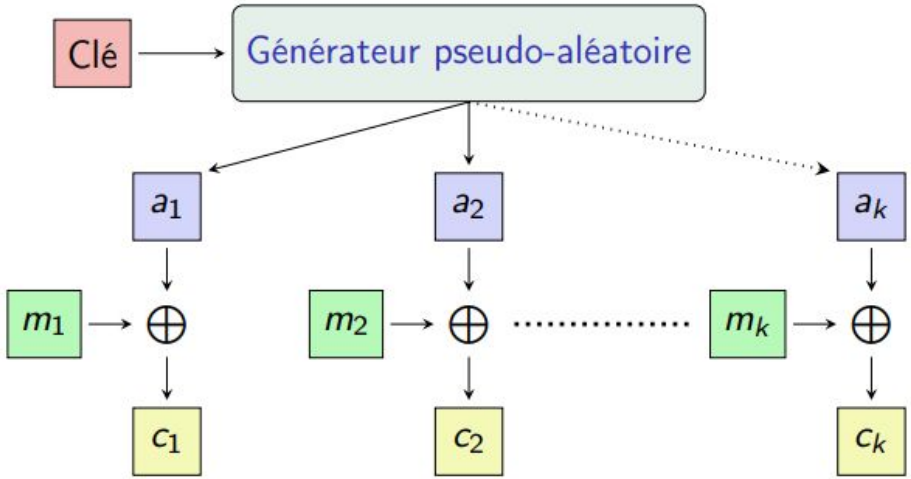


Image par Yves Legrandgérard, IRIF, Université Paris Diderot
https://www.irif.fr/_media/users/ylg/crypto.pdf

Chiffrement par flot

Pour éviter cela, on ajoute un vecteur d'initialisation qui modifie le comportement du générateur:

VI = bloc de bits combiné avec le premier bloc de données lors d'une opération de chiffrement.

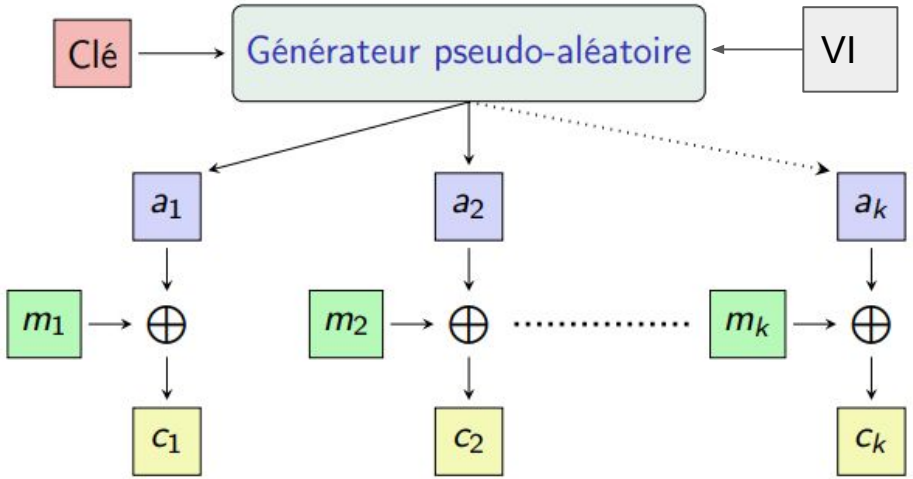


Image par Yves Legrandgérard, IRIF, Université Paris Diderot
https://www.irif.fr/_media/users/ylg/crypto.pdf

Chiffrement par flot

Chiffre de Vernam

- Algorithme créé en 1917
- Théoriquement incassable
- Difficile à mettre en oeuvre pour les communications via internet

Particularité: la création des clés

- La clé doit être au moins aussi longue que le message
- La clé doit être choisie de manière aléatoire
- Chaque clé ne doit être utilisée qu'une seule fois

En résumé

Par bloc:

- Découpage en bloc
- Chiffrement de chaque bloc pour chiffrer le message complet
- Des motifs peuvent être retrouvés si l'opération de chiffrement est trop simple (e.g., XOR):

Par flot:

