Introduction à la cryptographie

I. Akharraz
Université Sidi Mohamed Ben Abdellah

ismail.akharraz@usmba.ac.ma

Sommaire

1. Introduction.

- Le développement de l'usage d'internet (fixe et mobile) et des appareils connectés, a encouragé l'échange d'énormes quantités de données de tous types (personnelles, économique, monétaires, ...).

- Ces données sont exposés à des menaces considérables.
- Il est indispensable de mettre en oeuvre une stratégie de sécurité informatique pour se protéger contre toutes les menaces potentielles.
- La partie soft de cette stratégie se base sur la cryptographie.

2. Définition et histoire.

Cryptographie :

- Art de dissimuler et de cacher un secret dans une écriture.
- Ensemble de principes et de moyens qu'on applique à des informations afin de les transformer et les rendre illisible et non utilisable que par les personnes auxquelles ils sont destinées.
- Protéger l'information contre toute utilisation frauduleuse.

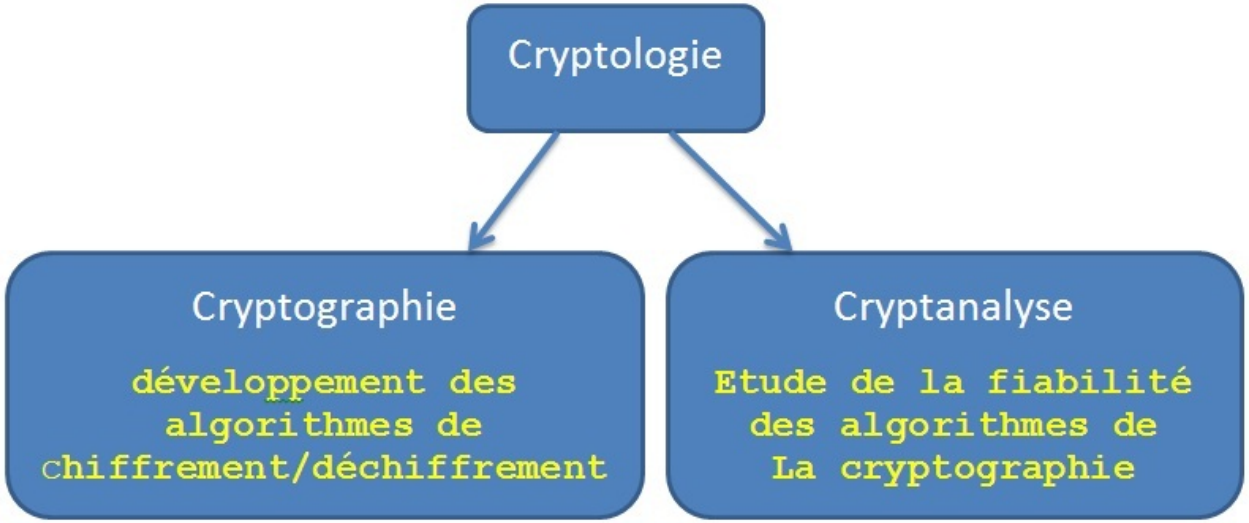
Histoire :

- Sparte entre 4000 et 5000 av.JC : scytales (bâton et un ruban pour colporter le message).

- Egypte à partir de 2350 Av.JC : plusieurs méthodes.
- Rome, vers 50 Av.JC, méthode ce Jules César : décalage des caratères.

2. Définition et histoire.

- Cryptologie : Science du secret; mathématique de conception d'algorithmes pour cacher des nombres.



- Il n y'a pas de sécurité sans cryptologie.

3. Object de la cryptographie

La cryptographie a pour objectif d'assurer les services suivants :

- Confidentialité :L'information ne peut être connue que par les personnes ayant droit.
- Disponibilité :L'information doit être à la disposition des utilisateurs auxquelles elle est destinée.
- Intégrité :L'information ne doit pas être modifiée ou détruite par accident ou par malveillance.
- Authentification :Le Contrôle des droits d'accès aux données.
- Traçabilité :Pouvoir suivre toute activité sur les informations. Impossible de nier ses actions sur des informations.

