Objectifs

La cryptographie est généralement utilisée pour sécuriser les informations.
On recherche en particulier les propriétés suivantes :

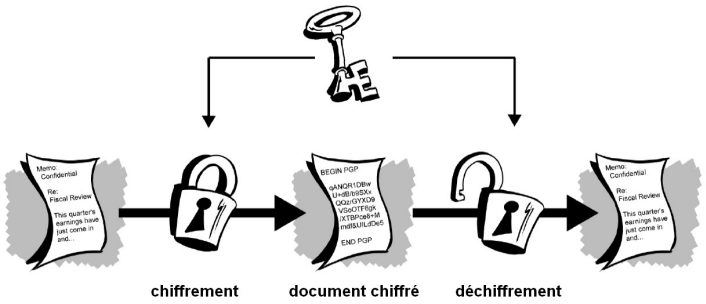
1. Confidentialité (ou secret) : seul le destinataire doit être capable de déchiffrer les messages. Il ne doit pas être possible à une autre personne d'obtenir des informations significatives à partir de ce qu'elle observe.
2. Intégrité : le destinataire doit être capable de déterminer si le message a été modifié [durant sa transmission].
3. Authentification : le destinataire doit être capable d'identifier l'expéditeur du message et de vérifier qu'il en est bien l'auteur.
4. Non-répudiation : en conséquence des points 2. et 3., l'expéditeur ne peut nier être l'auteur du message.
5. Non-rejouabilité (anti-replay) : le message ne peut-être envoyé plusieurs fois sans que le destinataire ne puisse le distinguer.
6. Preuve de délivrance : l'expéditeur doit avoir moyen de prouver que le destinataire à bien reçu le message.

La cryptographie fournie des mécanismes pour atteindre tous ces objectifs. Cependant, certains ne sont pas toujours nécessaires, pratiques ou même souhaitable dans certains contextes. Par exemple, un expéditeur peut vouloir rester anonyme.

Cryptographie symétrique (à clé secrète)

La clé secrète est l'information devant permettre de chiffrer et de déchiffrer un message et à laquelle doit se réduire la sécurité de la communication. Il s'agit généralement d'un fragment binaire de longueur fixe, sans signification mathématique, produit à partir d'une phrase ou mot de passe.

En conséquence un même secret est partagé par l'émetteur et le destinataire du message. Le principal inconvénient réside dans la difficulté de stocker et distribuer les clés de manière fiables.

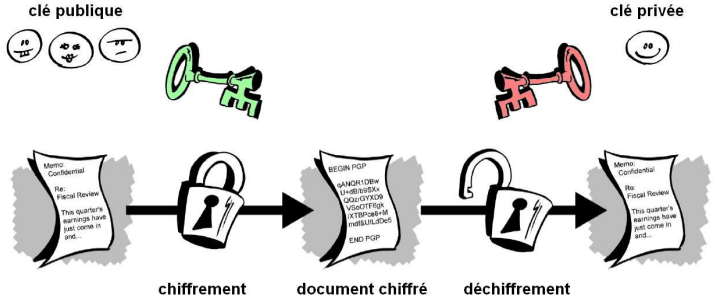


exemple : AES, Cast, Idea, Blowfish

Cryptographie asymétrique (à clé publique)

La cryptographie à clé publique ou asymétrique, est un système qui permet de communiquer en toute sécurité sans avoir besoin d'échanger au préalable une clé secrète. Ceci est réalisé grâce à une paire de clés, dont l'une est gardée secrète et l'autre diffusée publiquement. La relation (mathématique) qui les lie ne permet pas de déduire l'une à partir de l'autre.

Le chiffrement est réalisé en utilisant la clé publique du destinataire.
Seul le détenteur de la clé privée correspondante pourra déchiffrer le message.

