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

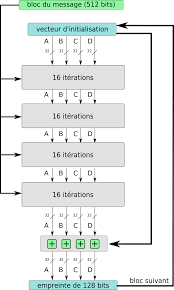
Utilisateur qui fait du Ice dropping : Eve

> 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)

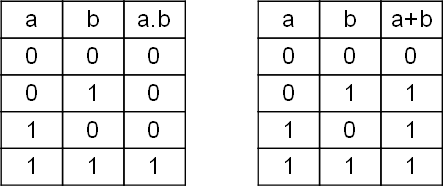
Soit :

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

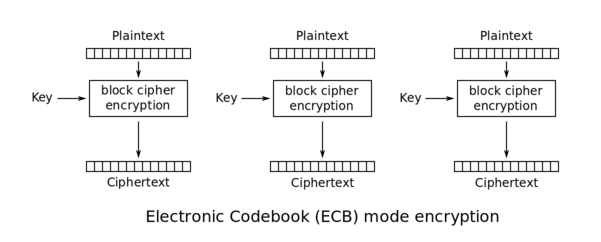
* Algo de chiffrement par flux (Stream Ciphers)
* Algo de chiffrement par bloc (Block Ciphers)

Les algorithmes cryptographiques symétriques par flux

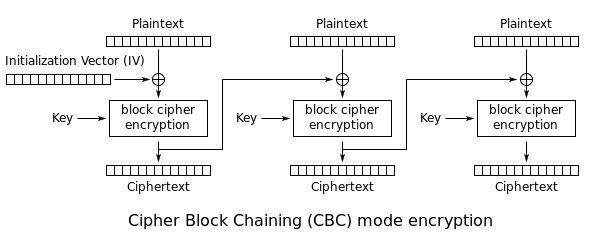
* Message à chiffrer de longueur quelconque
* Chiffré bit par bit, ou octet par octet (dans certains cas en mot de 32bits)
* En général réalisé au moyen d’un XOR

Principaux algorithmes symétriques par flux :

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



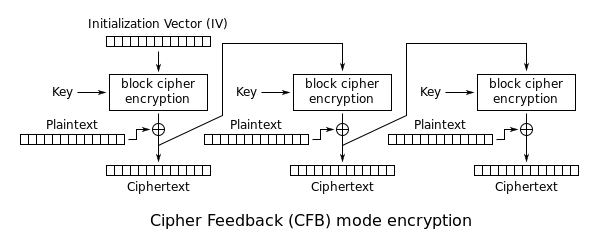
* Le mode d’opération CBC (Cipher Block Chaining)
  + Chiffrement



* + 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
* A propos de RSA
  + Fondé en 1877 par Ron Rivest, Adi Shamir et Leonard Adlemant
  + Basé sur la complexité de factoriser des grands nombres
* Détermination de la clef publique :
  + On choisi n produit de deux nombres premiers p et q (qui doivent rester secrets), donc n = p.q
  + On choisi e tel que e soit premier avec (p-1) et (q-1)
  + Le nombre n est appelé modulus de la clef
* Calcul de la clef privée
  + L’entier d est alors calculé avec l’algo d’Euclid tel que d = e-1 mod ((p-1)(q-1))
  + L’entier d est la clé privé
* Chiffrement
  + M = message clair
  + C = message chiffre
  + E exposant public
  + N le modulus

Alors

C = M(e) mod n

* Déchiffrement
  + Idem +
  + D la clé privée

Alors :

C = M(d) mod n

1. Les infrastructures à clé publique (PKI)

Sécuriser ses échanges électroniques avec une PKI (ISBN : 2-212-11045-6)

1. Définir une PKI et de ses acteurs (ICP)
   1. Qu’est-ce qu’une PKI ? A quoi ça sert ?

Problématique :

* + - Confidentialité
    - Intégrité
    - Non répudiation
    - Authentification
    - Mais comment garantir l’authenticité de la clef publique
    - Nécessité de faire intervenir un tiers de confiance.
    - Certificat Electronique :
      * En 78 Loren Kohnfilden
      * Ensemble de données contenant un nom et une clef publique signé numériquement
    - Certificat de clef publique
      * Document électronique qui contient des données publiques
      * Garantir l’authentification de la clef publique qu’il contient
      * Garantir à Bob que la clef publique qu’il utilise est bien celle de Alice
    - La clef publique qu’il contient permettra de chiffrer des données et/ou de vérifier une signature électronique.
    - Pour remplir correctement sa fonction, un certificat doit :
      * Etre propre à l’entité pour laquelle il a été émis.
      * Permettre de trouver facilement et rapidement l’identité de cette entité.
      * Contenir la clef publique de cette entité
      * Permettre de trouver rapidement et facilement l’autorité qui garantit son contenu
      * Etre infalsifiable 🡪 (Signé)
      * Période de validité
      * Avoir un numéro d’identification
      * Faire figurer l’utilisation qui doit être fait de la clef qu’il contient

Un certificat X509 contient différents types de champs :

* + - Standards
    - Extension (type, criticité, valeur)
  + 4 grands groupes de type d’extension :
    - Information sur les clefs
    - Information sur l’utilisation du certificat
    - Attribut de l’utilisateur et de l’AC (Autorité de Certification)
    - Contrainte de co-certification

Le porteur du certificat

* + - Propriétaire de la clef publique contenu dans la certification
    - L’entité qui a demandé que sa clef pub soit certifié

L’utilisateur

* + - Celui qui utilise la clef contenue dans le certificat

L’infrastructure de confiance :

* + - L’autorité de certif (AC)
    - Autorité d’enregistrement (AE)
    - Le service de publication
    - Le dépôt de la LCR, et
    - L’Autorité d’horodatage (AH)
    - L’Autorité de Validation (AV)
  1. Le certificat électronique
  2. Les acteurs d’une PKI et leur rôle

1. Les processus d’un PKI(ICP)
   1. Le cycle de vie des certificats
      1. Phase d’initialisation
         1. Enregistrement d’une demande
         2. Authentification d’une demande d’enregistrement
         3. Génération du certificat
         4. Distribution au certificat (et de la biclef)
      2. Phase d’utilisation
      3. Phase de révocation / suspension
      4. Phase de renouvellement
      5. La création des supports physiques.
   2. Création d’un certificat

1° Le sujet fait une demande de certificat

2° L’AE demandes des précisions sur son identité et l’utilisation du certificat

3° Le sujet transmet les informations ainsi que sa clef pub

4° L’AE transmet un challenge et le sujet le déchiffre

5° L’AE possède 2 vérification

6° Si OK l’AE demande la création du certificat à l’AC

7° L’AC génère le certificat et le signe

8° Puis le renvoie à l’AE et le publie dans le dépôt

9° L’AE transmet le certificat au porteur

* 1. Expiration / renouvellement
  2. Révocation du certificat
  3. Processus de validation

1. Les modèles de confiance
   1. Les différents modèles de confiance
   2. Les différentes architectures des PKI
2. Le fonctionnement du protocole TLS (Transport layer security)