Numérique et sciences informatiques

Lycée Hoche

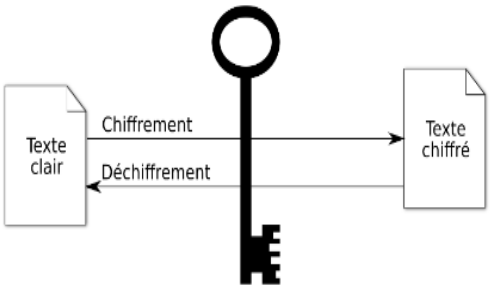
année scolaire 2025-2026

Contents

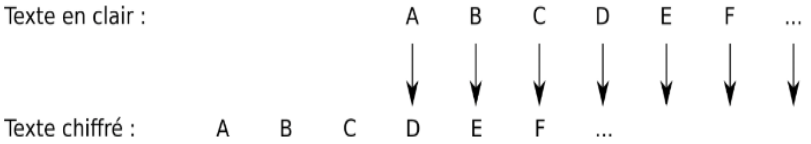
1 chiffrement symétrique

1.1 Les principes de chiffrement symétrique

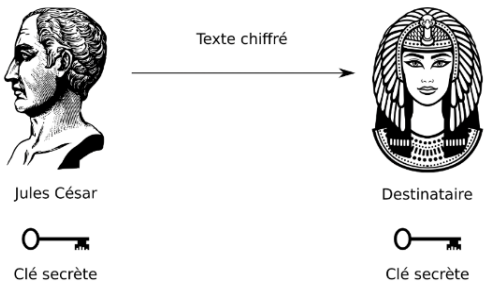
Le chiffrement symétrique, ou à clef partagée, permet de chiffrer et de déchiffrer des messages à l'aide d'une même clef. Cette clef doit donc être partagée par l'expéditeur et son destinataire tout en n'étant connue que par eux.



L'exemple le plus connu de chiffrement symétrique, et un des plus simples, est le chiffre de César. Cette méthode de communication chiffrée aurait été inventée par Jules César lui-même. Pour obtenir le texte chiffré, le chiffre de César consiste à remplacer chaque lettre du texte en clair par la lettre obtenue après un décalage d'un nombre fixe de lettres dans l'alphabet. Pour un décalage de 3 lettres, le A devient D, le B devient E... Comme le montre l'image



Le nombre 3, qui correspond au nombre de lettres à décaler, est appelé la clef secrète de chiffrement. Pour déchiffrer le message, il suffit de donner la clef de chiffrement au destinataire du message qui réalise l'opération inverse pour déchiffrer le message.



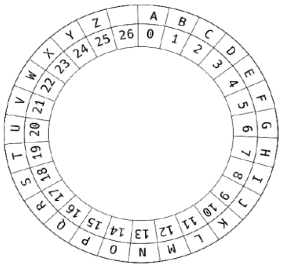
Jules César et son destinataire utilisent la même clef de chiffrement et elle n'est connue que par eux. Ce chiffrement est donc symétrique et cette clef est la clef partagée.

Fonction Python qui déchiffre un message encodé par le chiffrement de César avec un décalage de n caractères :

1.2 le chiffrement de Vernam

Le chiffrement symétrique dit de Vernam utilise comme clef partagée une chaîne de caractères aussi longue que le message à chiffrer. L'algorithme consiste alors à :

1. faire correspondre chaque lettre du message à chiffrer avec chaque lettre de la clef partagée ;
2. convertir chaque lettre en nombre. Par exemple : 0 pour A, 1 pour B, 2 pour C... Le caractère « espace » est aussi codé par le nombre 26. Les décalages sont alors modulo 27 : la lettre est codée par le reste de la division euclidienne par 27.
3. Il est aussi possible d'utiliser le codage ASCII pour convertir chaque lettre en nombre : 65 pour A, 66 pour B... ;
4. décaler dans l'alphabet chaque lettre du message à chiffrer. Ce décalage est égal au nombre correspondant à la lettre qui a la même position dans la clef partagée. Cela revient à effectuer un chiffrement de César avec un décalage différent pour chaque lettre du message à chiffrer.



En utilisant le codage de l'illustration, le texte :

L	A		T	E	R	R	E		E	S	T		R	O	N	D	E

chiffré avec la clef :

Q	W	R	B	O	K	L	E	P	Y	C	F	O	R	A	H	Z	Q

devient :

A	W	Q	U	S	A	B	I	O	B	U	Y	N	H	O	U	B	U

Prenons l'exemple de la lettre S à chiffrer. Sa lettre correspondante dans la clef est C. Ceci occasionne un décalage de 2 dans l'alphabet et donc la lettre S devient U.