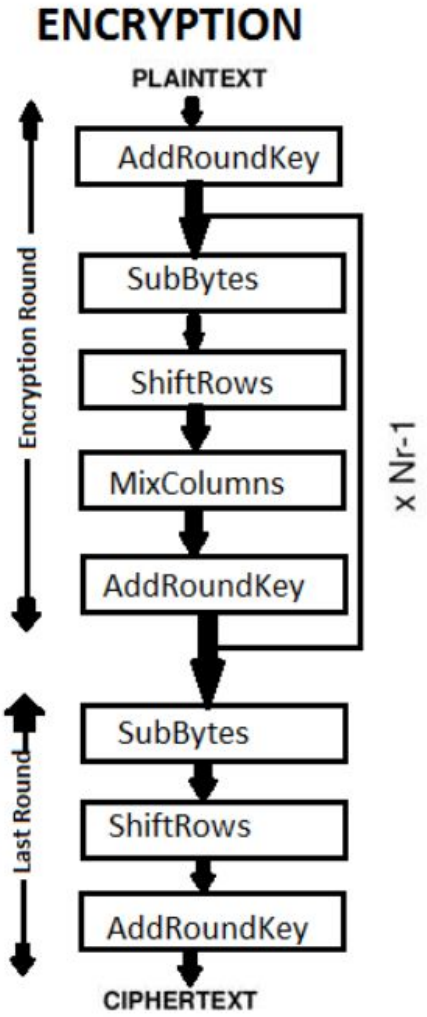
- Pas de découpage en blocs
- Chiffrement rapide: chiffrement "à la volée"
- Pratique pour les applications temps réel (e.g., wifi, bluetooth, etc.)

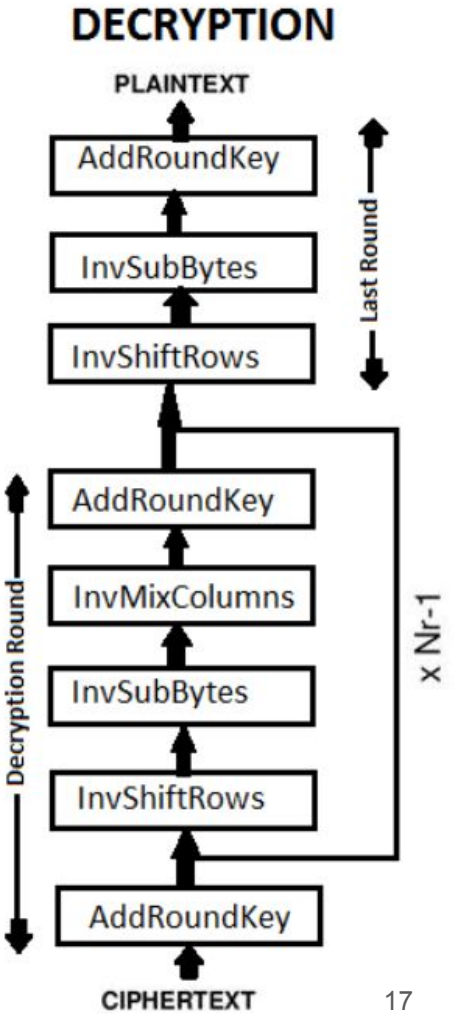
AES

Chiffrement AES (Advanced Encryption Standard)

- La clef est dérivée en plusieurs versions (10 à 14 selon la taille de la clef)
- Chaque version de la clef chiffre une fois un bloc
- Chaque bloc est chiffré avec la clé et le bloc précédent.
- Chaque tour effectue plusieurs opérations matricielles permettant de “mélanger” les bits du message

Chaque opération peut s’inverser de manière à retrouver le message initial.





AES

Avantages :

- Les octets ressemblent à des données aléatoires: pas de motifs = complexe à déchiffrer

Inconvénients :

- Un fichier chiffré est plus lourd qu'un fichier non chiffré => plus compliqué à envoyer par internet

Conclusion sur les chiffrements symétriques

Ces méthodes sont intuitives mais quelques inconvénients nuances leur utilisation:

- La longueur de la clé doit être la plus longue possible
- Les chiffrement symétriques nécessitent de transmettre la clé
  - très difficile sur internet car la clé peut être interceptée (il faut la chiffrer aussi)

Quand utiliser le chiffrement symétrique ?

- Utile pour chiffrer des données sensibles avec motifs

Ressources

https://fr.wikipedia.org/wiki/Advanced_Encryption_Standard

http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html

https://www.irif.fr/_media/users/ylg/crypto.pdf

https://nevonprojects.com/image-encryption-using-aes-algorithm/