Prof : Thierry Meyer

@Thitax

Thierry.meyer@tm.consultants.fr

# Cours du 05 Sept 2017

1. Les fondamentaux de la cryptographie appliquée

Bruce Schneier - @schneierblog

Applied Cryptography

<https://www.schneier.com>

Jean Philippe Aumasson - @veorq

<https://131002.net>

Il a fait le SSTIC

Renaud Lifchitz - @nono2357

Il a fait une présentation à la St’hack

## **Qu’est-ce que la cryptographie**

C’est la science des écritures.

C’est un sous-ensemble de la cryptologie :

* + - Cryptographie
    - Cryptanalyse

## **A quoi sert la cryptographie ?**

Elle a une utilité pour un SI

4 services de sécurité :

* + - Confidentialité
    - Intégrité
      * Permettre au destinataire de savoir qu’il est exact et …
    - Authentification
    - Non répudiation
      * Impossibilité de nier l’évidence

Les acteurs de la cryptographie

* L’utilisateur (Users) :
  + Expéditeur (Sender)
  + Destinataire (Receiver)
* Le cryptographe (Cryptographers)
* Le cryptanalyse (Cryptanalysts)

Utilisateur de confiance : trent

Utilisateur malicieux : Malory

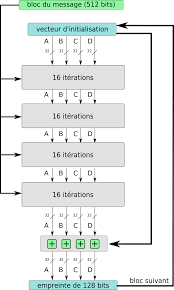
Utilisateur qui fait du Ice dropping : Eve

> La notion de message et de chffrement

* + Message clair (Plaintext ou cleartext)
  + Message chiffré (Ciphertext)
  + Chiffrement (Encryption)
  + Déchiffrement (Decryption) != Décryptage

> Les algo. Cryptographiques

* Cryptographic algorithm
* Cipher



*Vue générale des opérations de l’algorithme MD5*

> Les clefs cryptographiques

* Cryptographic keys

Exemple d’une clef de chiffrement RSA 2048bits

* One-time Pad
* Clefs cryptographiques à une seule utilisation
* Clef de même longueur que le message
* Technique de chiffrement parfaite si :
  + - La clef n’est effectivement utilisée qu’une seule fois ET
    - Qu’elle est générée de façon parfaitement aléatoire

Soit :

* ONE TIMEPAD le message
* TBFRGFARFM la clefs de chiffrement

Alors : IPKLPSFHGQ est le message chiffré

Car :

* O + T modulo 26 = I

> principe de fonctionnement générale (Image)

Soit :

* M le message clair
* C le message chiffré
* E la fonction de chiffrement
* D la fonction de déchiffrement

Alors :

E(M) = C & D(c) = M

La fonction booléenne XOR (« ou exclusif)

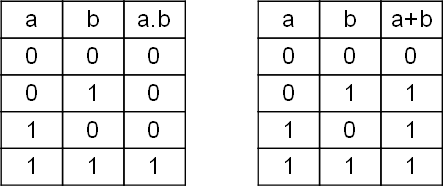
Soit :

A & B deux opérandes,

1 = true

0 = false

Tableau de vérité



Rotation de 13 caractère : ROT13 = code obfusqué

A+A = 0

A+A(barré) = 1

Les principaux systèmes crypto

Les fonctions de hachage

* Principe de fonctionnement
* Fonction de prise d’empreinte numérique
* A partir d’une donnée quelconque (pre-image), l’algorithme génère une donnée :
  + De longueur fixe
  + Représentative de la donnée initiale
  + On appelle cette donnée h empreinte (Hash)

Principe de fonctionnement (d’un point de vue mathématique)

Soit :

H l’empreinte de M

Alors :

H(M) = h

Principe de fonctionnement (en image)

* Renforcement par l’utilisation d’un sel (salt)
* SCHEMA
* Principaux algos
* MD5 (Message Digest Algorithm)
* SHA (Secure Hash Algorithm)
* Il ne faut plus utiliser MD5 et SHA1
* A quoi servent les fonctions de hachage ?
* Contrôle d’intégrité

IDS : Intrusion détection système

HIDS : Host based intrusion detection system

La cryptographie symétrique

Principe de fonctionnement

* Consiste à chiffrer et déchiffrer un message via :
  + La même clef ET
  + Le même algorithme
* Les partenaires partage la même clefs partagé secrète

