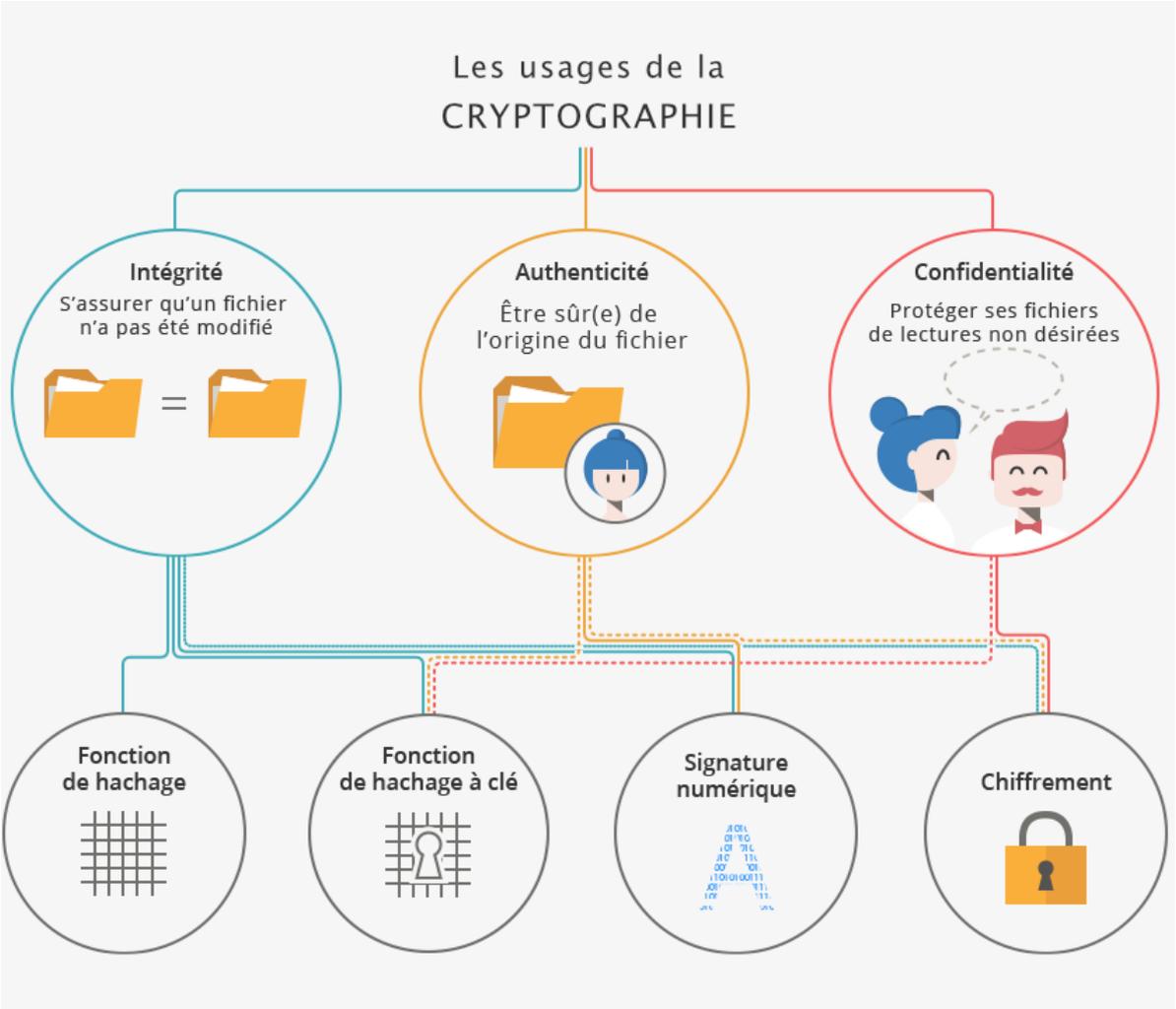


Source : <https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement>



Une « **fonction de hachage** » permettra d'associer à un message, à un fichier ou à un répertoire, une empreinte unique calculable et vérifiable par tous. Cette empreinte est souvent matérialisée par une longue suite de chiffres et de lettres précédées du nom de l'algorithme utilisé, par exemple « SHA2 » ou « SHA256 ».

INTÉGRITÉ

Comment fonctionnent les fonctions de HACHAGE et de HACHAGE À CLÉ ?

FONCTION DE HACHAGE
Une fonction de hachage calcule l'empreinte du document (message, fichier, répertoire) qui lui est passé.
Cette empreinte est une sorte d'identifiant unique du document généré à un moment précis.

FONCTION DE HACHAGE À CLÉ
Les fonctions de hachage à clé sont similaires aux fonctions de hachage, à l'exception du fait qu'une clé secrète est utilisée pour calculer l'empreinte du document.
Un même document peut donc avoir plusieurs empreintes différentes en fonction de la clé secrète utilisée pour les calculer.