4. Concepts de bases

- Chiffrer/Déchiffrer (Crypter/~~Décrypter~~).
- Chiffre ou code : algorithme pour chiffrer et déchiffrer.
- Clé : Un ou plusieurs paramètres utilisés dans le calcul du chiffre et qui doivent tenu au secret.
- Cryptosystème ou Système cryptographique est un quintuplet S ={ *P , C , K , E , D* } *avec :*

(1) P : ensemble fini de textes clairs (plain texts).
(2) C : ensemble fini de textes chiffrés (cipher texts).
(3) K : ensemble fini de clés (key space).
(4) E : ensemble fini de règles de chiffrement (encryption rules).
(5) D : ensemble fini de règles de déchiffrement (decryption rules).

$$\forall k \in K, \exists e \in E, \exists d \in D \text{ tel que : } (e,k) : P \to C, (d,k) : C \to P \text{ et } (d,k) \circ (e,k) = id_P$$

(e,k) et (d,k) sont les algorithmes des chiffrement et de déchiffrement.

- *Robustesse : degré de résistance du cryptosystème aux attaques.*

5. Principe de chiffrement/déchiffrement

- Chiffrement: Les informations à chiffrer (texte clair ; lisible) subi un algorithme de chiffrement qui utilise un jeu de clé pour transformer le texte clair en texte chiffré.

- Déchiffrement : Un algorithme de déchiffrement et le jeu de clé sont appliqués au texte chiffré pour retrouver le texte claire.

6. Algorithmes Cryptographiques

- Jusqu'au 19ème siècle les algorithmes (méthodes de chiffrement) étaient gardé en secret.

- Principe de Kerckhoff (1883) :
  - La sécurité du chiffre ne doit pas dépendre de ce qui ne peut pas être facilement changé.
  - L'algorithme doit être connu par tout le monde et seul un paramètre (appelé clé) doit être secret.

- Principe de Claude shannon (1940): L'adversaire connait le système.

Avantage de la publication des algorithmes :

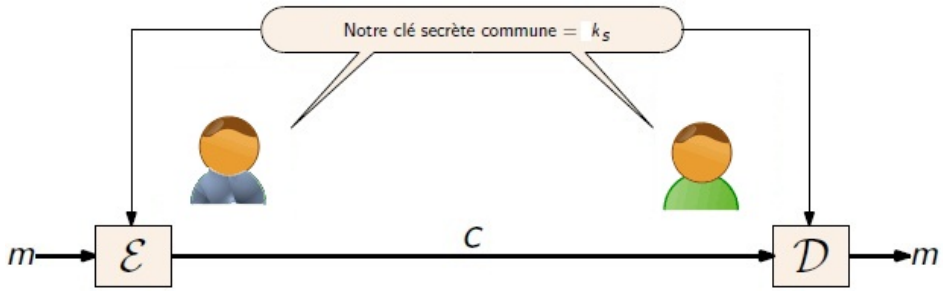
- Large utilisation : plus d'expérimentation.
- Découverte des failles : amélioration du code.
- Se libérer de la tâche de protection du code.
- Diversification des implémentations logicielles.
- Standardisation générale d'une version plus sûr.

6. Algorithmes Cryptographiques.

- Un système cryptographique est composé de trois algorithmes :
  - Un algorithme de génération des clés.
  - Un algorithme de chiffrement.
  - Un algorithme de déchiffrement.
- Il y'a trois grandes catégories d'algorithmes cryptographiques :
- Algorithmes symétriques :
  - Cryptographie symétrique.
  - Cryptosystèmes à clé symétrique.
- Algorithmes asymétriques :
  - Cryptographie symétrique.
  - Cryptosystèmes à clé symétrique.
- Algorithmes de hachage(fonctions de hachage).

