Introduction à la cryptologie moderne

1 Les buts de la cryptologie moderne

Il s'agit dans cette fiche de faire un bref tour d'horizon de l'organisation de la cryptologie moderne. Evidemment ce tour d'horizon est loin d'être complet. Son intérêt est de faire comprendre les divers niveaux auquels se situent les éléments que nous développerons par la suite :

- **Les buts de la cryptologie moderne**
- **Les techniques cryptographiques permettant d'atteindre ces buts et qui sont les briques des protocoles cryptographiques**
- **Les primitives cryptographiques utilisées par les techniques cryptographiques**
- **Les objets et problèmes mathématiques sur lesquelles s'appuient les primitives cryptographiques**
- **Les protocoles qui sont les constructions complexes ultimes répondant à un ou plusieurs buts à atteindre**
- **Les standards** qui définissent exactement le fonctionnement des fonctions cryptographiques (primitives et protocoles), de manière à assurer la sécurité et l'interopérabilité des produits industriels cryptographiques.
- **les produits industriels** qui sont des réalisations concrètes des fonctions cryptographiques et qui s'appuient sur des standards reconnus.

À côté de la fonction de chiffrement, qui permet de préserver le secret des données lors d'une transmission, et qui a été utilisée depuis très longtemps, la cryptologie moderne a développé de nouveaux buts à atteindre et qu'on peut énumérer de manière non exhaustive :

- **confidentialité**
- **intégrité des données**
- **authentification des divers acteurs**
- **anonymat**
- **non-répudiation d'un contrat numérique**
- **signature numérique**
- **certification**
- **contôle d'accès**
- **gestion des clés**
- **preuve de connaissance**

La cryptologie a pour but d'assurer ou de compromettre ces principales fonctions de sécurité. Elle se partage en deux problématiques. D'une part la *cryptographie* qui construit les mécanismes aptes à assurer les fonctionnalités de sécurité précédentes. D'autre part la *cryptanalyse*, dont le but est d'analyser les faiblesses de ces constructions et de proposer des attaques.

2 Les techniques cryptographiques

Les techniques cryptographiques de base sont les techniques qui permettent de répondre aux fonctionnalités que nous avons décrites précédemment. On peut citer essentiellement :

- **Les techniques de chiffrement**
- **Les techniques de signature**
- **Les techniques de construction de clé**
- **Les techniques d'échange de clé**
- **Les techniques d'authentification**
- **Les techniques de contrôle d'intégrité**

Il faut introduire ici une distinction importante : les techniques qui relèvent de la *cryptographie à clé secrète* et celles qui relèvent de la *cryptographie à clé publique*. Par exemple le chiffrement des données et l'authentification de ces données sont principalement traités par la cryptographie à clé secrète. L'échange des clés et la signature sont principalement du domaine de la cryptographie à clé publique.
Ces techniques font appels à des *primitives cryptographiques* qui elles mêmes sont basées sur des *objets et problèmes mathématiques*.

2.1 Les objets mathématiques principaux

La cryptographie à clé secrète fait plutôt usage de :

- **Fonctions booléennes**
- **Générateurs de suites pseudo-aléatoires**
- **Tests statistiques**
- **Corps finis**
- **algèbre commutative, polynômes, bases de Gröbner**
- **Codes correcteurs d'erreurs**

La cryptographie à clé publique fait plutôt usage de :

- **Problème de la factorisation des entiers**
- **Problèmes liés à la résiduosité quadratique**
- **Fractions continues, réseaux arithmétiques**
- **Problème du logarithme discret dans des groupes arithmétiques**
- **Courbes elliptiques et courbes algébriques**
- **Codes correcteurs d'erreurs**

2.2 Les primitives cryptographiques

Les principales primitives cryptographiques nécessaires à la mise en œuvre des techniques cryptographiques sont les suivantes :

