# CRYPTOGRAPHIE

Réseaux – Fiche 6

## I. Objectifs

- Confidentialité
- Intégrité
- Authenticité

## II. Définitions

- **Cryptographie :** science du chiffrement
- **Cryptanalyse :** déchiffrement sans la clé
- **Cryptologie :** Cryptographie + Cryptanalyse
- **Chiffrement :** clair à chiffré
- **Déchiffrement :** chiffré à clair avec clé
- **Décryptage :** chiffré à clair sans clé
- **Texte clair :** non chiffré
- **Attaque sur texte chiffré seul :** message chiffré uniquement
- **Attaque à texte clair connu :** message chiffré et clair
- **Attaque à texte clair choisi :** possède le système de chiffrement
- **Attaque à texte chiffré choisi :** possède le système de déchiffrement

## III. Attaques

### 1. Depuis le LAN de l'attaqué *(hub, wifi, switch)*

- APR cache poisoning
- ICMP redirect
- Reconfiguration des switchs
- Attaque sur le wifi

### 2. Depuis un autre réseau

- Se faire passer pour le serveur après du client (DNS cache poisoning, modif serveur DNS, …) : Man In The Middle
- Prendre la main sur un routeur et rediriger ou copier le flux

## IV. Cryptographie

### 1. Cryptographie symétrique

#### a. Principe

- A génère une clé et la communique à B
- A chiffre le message et l'envoie à B
- B déchiffre le message

#### b. Problèmes

- Génération de clé
- Transmission de la clé

#### c. Principaux algorithmes

- DES / 3DES / Blowfish / AES

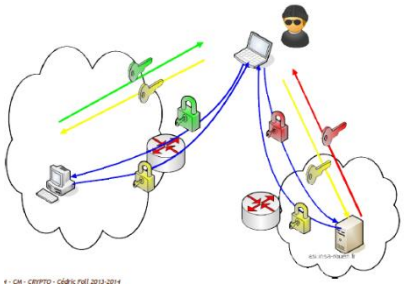
## 2. Cryptographie asymétrique

### a. Principe

- Clé publique : permet de chiffrer
- Clé privée : permet de déchiffrer

### b. Problèmes

- Génération de la clé
- Plus lent que symétrique
- Ne protège pas du MITM



### c. Principaux algorithmes

- RSA / DSA

### d. Diffie Hellman : principe d'échange de clé

- Echange de la clé symétrique avec la clé asymétrique

## 3. Fonction de hachage

### a. Définition

En théorie :

$$F(M) \nrightarrow M \quad | \quad M, F(M) \nrightarrow M' \mid F(M') = F(M) \quad | \quad \nexists (M, M') \mid F(M) = F(M')$$

En pratique, il existe collision

### b. Utilisation

- Ne pas stocker les **mots de passe** en clair
- Vérification de **l'intégrité** d'un message
- **Signature numérique**
  - On envoie : $\{M, S = C_{priv}(H(M))\}$
  - On vérifie l'authenticité à la réception si $C_{pub}(S) = H(M)$

## 4. Certification et PKI

### a. Principes

- Des tiers certifieurs fournissent des certificats associant entité et clé publique de l'entité signés par leur clé privés (connues par les navigateurs).
- Permet de confirmer l'authenticité d'une clé publique et éviter le MITM.
- Système de chaine de certifications : un grand certifieur certifie la clé d'un plus petit qui fournit un certificat.

### b. Services fournis par une infrastructure « IGC »

#### *i. Services principaux*

1. Fabrication des comptes clés
2. Certification des clés publiques et publications des certificats
3. Révocation de certificats (et publication des listes de révocation)
4. Gestion de la confiance dans la fonction de certification

#### *ii. Services connexes*

5. Gestion des tokens
6. Stockage de clés privées/certificats (comptes séquestres)
7. Horodatage (vital pour la révocation et les durées de validité)