Introduction à la Cryptographie

Ilyas Bambrik

Table des matières

Qu'est-ce que la cryptographie?

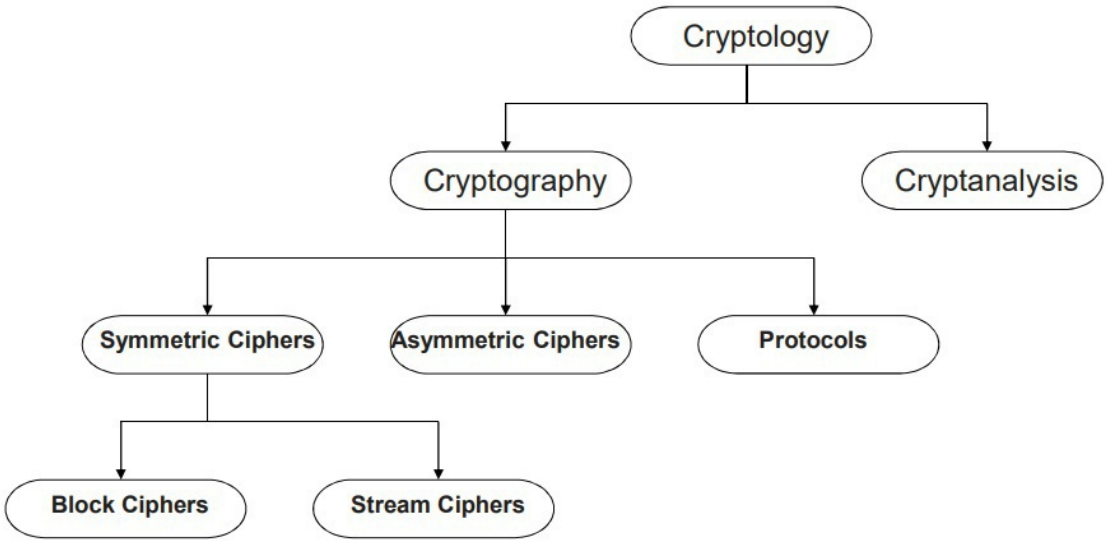


Figure 1. La cryptographie

- La cryptographie est un sous domaine de la *cryptologie* qui consiste à appliquer des opérations mathématiques permettant de cacher un texte claire des parties non autorisées.
- La cryptographie a existé pour plus de 4000 ans.
- Actuellement, cette technologie est utilisée dans tout domaine où le contenu de l'information doit être protégé (téléphonie, carte de crédit, applications comme les navigateurs web,etc).
- Sous domaines de la cryptographie :
    - *Symetric Cryptography :* La même clé est utilisée pour chiffrer et déchiffrer. Dit aussi *private key encription*.
    - *Asymetric Cryptography :* La clé utilisée pour le chiffrement est différente de celle utilisée pour le déchiffrement. Dit aussi *public key encryption*.
    - *Stream Cyphers :* (Sous type de la cryptographie symétrique) chaque bit du contenu claire est chiffré individuellement.
    - *Bloc Cyphers :* le contenu à transmettre est divisé en bloques de tailles fixes selon algorithme, et chaque bloque est chiffré individuellement.
    - *Hardware Cryptography :* la possibilité d'implémenter un schéma de chiffrement dans le

matériel directement (au lieu d'une implémentation logicielle) donne une rapidité d' exécution du chiffrement/ déchiffrement très élevée.

- *Random Number Generation :* la génération de chiffres aléatoires est une partie importante des systèmes de sécurités.

Chiffrement par bloc vs Chiffrement par flot

II

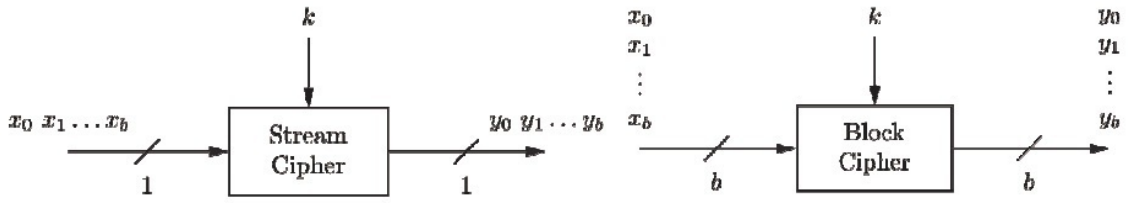


Figure 2. Chiffrement par bloc vs Chiffrement par flot

1. *Le chiffrement par bloque (bloc cypher)* effectue les opérations de chiffrement sur un bloque du contenu du texte claire de taille *"b"*. Utilisé dans les applications internet.
2. *Le chiffrement par flot (stream cypher)* effectue les opérations de chiffrement sur un seul bit avec un XOR. Ce genre de chiffrement est *utilisé comme une implémentation hardware* dans les appareilles à faible capacité (téléphone ou appareil embarqué).