1.3 Le chiffrement AES

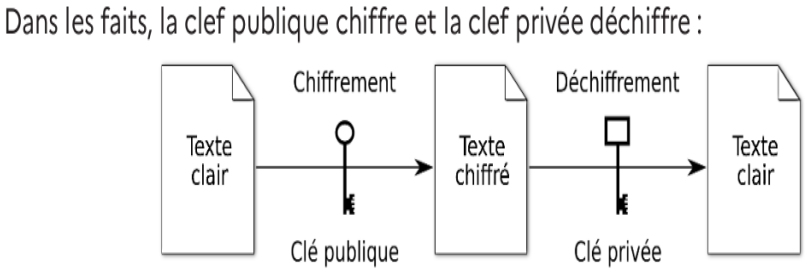
Le chiffrement AES (Advanced Encryption Standard) est un des algorithmes les plus utilisés actuellement et il est à l'heure actuelle considéré comme sûr. Dans les utilisations les plus fréquentes de l'AES, on peut citer :

- le chiffrement des données lors de l'ajout d'un mot de passe à un fichier PDF ou ZIP ;
- la sécurisation des connexions via l'utilisation de VPN ;
- la sécurisation des données utilisateurs lors de l'utilisation d'outils de gestion de mots de passe ;
- la protection de serveurs multi-joueurs contre les attaques. C'est le cas par exemple de l'entreprise Rockstar, développeur et éditeur de la série des Grand Theft Auto (GTA) ;
- le chiffrement des communications lors de l'utilisation de messageries instantanées. C'est le cas de l'application WhatsApp. Ce chiffrement symétrique utilise une clef de 128, 192 ou 256 bits et elle est utilisée pour paramétrer une suite de transformations qui permettent de chiffrer ou de déchiffrer le message.

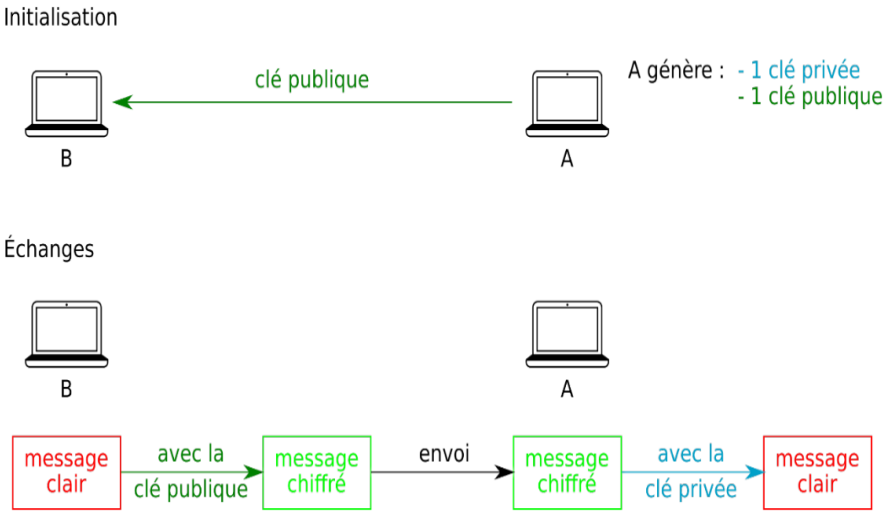
2 Les principes du chiffrement asymétrique

Dans le cas du chiffrement symétrique, la clef est partagée. Elle est alors commune à l'émetteur et au récepteur du message chiffré. Le chiffrement est symétrique, car une unique clef permet à la fois de chiffrer et de déchiffrer le message.

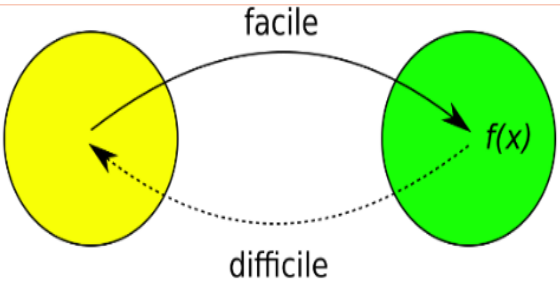
Pour le chiffrement asymétrique, la clef est en fait un couple de clefs, appelées **clef privée** et **clef publique**. Chaque clef peut être utilisée pour chiffrer un message, mais il n'est alors déchiffrable qu'avec l'autre clef du couple.



