Chap. I : Principes fondamentaux de la cryptographie

Laurent Poinsot

25 septembre 2009

Plan

Plan

Plan

Plan

Plan

Terminologie

1. Cryptologie : Cela signifie la ”science du secret”. La cryptologie se partage entre la *cryptographie* et la *cryptanalyse* ;
2. Cryptographie : Étude des mécanismes destinés à assurer - entre autres - la confidentialité des communications ;
3. Cryptanalyse : Son but est de déjouer les protections cryptographiques mises en place.

Plus précisément,

1. Cryptographie : Étude et conception des procédés de chiffrement des informations ;
2. Cryptanalyse : Analyse des textes chiffrés pour retrouver des informations dissimulées, Analyse des procédés de chiffrement afin d'en découvrir les failles de sécurité.

Cryptographie VS stéganographie

Il faut distinguer la cryptographie de la stéganographie.
La cryptographie permet de transformer un message ”clair” en un cryptogramme (message ”chiffré”) de sorte que le message originel soit complétement incompréhensible.
La stéganographie permet de dissimuler l'existence même de l'information secrète. Par ex. l'encre sympathique ou encore la lettre de George Sand à Alfred de Musset.

Les protagonistes traditionnels d'une communication chiffrée :

1. Alice et Bob : ils souhaitent se transmettre des informations de façon confidentielle. Ce sont les interlocuteurs légitimes ;
2. Oscar : un opposant (ou ennemi, espion, adversaire) qui a pour but d'espionner les communications entre Alice et Bob.

Objectif de la cryptographie

L'objectif fondamental de la cryptographie :
Permettre à Alice et Bob de communiquer sur un canal **public** peu sûr de telle façon qu'Oscar ne soit pas en mesure de comprendre les données échangées.
Un canal public est un canal de communication auquel tout le monde à accès et dont les commications sont susceptibles d'être écoutées par n'importe qui, sans trop de difficultés. Par exemple, le réseau téléphonique, le réseau Internet, mais aussi l'atmosphère (pour les fumées utilisées par les amérindiens pour communiquer à distance).

1. Texte (ou message) clair : Information qu'Alice souhaite transmettre à Bob. Par exemple, un texte en français ou des données numériques ;
2. Chiffrement : Processus de transformation d'un message clair M de façon à le rendre incompréhensible (sauf aux interlocuteurs légitimes). Il est basé sur une fonction de chiffrement E qui permet de générer un message chiffré $C := E(M)$;
3. Déchiffrement : Processus de reconstruction du message clair à partir du message chiffré. Il est basé sur une fonction de déchiffrement D telle que si C est le message chiffré correspondant au message clair M, alors $D(C) = M$.

Propriété essentielle au déchiffrement

Pour que l'on puisse réaliser le déchiffrement, il faut que les fonctions E et D vérifient la propriété suivante :
Soit M un message clair. Si $C = E(M)$, alors
$D(C) = D(E(M)) = M$.

Notion de clef

En pratique, et pour plus de sécurité, les fonctions E et D sont paramétrées par des clefs K_e et K_d (K_e est la clef de chiffrement et K_d est la clef de déchiffrement). Dire que E et D sont paramétrées signifie qu'elles dépendent de la clef. On note cette dépendance E_{K_e} ou D_{K_d}. Pour M un message clair, on doit avoir

$$\left\{ \begin{array}{rcl} E_{K_e}(M) & = & C\,, \\ D_{K_d}(C) & = & M\,. \end{array} \right.$$

K_e et K_d appartiennent à l'espace des clefs $\mathcal{K}$.

Propriété de déchiffrement

Pour permettre le déchiffrement, la propriété suivante doit être vraie dans l'espace des clefs $\mathcal{K}$:
Quelle que soit la clef de chiffrement $K_e \in \mathcal{K}$, il existe au moins une clef de déchiffrement $K_d \in \mathcal{K}$ telle que quel que soit le message clair M, $D_{K_d}(E_{K_e}(M)) = M$.
Cette propriété est essentielle pour réaliser le déchiffrement.

Protocole d'utilisation d'un système cryptographique

Un **système cryptographique** ou **procédé** (ou **algorithme**) **de chiffrement** est la donnée

1. d'un espace des clefs $\mathcal{K}$;
2. de fonctions de chiffrement et de déchiffrement paramétrées par des éléments de $\mathcal{K}$ et qui vérifient la *propriété de déchiffrement*.

Deux catégories de cryptosystèmes

Il existe deux grandes catégories de systèmes cryptographiques :

1. systèmes à clef secrète (ou symétriques) : $K_e = K_d = K$ et la clef K est gardée secrète par Alice et Bob. On dit que K est la **clef secrète** ;
2. systèmes à clef publique (ou asymétriques) : $K_e \neq K_d$, K_e est connue de tout le monde : c'est la **clef publique**, K_d n'est connue que du seul Bob : c'est la **clef privée**.

Exemples

1. Algorithmes à clef secrète : DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), AES (Advanced Encryption Standard) ;
2. Algorithmes à clef publique : RSA (Rivest Shamir Adleman), El-Gamal.

Types de menaces pesant sur la communication

1. Attaques passives ;
2. Attaques actives.

Attaques passives

Dans une attaque passive, Oscar se contente d'**écouter** (lire ou analyser le flux) les messages qui transitent sur le canal de communication. C'est une menace sur la confidentialité de l'information.

Attaques actives

Dans une attaque active, Oscar **modifie** le contenu des messages échangés. C'est une menace sur l'**intégrité** de l'information.

La cryptographie permet principalement de lutter contre ces menaces afin de protéger la **confidentialité de l'information**.

La cryptanalyse comprend toutes les techniques de mise en défaut des cryptosystèmes. Il existe plusieurs niveaux d'attaques possibles. Les niveaux représentent la "force" des attaques.

Niveaux d'attaques

1. Attaque à texte chiffré connu : Oscar connaît un certain nombre de textes chiffrés, tous chiffrés avec la même clef K_e, et il essaie de retrouver K_d (de sorte qu'il soit capable de déchiffrer les messages). C'est une attaque passive ;
2. Attaque à texte clair connu : Oscar connaît un certain nombre de couples textes clairs et chiffrés correspondants, tous chiffrés avec la même clef K_e. Il essaie de retrouver K_d. C'est une attaque passive.

Niveaux d'attaque (suite)

3. Attaque à texte clair choisi : Oscar a accès à une "boîte noire" : la machine de chiffrement pour une clef K_e donnée. Il choisit un certain nombre de messages clairs qu'il chiffre avec la boîte noire. À l'aide des textes clairs/chiffrés, il tente de deviner K_d. C'est une attaque active ;
4. Attaque à texte chiffré choisi : Oscar a cette fois accès à la "boîte noire" de déchiffrement. Il choisi des textes chiffrés qu'il déchiffre à l'aide de la boîte noire. Il essaie de retrouver K_d. C'est une attaque active.

Pour assurer la confidentialité

- Utilisation d'un algorithme de chiffrement ;
- Cela consiste à empêcher l'accès aux informations qui transitent à toute personne excepté les interlocuteurs légitimes (Alice et Bob).

Pour lutter contre l'usurpation d'identité

- Utilisation d'algorithmes d'authentification ;
- Alice s'identifie auprès de Bob en prouvant qu'elle connaît un secret (par ex., un mot de passe).

Lutter contre la répudiation

Utilisation d'algorithmes de signature.