MISE EN PRATIQUE

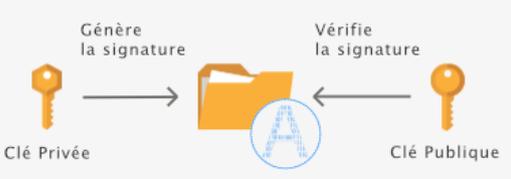
Alice veut charger un de ses fichiers sur le cloud et veut être sûre que son fichier n'a pas été altéré lors du transfert.

1. Elle va d'abord calculer l'empreinte du fichier sur son ordinateur.
2. Une fois cela fait, elle charge son fichier sur le cloud.
3. Le fichier chargé, elle calcule alors l'empreinte du fichier transféré.
4. Alice compare les deux fichiers pour savoir si une modification involontaire a eu lieu ou non.

La « **signature** » - numérique - permet de vérifier qu'un message a bien été envoyé par le détenteur d'une « clé publique ». Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus d'assurer que celui-ci n'a pas été modifié.

AUTHENTICITÉ

Comment fonctionnent les SIGNATURES NUMÉRIQUES ?



SIGNATURE NUMÉRIQUE

Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus d'assurer que celui-ci n'a pas été modifié.

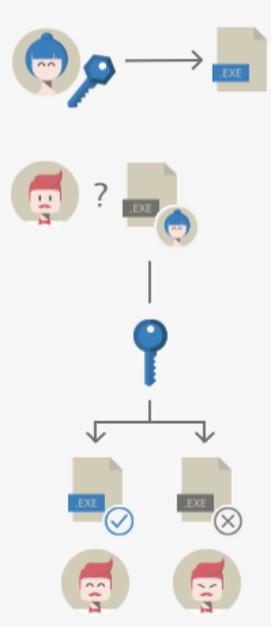
Le procédé repose sur un couple de clés : l'une est privée et connue uniquement de son détenteur, l'autre est publique et accessible à tous.

La signature est générée en utilisant la clé privée. La clé publique est utilisée pour vérifier cette signature. Cette vérification peut donc être effectuée par n'importe quelle personne ayant accès à la clé publique.

MISE EN PRATIQUE

Alice vient de publier un nouveau logiciel et souhaite assurer à ses futurs utilisateurs l'authenticité des copies qu'ils obtiennent.

1. Avant de publier librement son logiciel, Alice prend soin de le signer.
2. Bob vient de télécharger une copie du logiciel mais il veut s'assurer que cette copie provient bien d'Alice.
3. Bob utilise la clé publique d'Alice pour vérifier la signature de la copie.
4. Si la clé reconnaît la signature, alors c'est une bonne copie ! Dans le cas contraire, Bob préfère ne pas prendre de risques. Il supprimera la copie.



Le **chiffrement** d'un message permet de garantir que seuls l'émetteur et le(s) destinataire(s) légitime(s) d'un message en connaissent le contenu. C'est une sorte d'enveloppe scellée numérique. Une fois chiffré, faute d'avoir la clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines.

CONFIDENTIALITÉ Comment fonctionne le CHIFFREMENT ?

Clé Secrète

CHIFFREMENT SYMÉTRIQUE

Le chiffrement symétrique permet de chiffrer et déchiffrer un fichier avec la même clé, dite secrète. Pour s'échanger un message il faut donc que les deux parties partagent la même clé.

MISE EN PRATIQUE

Alice vient d'enregistrer la liste des cadeaux de Noël de sa famille sur l'ordinateur familial. Elle souhaite être la seule à pouvoir y accéder.

1. Pour ce faire, Alice chiffre la liste en utilisant sa clé secrète.
2. Plus tard dans la journée, Bob trouve la liste et cherche à l'ouvrir.
3. Malheureusement pour lui, Bob est incapable de lire la liste car il ne possède pas la clé secrète.
4. La liste est donc bien protégée. Seule Alice peut réussir à la déchiffrer et la lire !

Clé publique Clé privée

CHIFFREMENT ASYMÉTRIQUE

Le chiffrement asymétrique repose sur l'utilisation d'une paire de clés : une publique et une privée.

La clé publique, accessible à tous, est utilisée pour chiffrer les fichiers. Seule la clé privée permet de déchiffrer ces fichiers, celle-ci étant connue que d'un seul individu.

MISE EN PRATIQUE

Alice, hackeuse, vient de découvrir des informations d'intérêt public. Elle veut les transmettre à Bob, journaliste, pour qu'il enquête.

1. Alice vient de récupérer la clé publique de Bob. Elle l'utilise pour chiffrer son document.
2. Elle l'envoie à Bob.
3. Bob reçoit le document et le déchiffre à l'aide de sa clé privée.
4. Une fois le document déchiffré, il rédige un article puis le publie dans son journal.