Plus précisément, dans une communication, lorsqu'on chiffre un message avec un algorithme asymétrique, on utilise la clef publique du destinataire. Le message ou les données ne sont alors déchiffrables que par la personne qui possède l'autre clef du couple, normalement la clef privée du destinataire. Contrairement à la clef publique, la clef privée n'est jamais diffusée.



Le chiffrement asymétrique repose sur des fonctions mathématiques à **sens unique**. En effet, une fois qu'elles ont été appliquées, il est très difficile de les inverser sans connaître l'information contenue dans la clef de déchiffrement.



Les chiffrements asymétriques sont plus coûteux en temps de traitement que les chiffrements symétriques, et à niveau de sécurité équivalent, les clefs sont généralement plus longues que les clefs des algorithmes symétriques.

3 le chiffrement RSA

Le concept de chiffrement asymétrique est attribué à Whitfield Diffie et à Martin Hellman, qui l'ont présenté en 1976. Le premier exemple de chiffrement asymétrique est le chiffrement RSA (abréviation des noms de ses inventeurs Ronald Rivest, Adi Shamir, Loenard Adleman).
La sécurité du RSA repose sur la facilité à multiplier deux nombres premiers entre eux et la difficulté de factoriser le produit de deux nombres premiers, pourvu qu'ils soient suffisamment grands. C'est à l'heure actuelle l'algorithme de chiffrement asymétrique le plus utilisé.

Pour comprendre les mécanismes sous-jacents au chiffrement RSA, et ceci n'est pas un attendu des programmes, on pourra lire l'article édité sur Interstices.info 5 qui propose aussi une animation interactive de ce chiffrement.

À noter qu'il existe d'autres algorithmes asymétriques : On peut citer, par exemple, la « cryptographie sur les courbes elliptiques » qui permet d'avoir un niveau de sécurité comparable à celui de RSA, mais en utilisant une clef beaucoup plus courte. Cette clef plus courte engendre des calculs plus rapides ainsi qu'une utilisation moins importante de mémoire et d'énergie.

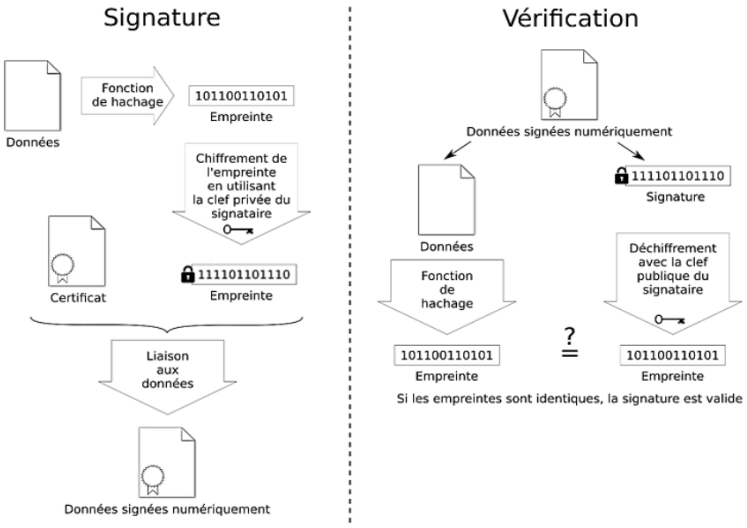
3.1 Autre utilisation:la signature numérique

Le chiffrement asymétrique permet également de réaliser une signature numérique. Par analogie avec la signature traditionnelle d'un document papier, la signature numérique :

- relie un document à son auteur ;

- est difficilement imitable. Contrairement à une signature « papier », la signature numérique possède des propriétés supplémentaires :
- elle appartient à un seul message. Il est donc impossible de la copier pour la coller sur un autre message ;
- elle ne peut pas être falsifiée ni reniée.

La signature numérique est calculée à partir de la clef privée du signataire et peut être vérifiée en utilisant la clef publique du signataire.



3.2 Le protocole HTTPS

Le protocole HTTPS est la version sécurisée du protocole HTTP. L'objectif du protocole HTTP est de recevoir et d'envoyer des informations de et vers des serveurs web sans se soucier de la façon dont ces informations se déplacent d'un endroit à un autre.
Le protocole HTTP n'étant pas sécurisé, il est donc possible de :

- falsifier un site : on ne peut avoir la garantie que le site auquel on se connecte est bien le bon ;
- intercepter et altérer les communications : n'importe quel élément du réseau sur le chemin de la connexion peut consulter les données échangées, et même les modifier au passage. Par exemple, modifier le montant d'une transaction bancaire, sans qu'il soit possible de le détecter.