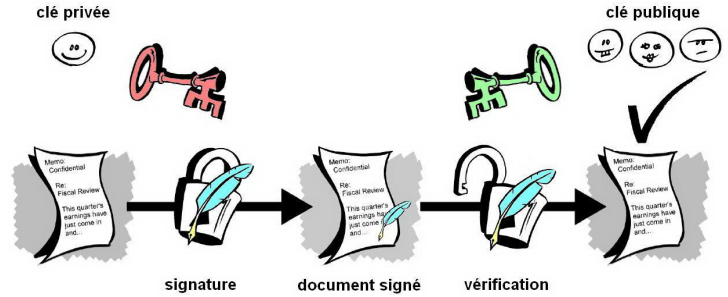


exemple : RSA, ElGamal

Signature numérique

Un des avantages majeurs de la cryptographie à clé publique est qu'elle procure au destinataire le moyen de contrôler l'origine d'un message, et également de vérifier que son contenu n'a pas été altéré. Ainsi, elle empêche l'expéditeur de contester ultérieurement avoir bien émis cette information.
Ces éléments sont au moins aussi importants que le chiffrement des données, sinon davantage.

La signature est produite en utilisant la clé privée, et vérifiable par tout-un-chacun au moyen de la clé publique.



En pratique, et afin d'éviter que la signature ne soit aussi volumineuse que le document original, elle est calculée à partir d'une empreinte de ce dernier.

Empreinte (condensé)

Il est possible de 'résumer' ou de 'caractériser' des données au moyen de fonctions dites de 'hachage'. Pour ce faire, on convertit un grand ensemble (de taille variable) en un plus petit (de taille fixe), appelé 'empreinte'.

document **empreinte (condensé)**

Dans un contexte cryptographique, il faut en particulier :

- ne rien permettre de connaître du message à partir de son empreinte,
- résister aux collisions, c'est-à-dire trouver deux messages distincts qui produiraient le même condensé
  (de par sa nature, tout algorithme de hachage génère des collisions),
- rendre très difficile la génération d'un message différent à partir d'une empreinte et d'un message donné

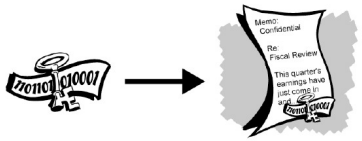
De par leur nature 'irréversible', les condensés sont souvent impliqués dans les stratégies de stockage des mots de passe. Pour identifier un utilisateur, il suffit de comparer l'empreinte du mot de passe d'origine (stocké) avec l'empreinte du mot de passe demandé. Le mot de passe n'est jamais stocké.

La plupart des algorithmes de hachage sont aussi d'excellents générateurs de valeurs pseudo-aléatoires. A ce titre ils interviennent dans la génération de clés secrètes à partir de phrases ou mots de passe.

exemple : SHA, RipeMD

Authentification de message

Lorsque la confidentialité d'un message n'est pas requise, il est néanmoins parfois utile de s'assurer qu'il ne puisse être modifié.
En protégeant son empreinte par une clé secrète, on produit un 'code d'authentification de message' qui protège contre toute altération extérieure (au groupe qui partage la clé).



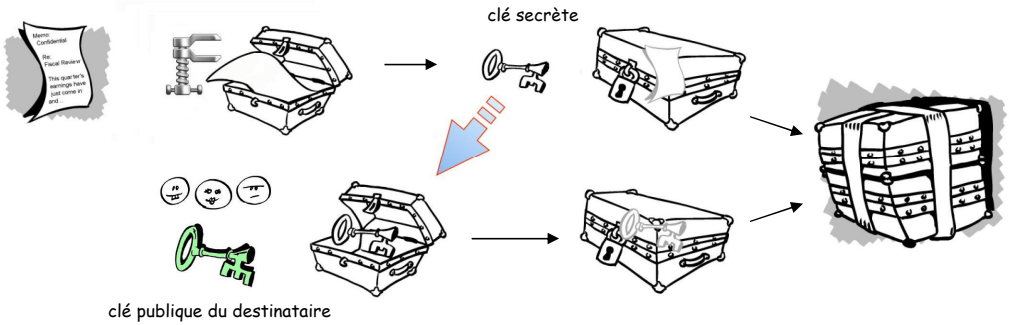
Toutefois, il ne s'agit pas de signature, car quiconque peut vérifier le message peut aussi produire le code de protection.

Cryptographie hybride – principe général

La cryptographie asymétrique est intrinsèquement lente à cause des calculs complexes qui sont nécessaires alors que la cryptographie symétrique est beaucoup plus rapide (environ 1000 fois).
Utilisés conjointement, la performance et la distribution de la clé sont améliorées sans aucun sacrifice sur la sécurité.

