

La cryptologie est la science des messages secrets.

Longtemps restreinte aux usages diplomatiques et militaires, elle est maintenant une discipline scientifique à part entière, dont l'objet est l'étude des méthodes permettant d'assurer les services **d'intégrité, d'authenticité et de confidentialité** dans les systèmes d'information et de communication.

Un service d'intégrité garantit que le contenu d'une communication ou d'un fichier n'a pas été modifié. Par exemple, on peut souhaiter vérifier qu'aucun changement du contenu d'un disque dur n'a eu lieu: des produits commerciaux, mettant en jeu des méthodes cryptologiques, sont disponibles à cet effet.

Un service d'authenticité garantit l'identité d'une entité donnée ou l'origine d'une communication ou d'un fichier. Lorsqu'il s'agit d'un fichier et que l'entité qui l'a créé est la seule à avoir pu apporter la garantie d'authenticité, on parle de **non-répudiation**. Le service de non-répudiation est réalisé par une **signature numérique**.

Un service de confidentialité garantit que le contenu d'une communication ou d'un fichier n'est pas accessible aux tiers. Des services de confidentialité sont offerts dans de nombreux contextes

- en téléphonie mobile, pour protéger les communications dans la partie “aérienne”;
- en télévision à péage pour réserver la réception des données aux abonnés;
- dans les navigateurs, par l'intermédiaire du protocole SSL (Secure Socket Layer), dont l'activation est souvent indiquée par un cadenas fermé représenté en bas de la fenêtre.
- ...

La cryptologie se partage en deux sous-disciplines, également importantes: la **cryptographie** dont l'objet est de proposer des méthodes pour assurer les services définis plus haut et la **cryptanalyse** qui recherche des failles dans les mécanismes ainsi proposés.

Elle est utilisée depuis l'Antiquité, mais certaines de ses méthodes les plus importantes, comme la cryptographie asymétrique, n'ont que quelques dizaines d'années d'existence.

Définitions

- chiffrement:** transformation à l'aide d'une clé de chiffrement d'un message en clair en un message incompréhensible si on ne dispose pas d'une clé de déchiffrement (en anglais *encryption*) ;
- chiffre:** anciennement code secret, par extension l'algorithme utilisé pour le chiffrement ;
- cryptogramme:** message chiffré ;
- décrypter:** retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement (terme que ne possèdent pas les anglophones, qui eux "cassent" des codes secrets) ;
- cryptographie:** étymologiquement "écriture secrète", devenue par extension l'étude de cet art (donc aujourd'hui la science visant à créer des cryptogrammes, c'est-à-dire à chiffrer) ;
- cryptanalyse:** science analysant les cryptogrammes en vue de les décrypter ;
- cryptologie:** science regroupant la cryptographie et la cryptanalyse.

Cryptographie conventionnelle

Chiffrement et déchiffrement

La cryptographie conventionnelle est principalement liée aux **services de confidentialité**.

Elle réalise sur les données m une transformation $c = E_k(m)$, par l'intermédiaire d'un algorithme de chiffrement E .

Cet algorithme prend en entrée le message clair m et un paramètre secret k , qu'on appelle la **clé**.

Le message m varie dans un ensemble M et la clé k dans un ensemble K .

La restauration du texte clair à partir du chiffré ou cryptogramme c se fait par un algorithme de déchiffrement D_k , prenant en entrée le chiffré et la même clé.