7. Algorithmes symétriques

- Cryptographie à clé secrète : usage d'une seule clé, tenue secrète, lors du chiffrement et du déchiffrement.
- Le message est tarnsformé en suite de bits qui subit des permutations et des substitution.



- Clés générées aléatoirement.
- Avantage principal : la rapidité.
- Problème :
  - Distribution des clés.
  - Système à N utilisateurs : N.(N-1)/2 paires de clés.

7. Algorithmes symétriques

- Deux grandes catégories cryptosystèmes symétriques :

Chiffrement par blocs: les messages sont découpés en blocs

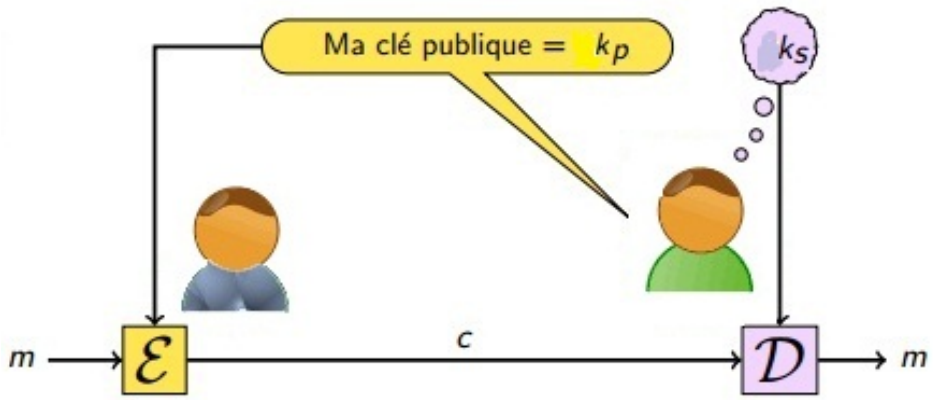
- DES: blocs de 64 bits, clés de 56 bits
- IDEA: blocs de 64 bits, clés de 128 bits
- AES: blocs de 128 bits, clés de 128, 256 bits
- ...

Chiffrement par flots: les données sont traitées en flux

- Pseudo-Vernam : on « XOR » un pseudo-aléa au flux
- RC4 : chiffrement octet par octet
- ...

8. Algorithmes asymétriques

- Cryptographie à clé publique.
- Le chiffrement se fait par une clé publique k_p.
- Le déchiffrement se fait par une clé secrète k_s.



- La clé secrète k_s ne sert qu'au déchiffrement.
- La clé secrète k_p ne peut pas déchiffrer et ne peut non plus retrouver k_s.

8. Algorithmes asymétriques

- Algorithme asymétrique le plus utilisé : RSA.

- Ces algorithmes se basent des fonction unidirectionnelle : facile à calculer dans un sens, mais presque impossible dans le sens inverse :

  - Exponentiation de grands nombres premiers (RSA),
  - Problème des logarithmes discrets (ElGamal),
  - Problème de Sac à dos (Merkle-Hellman).

- Le chiffrement asymétrique est environ 1000 fois plus lent que le chiffrement symétrique.

- Seules n paires de clés sont nécessaires; chaque utilisateur possède une paire (k_s, k_p).

9. Fonctions de hachage

Principe : Un message clair (en binaire) de longueur quelconque est transformé en un message de longueur fixe inférieure à celle de départ.

Le message réduit s'appelle "Haché" ou "Condensé".

$$H : \{0,1\}^* \longrightarrow \{0,1\}^n;\ M \longrightarrow H(M)$$

Deux caractéristiques importantes :

(1) H est unidirectionnelle : Il est calculatoirement presque impossible de retrouver M à partir de H(M).
(2) H est sans collisions : Etant donné un M, il est calculatoirement presque impossible de trouver un $M' \neq$ M tel que $H(M') = H(M)$.

Fonctions classiques : MD2, MD4, MD5, SHA-1 et SHA3.