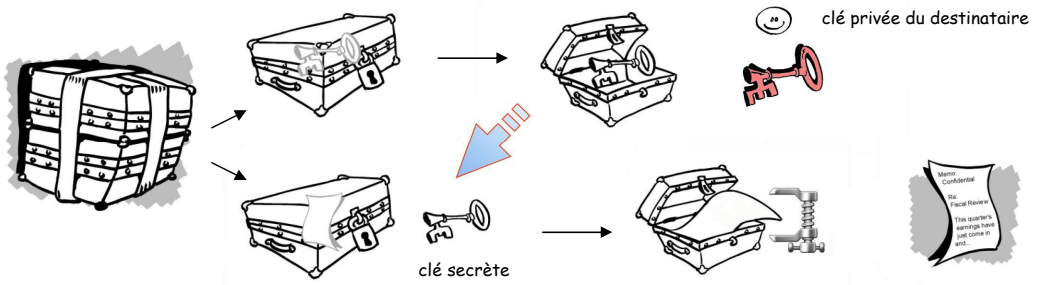
chiffrement :

1. compression des données : outre la diminution de taille, diminue la redondance du document original et augmente la résistance à la cryptanalyse
2. génération d'une clé de session (symétrique)
3. chiffrement du document avec la clé de session
4. chiffrement de la clé de session avec la clé publique du destinataire
5. transmission au destinataire de l'ensemble : document crypté + clé de session cryptée + ...



déchiffrement :

1. utilisation de la clé privée pour décrypter la clé de session (symétrique)
2. décryptage du document avec la clé secrète
3. décompression du document



Chiffrement et Signature :

On peut bien sur chiffrer et signer à la fois. Reste à définir dans quel ordre. En application du principe général 'Only What is Seen Should be Signed' (ne doivent être signés que des données intelligibles), on signe d'abord et on chiffre ensuite, mais il existe des situations et des protocoles ou il est préférable d'agir autrement.

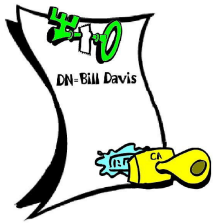
Certificat :

Un problème, avec les cryptosystèmes à clés publiques, est que les utilisateurs doivent être constamment vigilants pour s'assurer qu'ils chiffrent leurs messages en utilisant la véritable clé du destinataire. Dans un environnement où l'on peut échanger des clés à travers des serveurs publics, les attaques utilisant une personne interposée sont un danger potentiel. Dans ce type d'attaque, un imposteur fournit une clé bidon portant le nom et l'identifiant d'utilisateur du destinataire réel des messages de l'utilisateur. Les données chiffrées pour – et interceptées par – le vrai propriétaire de cette fausse clé, seront tombées en de mauvaises mains.

On pourrait imaginer se limiter à utiliser les clés publiques remises physiquement, de la main à la main, par leur propriétaire. Mais la plupart du temps, on doit échanger des informations avec des gens qu'on n'a jamais rencontrés.

Une manière d'établir la validité d'une clé est de faire confiance à quelqu'un d'autre, qui aura lui-même effectué le processus de vérification.

Un certificat numérique est un document qui permet de s'assurer qu'une clé publique appartient bien à une personne ou une entité nommément désignée.



Il contient notamment les parties suivantes :

- la clé publique objet du certificat,
- des informations identifiant clairement le propriétaire de la clé, telles que son nom, son adresse électronique, ses coordonnées, …
- et enfin la signature numérique des données ci-dessus par la personne ou l'organisation qui atteste de leur véracité.

Dans le modèle hiérarchique X.509, une Autorité de Certification (A.C.), est tenue de s'assurer soigneusement qu'une clé appartient bien à son propriétaire supposé, avant d'apposer sa signature sur un certificat.
Quiconque a confiance en l'A.C. considérera automatiquement comme valides tous les certificats signés par cette A.C.

> Avoir confiance en une clé (être absolument sûr que la clé appartient réellement à une personne) n'est pas la même chose que d'avoir confiance dans le propriétaire de la clé.

Considérations sur la sécurité et la vulnérabilité

La cryptographie peut être forte ou faible.
La force de la cryptographie est mesurée par le temps et les ressources qui seraient nécessaires pour retrouver le texte clair.

La sécurité des données chiffrées est entièrement dépendante de deux choses : la force de l'algorithme cryptographique et le secret de la clé.