Les différents types d’algo

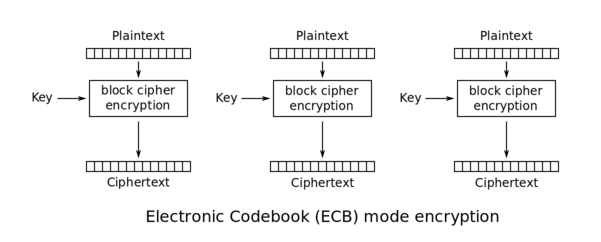
* Algo de chiffrement par flux (Stream Ciphers)
* Algo de chiffrement par bloc (Block Ciphers)

Les algorithmes cryptographiques symétriques par flux

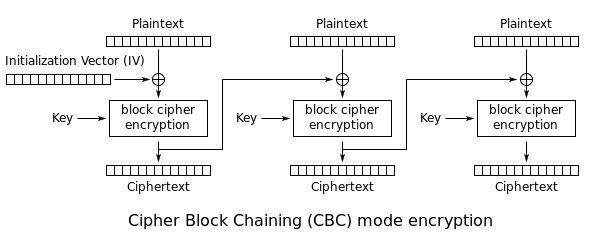
* Message à chiffrer de longueur quelconque
* Chiffré bit par bit, ou octet par octet (dans certains cas en mot de 32bits)
* En général réalisé au moyen d’un XOR

Principaux algorithmes symétriques par flux :

* RC4
* SEAL
* …
* Le mode d’opération ECB (Electronique Codebook)
  + Chiffrement (déchiffrement)



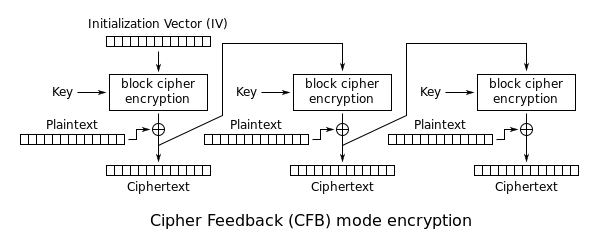
* Le mode d’opération CBC (Cipher Block Chaining)
  + Chiffrement



* + Dechiffrement



* Le mode d’opération CFB (Cipher feedback)
  + Chiffrement



* + Déchiffrement
* Le mode d’opération OFB (Output feedback)
  + Chiffrement
  + Déchiffrement
* A propos du Vecteur d’initialisation (IV)
  + Bloc de données aléatoire utilisé pour démarrer le chiffrement du premier bloc
  + Ajouté une notion de hasard au chiffrement
  + /!\ ne pas utiliser le même IV avec deux clefs différentes !
  + Pas nécessaire de chiffrer l’IV
* Principaux algos symétriques par blocs :
  + DES, 3DES (DATA Encryption STANDARD) : A banir !
  + AES (Advanced Encryption Standard)
  + IDEA
  + BlowFish
  + SAFER

Il est recommandé d’utiliser **AES-256-CBC**

* A quoi sert la cryptographie symétrique ?
  + Authentification
  + Confidentialité

## La cryptographie Asymétriques

* Principe de fonctionnement
  + Chaque participant dispose d’une paire de clefs (biclef)
    - Une clé privée
    - Une clé publique
  + L’une sert à chiffrer, l’autre à déchiffrer
  + Le même algorithme est utilisé par le chiffrement et le déchiffrement
* Suite :
  + Repose essentiellement sur des problèmes mathématiques complexes :
    - Factorisation d’un nombre entier formé de grand facteurs premiers
    - Résolution d’un algorithme discret sur un corps fini
    - Résolution d’un logarithme discret sur une courbe elliptique
* Deux applications
  + Chiffrement
  + La signature électronique
* Le chiffrement avec la cryptographie asymétrique
  + Alice chiffre son message avec la clef publique de Bob
  + Alice envoie le message à bob
* La signature électronique avec la cryptographie asymétrique
  + Alice chiffre avec sa propre clef privée
  + Alice envoi le message ainsi que la signature à Bob
  + Bob déchiffre la signature avec la clef publique de Alice
* Principaux algos asymétriques :
  + RSA
  + ELGamal
  + Systèmes à courbes elliptiques
  + DSA (Uniquement pour la signature électronique)

Il est recommandé d’utiliser RSA avec des clefs de 2048 bits

A quoi sert la crypto asymétrique ?

* Authentification
* Confidentialité
* Intégrité
* Non-répudiation

1. Les infrastructures à clé publique (PKI)
2. Le fonctionnement du protocole TLS (Transport layer security)