  Pour résoudre ces problèmes, HTTPS utilise la suite de protocoles SSL/TLS qui met en jeu les 3 principes vus précédemment : signature numérique, cryptographie asymétrique et cryptographie symétrique.

3.3 Authentification du site

Lors de l'accès à un site utilisant le protocole HTTPS, le serveur envoie sa clef publique, ainsi qu'une signature numérique de cette clef, c'est ce qu'on appelle le certificat du site. Pour être valide, la signature du certificat du site doit avoir été réalisée par une autorité en laquelle le navigateur a confiance.

En pratique, le navigateur ou le système d'exploitation maintiennent une liste de clefs publiques en laquelle ils ont confiance, appelés certificats racines, et avec lesquelles ils vérifient le certificat présenté par le serveur web. Un principe résume correctement cette vérification : « les amis de mes amis sont mes amis ». Cela permet de ne pas avoir à stocker dans le navigateur l'intégralité des certificats des sites sûrs. L'inconvénient de cette méthode est que cette liste de certificats racines est critique.

En effet si une entrée « malveillante » est ajoutée, tous les sites qui auront été signés avec cette entrée seront considérés comme sûrs par le navigateur. En pratique, d'autres informations sont vérifiées comme la date de validité et la liste de révocations.

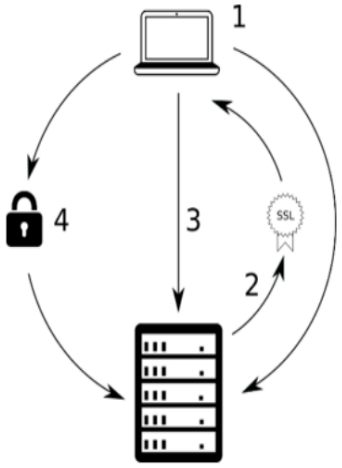
3.4 chiffrement des communications

Une fois le serveur authentifié, la communication peut commencer. Les algorithmes de chiffrement asymétrique sont en général assez coûteux en temps de calcul, c'est donc un algorithme de chiffrement symétrique qui va être utilisé pour chiffrer les échanges. Le problème est alors celui du partage de la clef.

- Une possibilité est que le client génère une clef, puis qu'il la partage avec le serveur en utilisant la clef publique du serveur pour la chiffrer. De cette façon, seul le serveur pourra déchiffrer la clef partagée et l'échange pourra continuer en utilisant cette clef et un algorithme symétrique.
- Une autre possibilité est d'utiliser un autre protocole appelé l'« Échange de clefs Diffie-Hellman 7 » du nom de ses auteurs, en 1976. Cet algorithme permet aux deux participants de se mettre d'accord sur la clef partagée, sans que celle-ci ait à transiter, même cryptée, sur le réseau. Cet échange est d'ailleurs obligatoire dans les versions récentes du protocole et il est utilisé, entre autres, par le réseau Tor.

3.5 En Résumé

L'implémentation du protocole SSL/TLS, et donc du protocole HTTPS, est assez complexe. Les algorithmes utilisés en pratique sont en quelque sorte négociés entre le client et le serveur lors de l'établissement de la connexion. En revanche, il faut être attentif à tous les détails pour que la sécurité soit assurée.



1. Demande d'initialisation d'une connexion par le protocole SSL.

2. Présentation du certificat :
- validité,
- signature par un tiers de confiance.

3. Transmission d'une clé de chiffrement unique, encodée avec la clef publique du serveur.

4. Déchiffrement de la clé de chiffrement par le serveur, à l'aide de sa clef privée :
- établissement de la connexion sécurisée.

3.6 Conclusion

Aujourd'hui, la cryptographie est partout, notamment dans les échanges informatiques pour protéger sa vie privée, sécuriser les échanges entre entreprises ou clients, acheter ou vendre en ligne, etc. La recherche dans le domaine est permanente, qu'elle soit d'ordre :

- mathématique : nouveaux algorithmes, nouvelles attaques ;
- ou informatique : augmentation de la puissance de calcul, innovation technologique (ordinateur quantique...).
  Pour ne citer qu'un seul exemple, le chiffrement DES (Data Encryption Standard), adopté comme standard en 1976, est devenu obsolète en 2001 à cause de l'augmentation de la puissance de calcul des ordinateurs.

€