Pas de réelle protection [du message] sans vigilance, rigueur et secret.

- Les techniques cryptographiques ne protègent les données que lorsqu'elles sont chiffrées – une violation directe de la sécurité physique peut encore compromettre les données en clair ou les informations écrites ou orales.
(si on sait que vous possédez le secret, il est plus facile de faire pression sur vous, voire d'attenter à vous)
- Analyse de trafic : pour l'attaquant, c'est comme examiner votre facture de téléphone pour voir qui vous appelez, quand et pour combien de temps, quand bien même le contenu actuel des appels lui demeure inconnu.
- Attaques 'Tempest' : la détection à distance des signaux électromagnétiques émis par l'ordinateur. Cette coûteuse et parfois laborieuse attaque est probablement toujours moins coûteuse que l'attaque cryptanalytique directe.

http://www.schneier.com

« Security is a chain; it's only as strong as the weakest link. The security of any CA-based system is based on many links and they're not all cryptographic. People are involved ».

Les clés plus longues ne signifient pas toujours plus de sécurité.
Comparez l'algorithme cryptographique au verrou de votre porte d'entrée. […] Des cambrioleurs n'essayent pas toutes les clés (attaque systématique); la plupart ne sont pas assez intelligents pour crocheter la serrure (attaque cryptographique contre l'algorithme). Ils fracassent les fenêtres, donnent des coups de pieds dans les portes, se déguisent en policiers, ou bien dévalisent les détenteurs de clés avec une arme. Un groupe de voleurs en Californie mettait en défaut les systèmes de sécurité en attaquant les murs à la tronçonneuse. Contre ces attaques, de meilleures serrures ne sont d'aucun secours.

> La cryptographie forte est très puissante quand elle est bien faite, mais ce n'est pas une panacée. Se focaliser sur les algorithmes cryptologiques tout en ignorant les autres aspects de la sécurité revient à défendre votre maison, non pas en dressant une barrière autour, mais en plantant un seul immense poteau devant en espérant que votre adversaire va juste s'y heurter. Les attaquants intelligents se contentent de contourner les algorithmes.
> […]

Nous n'avons pas à essayer toutes les clés possibles, ni même à trouver une faille dans les algorithmes; nous exploitons les erreurs de conceptions, les erreurs de réalisations, et les erreurs d'installations. […] les vieilles fautes classiques qui se répètent indéfiniment. […]

> Un système cryptologique ne peut pas être plus solide que les éléments sur lesquels il repose. De la même façon qu'il est possible de construire une structure faible avec de solides matériaux, il reste possible de construire un système cryptologique faible en utilisant des algorithmes et des protocoles forts. Nous trouvons souvent des systèmes qui "annulent la garantie" de leur cryptologie en ne l'utilisant pas correctement

[…]
Beaucoup de systèmes font défaut suite à des erreurs de réalisation. Quelques systèmes ne garantissent pas que le texte clairement lisible soit détruit après avoir été chiffré.

[…]
Beaucoup de systèmes sont cassés car ils reposent sur des mots de passe choisis par l'utilisateur. Laissés à eux-mêmes les utilisateurs ne choisissent pas des mots de passe forts. Et s'ils sont forcés de le faire, ils ne peuvent s'en souvenir. Beaucoup des attaques les plus intéressantes visent le modèle sous-jacent de la confiance dans le système : à qui ou à quoi fait-on confiance, de quelle façon, et à quel degré ? […] Souvent, un système sera conçu pour un modèle de confiance, et implanté avec un autre.

[…]
Beaucoup de systèmes logiciels font de mauvaises hypothèses quant à la confiance à accorder aux ordinateurs sur lesquels ils tournent; Ces programmes peuvent souvent être cassés par des vers qui reniflent les mots de passe, lisent les textes clairs, ou contournent de toute autre façon les mesures de sécurité.

[…]
Même quand un système est sécurisé sous réserve d'une utilisation correcte, ses utilisateurs peuvent mettre en danger la sécurité par accident ou négligence. L'exemple le plus classique en est l'utilisateur qui donne son mot de passe à ses collègues pour qu'ils dépannent des problèmes en son absence.

[…]
Cela ne prend que quelques jours pour reconstituer par rétro-analyse l'algorithme à partir du code exécutable. Le système pour les disques DVD prenait un algorithme faible et le rendait encore plus faible…