La cryptographie

Table des matières

La cryptographie, c’est quoi ?

Définition :

Ensemble des techniques de chiffrement qui assurent l'inviolabilité de textes et, en informatique, de données. (source : larousse.fr)

En clair, on pourrait résumer la cryptographie au fait de coder des messages afin de les rendre lisibles uniquement par les personnes possédants la clé pour les déchiffrer. Il existe deux grandes familles dans la cryptographie : le **chiffrement symétrique** et le **chiffrement asymétrique.**

Utilisation :

La cryptographie est aujourd'hui principalement utilisée pour sécuriser les données informatiques dans tout type d'échanges : transfert d'argent, messagerie instantanée, appels téléphoniques, cryptomonnaies, etc..

Pourtant, cet outil qu'est la cryptographie ne date pas d'hier. Les premières traces remontent à l'Egypte ancienne en -2000 avant J.-C mais l'exemple le plus connu se passe en -54 avant JC. Il s'agirait d'un messager envoyé par César pour prévenir l'arrivée de renfort dans un camp romain assiégé. Ce message était cependant codé. En effet le message était illisible si l'on ne connaissait pas la clé de déchiffrement. Toutes les lettres ayant été déplacées de 3 crans : CESAR devenait alors FHVDU. Par ce biais, même si le message était intercepté, les gaullois n'auraient pas étaient en mesure de pouvoir comprendre ce qui se passait. C'est ainsi qu'est né le chiffrement de CESAR encore utilisé aujourd'hui bien qu'il soit très vulnérable.

Le chiffrement symétrique

Qu'est-ce que c'est ?

Le chiffrement symétrique repose sur le fait qu'une seule clé de chiffrement sera utilisée pour crypter le message, mais également pour le décrypter.

Exemples :

- Vers -400 avant JC, les spartiates utilisaient un outil utilisé scytale qui servait à codait leurs messages. Le principe était simple, ils enroulaient un bandeau où ils inscrivaient des lettres autour d'un baton d'un certain diamètre afin de coder un message. La clé de chiffrement était alors le diamètre du baton utilisé.
- Le chiffrement de CESAR en -54 avant JC. (voir utilisation de cryptographie au dessus)

Avantages

Le principale avantage du chiffrement symétrique est d’être le plus rapide à coder et à décoder. Les algorythmes à mettre en place pour ce chiffrement sont beaucoup moins complexes. Du fait de ces algorythmes moins complexes, moins de ressources (ordinateur) sont nécessaires pour pouvoir utiliser ce chiffrement.

Inconvéniants

Le principal inconvéniant repose sur le fait que la clé de déchiffrement doit absolument restée secrète. De plus, étant donné que les algorythmes sont moins complexes, il est alors plus facile de les « craquer ».

Le chiffrement asymétrique

Qu’est-ce que c’est ?

(Source : venafi.com)

Également connue sous le terme de chiffrement asymétrique, la cryptographie à clé publique sert de moyen d'assurer la confidentialité, l'authenticité et la non-répudiation des communications et du stockage de données électroniques. Le chiffrement à clé publique emploie deux clés simultanément, une combinaison d'une clé privée et d'une clé publique. La clé privée doit rester connue uniquement par son propriétaire respectif, tandis que la clé publique est mise à disposition de tous sur une base de données ou un annuaire publiquement accessible. Pour décoder un message chiffré, un ordinateur doit utiliser la clé publique fournie par l'ordinateur expéditeur ainsi que sa propre clé privée. Bien que l'envoi d'un message d'un ordinateur à un autre ne soit pas sécurisé, car la clé publique employée pour le chiffrement est publiée et à la disposition de tous, personne ne peut le lire sans disposer de la clé privée.

La paire de clés se base sur de très longs chiffres premiers. La clé publique et la clé privée sont calculées ensemble simultanément au cours d'un même calcul mathématique faisant appel à des fonctions « à trappe ». La principale caractéristique de ce type de fonctions réside dans le fait qu'elles sont très simples à calculer dans un sens, mais difficiles à calculer dans l'autre (en trouvant leur inverse) en l'absence d'informations spécifiques.

Avantages

Comme dit précédemment, le principal avantage réside dans le fait que le chiffrement s’effectue facilement dans un sens mais très difficilement dans l’autre si l’on ne connaît pas la clé privée qui a été utilisée avec clé publique pour chiffer le message.

Inconvéniants

Contrairement au chiffrement symétrique, la puissance de calcul demandée est très importante et demande beaucoup de ressources pour l’exécuter.

La signature électronique

Définition :

(source: futura-sciences.com)

Signature reposant sur un système de chiffrement à clé publique et clé privée permettant d'authentifier l'émetteur d'un document. La clé privée sert à signer, la clé publique sert à vérifier cette signature. La signature électronique est l'équivalent numérique de la signature manuscrite.

Utilisation :

Cette signature repose sur le chiffrement asymétrique. Il est principalement utilisé dans les domaines de la banque, de l’assurance et de la finance.

Les types de signature électronique

Signature électronique simple : elle comporte de faibles conséquences financières pour le signataire (ex : adhésion, contrat de travail, etc.)

Signature électronique avancée : obligation d'utiliser un certificat numérique (SSL) ainsi qu'un système de reconnaissance d'identité avancé. Par ce biais, il est également assuré que le document n'a pas été modifié après signature. (ex : contrats de crédit, compromis de ventes immobilières, etc.)

Signature électronique qualifiée : Au niveau juridique, elle a la même valeur qu'une signature manuscrite. Cependant, elle ne peut être entièrement réalisée à distance. Elle est donc très contraignante de par ce fait. Elle est principalement utilisée pour des actes d'huissiers, de notaires, etc.

Cas exceptionnels

Il est formellement interdit d'utiliser une signature numérique sur tout document se rattachant au droit de la famille (convention de Pacs, droit de succession, caution d'un bail de location par un membre de la famille.).

Obligations :

Il est obligatoire qu'à travers cette signature numérique, il soit possible d'identifier le signataire, impossible de modifier un document signé, etc.

Certificats

Définition :

(Source : lemagit.fr)

Un certificat numérique est une sorte de passeport électronique qui permet à une personne, un ordinateur ou une organisation d'échanger de manière sûre des informations sur Internet en s'appuyant sur une infrastructure à clé publique (PKI).

A l'instar d'un passeport, un certificat numérique fournit des informations d'identité, se veut résistant aux tentatives de réalisation de faux, et peut être vérifié parce qu'il est émis par une agence officielle, de confiance. Le certificat contient le nom de son porteur, un numéro de série, des dates de validité, une copie de clé publique de son porteur – utilisée pour chiffrer des messages et produire des signatures électroniques – et la signature électronique de l'autorité qui l'a émis (CA) afin de permettre au destinataire d'en vérifier l'authenticité.

Pour prouver son authenticité et sa validité, un certificat est signé numériquement par un certificat racine appartenant à une autorité de certification de confiance. Les systèmes d'exploitation et les navigateurs Web tiennent à jour des listes de certificats racines afin de pouvoir vérifier aisément les certificats émis et signés par les autorités de certification. Dans le cadre d'un déploiement interne de PKI, les certificats peuvent être auto-signés.