Glossaire

La cryptologie en 10 mots clés

Authentification
Action de s'assurer de l'identité d'une entité donnée ou de l'origine d'une communication ou d'un fichier.

Clé
Information nécessaire à l'émetteur et au destinataire pour envoyer ou recevoir un message ou des données confidentielles, ou pour s'authentifier.

Cryptanalyse
Consiste à tenter d'attaquer un système cryptographique, notamment pour en étudier le niveau de sécurité effectif.

Cryptographie
Conception de mécanismes cryptologiques destinés à garantir les notions de sécurité à des fins de confidentialité, d'authenticité et d'intégrité de l'information, mais aussi pour d'autres notions comme l'anonymat.

Cryptographie asymétrique (clé publique)
Les algorithmes sont publics, mais chaque individu possède un couple de clés : l'une secrète lui permettant d'effectuer les opérations que lui seul est sensé être en mesure de faire (signature ou déchiffrement), tandis que sa clé publique est diffusée afin de permettre à ses interlocuteurs de mettre en œuvre les opérations réciproques (vérification de signature ou chiffrement de message). Les deux clés ont un rôle « asymétrique », d'où la terminologie.

Cryptographie symétrique (clé secrète)
Les algorithmes sont publics, mais une information secrète commune à l'émetteur et au destinataire permet leur usage entre plusieurs personnes. On dit « symétrique » car émetteur et destinataire ont le même niveau d'information.

Cryptologie

Du grec *kryptos* (caché) et *logos* (science), « cryptologie » signifie littéralement science du secret et a pour objet de cacher les informations d'un message. Son but est triple : assurer la confidentialité, garantir l'authenticité et conserver l'intégrité des informations. Cette science, née il y a plusieurs millénaires mais organisée en discipline depuis quelques décennies seulement, comprend principalement deux champs d'étude, la cryptographie et la cryptanalyse.

Preuve de sécurité

Méthodologie qui complète la cryptanalyse par des preuves mathématiques d'absence de failles.

RSA

Du nom de ses inventeurs Ron Rivest, Adi Shamir et Leonard Adleman, premier algorithme qui utilise le principe de clé publique.

Signature numérique

Service d'authenticité, ayant une valeur juridique depuis la loi du 20 mars 2000, et qui permet de s'assurer de l'identité d'une entité donnée ou l'origine d'une communication ou d'un fichier.