- **Les fonctions de hachage.** Elles assurent la transformation d'une suite d'octets en un bloc de taille fixe.
- **Les fonctions de "seeding" .** Elles permettent de générer un germe imprévisible, valeur initiale pour la construction d'une suite pseudo-aléatoire ou d'un générateur de masque (key derivation function KDF). Elles sont construites à partir de phénomènes physiques imprévisibles.
- **Fonctions de dérivation de clés (KDF).** On les appelle aussi générateurs de masques. Ce sont des générateurs pseudo-aléatoires destinés à produire des aléas courts (clés par exemples) contrairement à des générateurs pseudo-aléatoires destinés aux chiffrements à flots qui eux doivent produire très rapidement des suites longues. Elles sont souvent construites à partir d'une fonction de "seeding" et d'une fonction de hachage.
- **Fonctions de chiffrement à clé secrète (par bloc).** Elles comprennent deux volets : d'une part la primitive de base qui chiffre un bloc de données (en général 128 bits, ça peut être plus, mais il est déconseillé que ce soit moins), un mode d'utilisation qui définit comment on chiffre en pratique un message de taille quelconque et qui réalise en principe un chiffrement non déterministe (un même message chiffré deux fois ne donne pas le même chiffré). Le chiffrement à clé secrète est indispensable pour chiffrer des masses de données.
- **Fonctions de signature.** Compte tenu de l'évolution des tailles de clés, il est conseillé d'utiliser la cryptographie elliptique en remplacement de RSA ou DSA.
- **Fonctions d'échange de clé.** C'est une fonction importante qui permet d'échanger par de la cryptographie à clé publique une clé secrète d'un chiffrement à clé secrète.
- **Fonctions d'authentification de messages (MAC).** Elles sont appelées aussi fonctions de hachage à clé et servent à assurer l'intégrité des données et l'authentification de leur expéditeur ou de leur source auprès du destinataire (mais pas auprès d'un tiers).

À titre d'exemples citons pour la crypyographie à clé secrète par bloc AES, Twofish, pour les fonctions de hachage la gamme SHA2 (SHA224, SHA256, SHA384, SHA512) pour les MAC, le mode d'utilisation Galois Counter Mode (GCM) d'un chiffrement par bloc, HMAC. Pour la cryptographie à clé publique citons par exemple pour la signature numérique à clé publique RSA, DSA, ECDSA, pour les échanges de clé, échange de Diffie-Hellman DH (sur un groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$), ECDH (sur le groupe d'une courbe elliptique sur un corps fini, essentiellement $\mathbb{Z}/p\mathbb{Z}$), Psec-kem.

3 Les protocoles

Les protocoles sont des systèmes complexes construits en utilisant des techniques cryptographiques de base, qui définissent les modalités d'échanges de données entre divers participants et qui sont aptes à assurer une sécurité globale. Citons par exemple SSH pour l'accès sécurisé à des machines distantes, ou encore kerberos pour l'accès à des informations sur différents serveurs ou encore station to station protocol pour gérer par exemple des communications téléphoniques chiffrées, SSL/TLS qui fournit une infrastructure de gestion de clés et qui sert dans diverses applications : signature numérique certifiée, serveurs sécurisés etc, IPSec pour chiffrer les paquets IP du protocole TCP/IP etc. Plusieurs de ces protocoles peuvent se concurrencer pour certaines applications, ce qui laisse un choix aux concepteurs de sytèmes.

4 Cryptanalyse

La partie cryptanalyse étudie comment compromettre la sécurité des systèmes. Elle s'attaque aux divers composants : primitives, protocoles, implémentations. Il est à remarquer que les attaques réussies portent le plus souvent sur l'implémentation des systèmes et que ce sont des fautes d'implémentation qui engendrent la plupart des trous de sécurité.
Actuellement les attaques peuvent être classées en au moins deux grandes familles :

1. Les attaques directes qui s'en prennent directement à des failles calculatoires : on arrive à trouver un algorithme d'attaque faisable en pratique (sous certaines hypothèses sur ce qu'est capable de faire un attaquant) qui a une probabilité de succès notablement plus grande que le "tirage au sort" de la solution.
2. Les attaques physiques qui s'en prennent directement au composant pour lui "soutirer" des informations importantes. On compte parmi ces attaques :
   (a) les attaques qui analysent divers facteurs comme le temps d'exécution, le courant consommé, le rayonnement électromagnétique ;
   (b) les attaques qui font faire des fautes aux composants de manière bien choisie (utilisation d'un laser par exemple).

Rappelons enfin un principe important, qui hélas peut être en contradiction avec des intérêts commerciaux : un système cryptographique fiable doit être complètement ouvert (y compris les sources, puisque dans la plupart des affaires de cassage c'est l'implémentation qui est fautive) ; autrement dit un système propriétaire fermé est hautement suspect.