Exemple : Méthodes de chiffrements par bloque / flot

Chiffrement par bloque : DES (Data Encryption Standard), AES (Advanced Encryption Standard), Caesar.

Chiffrement par flot : Linear Feedback Shift Registers (LFSRs).

Opérations basique de chiffrement

III

Les opérations de base du chiffrement sont la substitution et la permutation :

- La *substitution* consiste à changer une valeur par une autre (la valeur peut être un caractère, une séquence de bits ou un seul bit) ;
- La *permutation* consiste à changer les positions des éléments composants le contenu ;

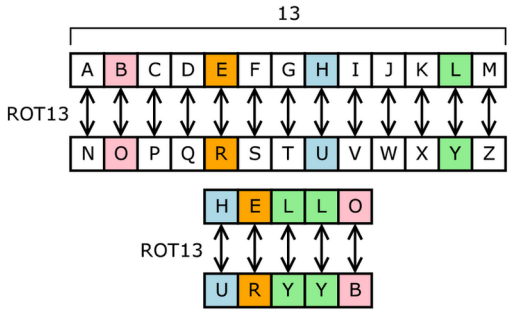


Figure 3. Substitution

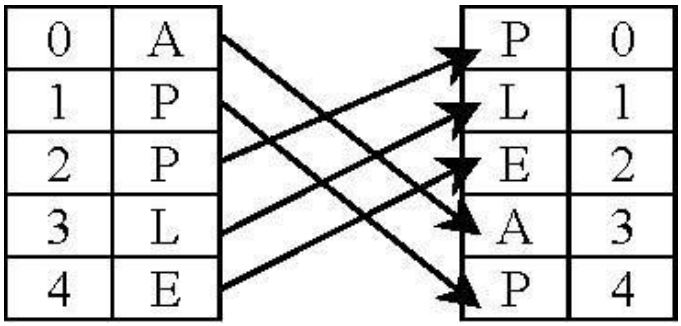


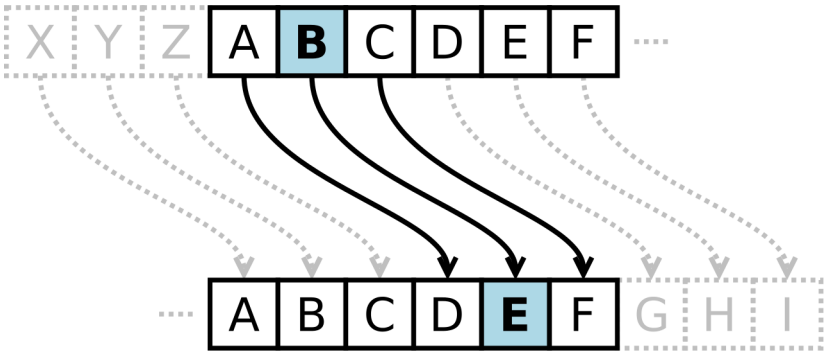
Figure 4. Permutation

Deux propriétés sont désirables dans les algorithmes de cryptographie modernes :

- *Conffusion :* Le contenu chiffré ne doit pas avoir de relation avec le contenu clair (cette propriété est assurée généralement par la substitution);
- *Diffusion :* Un changement d'un seul bit dans le contenu claire doit avoir un effet d'avalanche sur le contenu crypté (cette propriété est assurée généralement par la permutation);

Chiffrement de Caesar

IV



Exemple de chiffrement par substitution :

Chiffrement de Caesar (dit aussi *Shift Cypher*) :

Pour chaque caractère X dans le texte claire, celui-ci sera représenté par un caractère Y tel-que :

Y=E(X)=(X+K)%26

K : représente la clé privée.

Avec l'équation précédente X est substitué par un caractère du même alphabet.

Pour déchiffrer un texte crypté par ce système , il suffit de retrouver X a partir de Y et K.

X=D(Y)=(Y-K)%26

Problème :

- Combien de valeurs possibles pour la clé K ?
  K appartient à {0,1,2,3,...,24,25}. *Nombre de clés possibles == 26 (possible de casser ce chiffrement par brute force : tester touts les clés possibles)*
- Est ce que cette algorithme présente la propriété de *Diffusion* et/ou *Conffusion* ?
  La propriété Diffusion n'est pas assurée car le changement d'un bit du texte claire ne changera qu'un seul caractère dans le texte crypté.