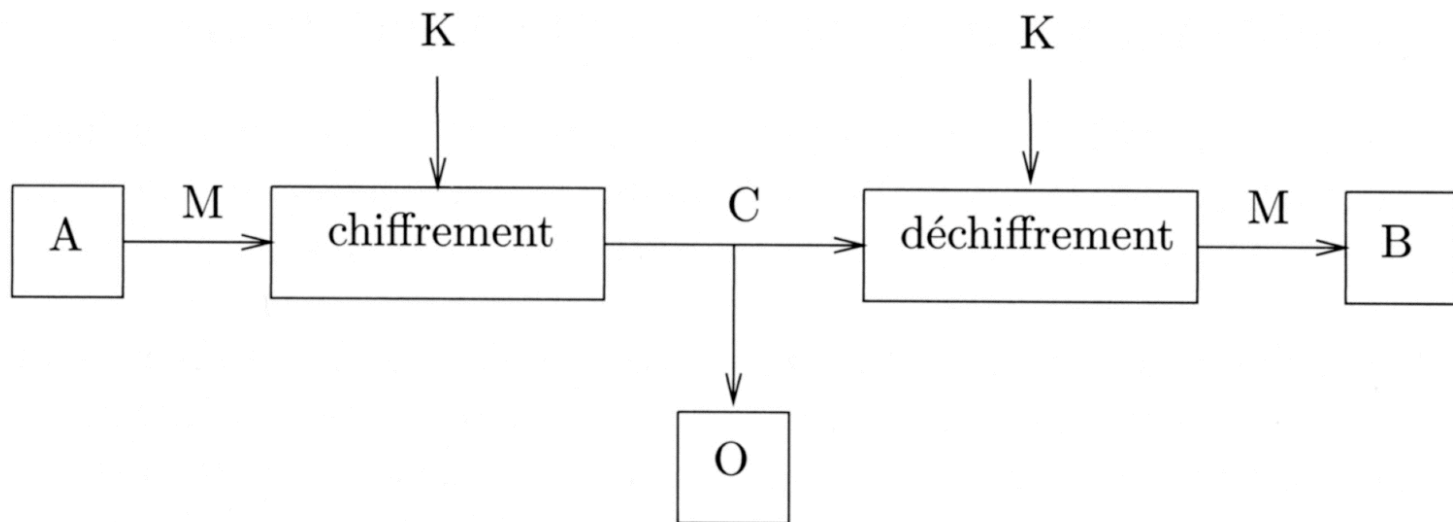
On doit avoir

$$D_k(E_k(m)) = m.$$

En général, le chiffré prend sa valeur dans le même espace M et l'on a aussi

$$E_k(D_k(c)) = c,$$

c'est à dire que les algorithmes E_k et D_k réalisent une permutation de M .



La distinction entre **l'algorithme** et la **clé** s'est établie au XIX^{ième} siècle, notamment dans les travaux du cryptologue Auguste Kerckhoffs. Ce dernier a en effet su reconnaître que **l'algorithme de chiffrement** n'exigeait pas le secret, dans la mesure où il risquait de toutes façons de passer aux mains de l'ennemi.

Dans un ouvrage fondamental qui ouvrit la cryptologie aux influences extérieures: "la cryptographie militaire" il mettait en relief le changement apporté aux communications militaires par le télégraphe.

Les chefs des armées désiraient que le chiffrement militaire possède les qualités suivantes: **sécurité, rapidité et donc simplicité.**

De ces principes de sélection d'un système de chiffrement opérationnel, il déduisit six conditions fondamentales:

- le système doit être **matériellement**, sinon mathématiquement, indécryptable
- il faut qu'il n'exige pas le secret et qu'**il puisse sans inconvénient tomber entre les mains de l'ennemi**
- la clé doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée et modifiée au gré des correspondants
- il faut qu'il soit applicable à la correspondance télégraphique
- il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes

- le système doit être d'un usage facile ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer

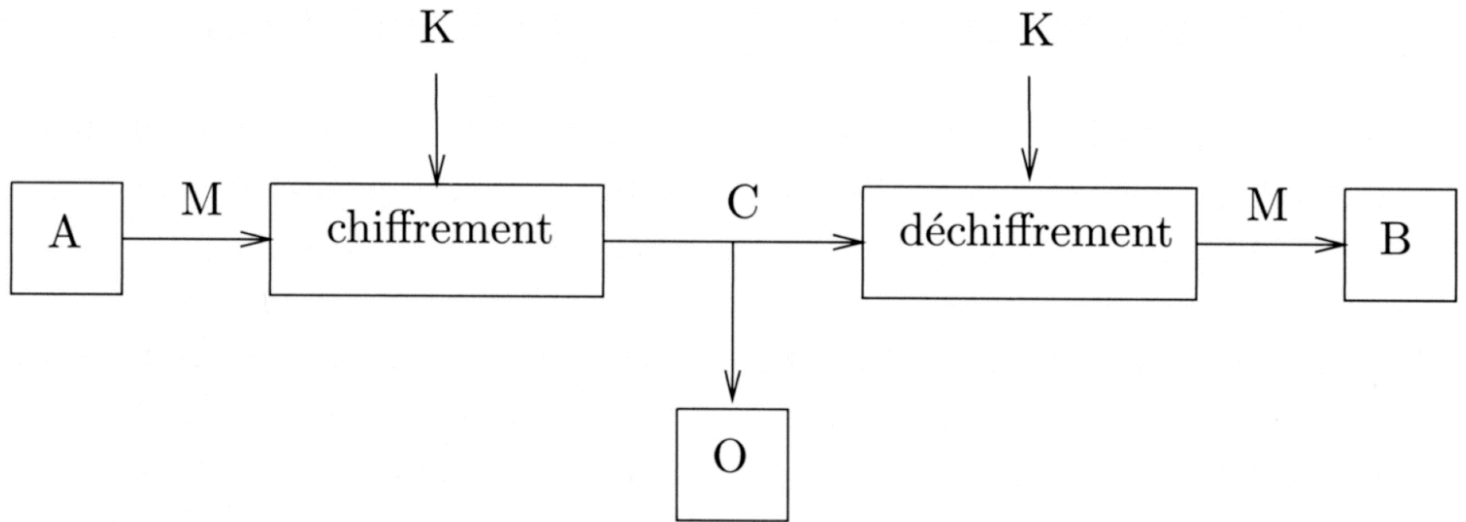
La cryptologie moderne recommande même des **méthodes de chiffrement totalement explicites**, de manière à ce qu'elles soient évaluées et validées par un débat ouvert entre experts.

Du coup, une convention secrète entre entités qui souhaitent communiquer de façon chiffrée, se limite à l'échange d'une clé k .

Décryptement

L'opération qui consiste à calculer le clair m à partir du chiffré $c = E_k(m)$, mais sans la connaissance de la clé k est appelée décryptement.

La confidentialité est assurée si cette opération est impossible.



On distingue divers scénarios possibles d'attaque

- les attaques à chiffré seul, où l'adversaire dispose d'un certain nombre de chiffrés $E_k(m_i)$;
- les attaques à clair connu, où l'adversaire dispose d'un certain nombre de chiffrés $E_k(m_i)$ et des clairs correspondants m_i ;
- les attaques à clair choisi, où l'adversaire dispose d'un certain nombre de chiffrés $E_k(m_i)$ correspondant à des clairs de son choix m_i ; si de plus chaque message m_i est défini en fonction des chiffrés obtenus antérieurement, on parle d'attaque à clair choisi adaptative.

Le but de l'attaque est la découverte de la clé ou le décryptement d'un chiffré c , correspondant à un clair dont on ne dispose pas.

Les attaques à chiffré seul sont les plus difficiles. Néanmoins, l'adversaire dispose en général d'informations statistiques sur le clair.

En d'autres termes, les messages sont créés en suivant une probabilité qui correspond à une distribution sur M , appelée distribution a priori. L'interception d'un (ou plusieurs) chiffrés a pour effet de conditionner cette distribution, produisant une distribution a posteriori:

Par exemple si l'on sait qu'un message chiffré provient d'une distribution équiprobable sur les mots "tas", "sas", "mur" et si le chiffrement est une substitution de lettres, alors l'interception du chiffré XUV élimine "sas".

Quelques repères historiques

Chiffrement par **substitution**.

Le message chiffré se déduit du message en clair par une permutation des lettres de l'alphabet.

Jules César utilisait un système où chaque lettre d'un message était remplacée par celle située trois positions plus loin dans l'alphabet.

Chiffrement par **permutation**.

La **cryptanalyse**, quant à elle, utilisait des méthodes statistiques simples, fondées principalement sur la fréquence des lettres ou des suites de deux lettres (digrammes) dans un texte.

Le XX^e siècle conserve les substitutions et les permutations mais les met en œuvre à l'aide de machines mécaniques ou électro-mécaniques. La plus célèbre est l'Enigma utilisée par l'armée allemande durant la seconde guerre mondiale.

Pour venir à bout de **l'Enigma**, un groupe de scientifiques parmi lesquels Alan Turing, se réunit. Il parvient à réaliser une spectaculaire cryptanalyse en la réduisant à une recherche de cas suffisamment restreinte pour être menée par une machine spécialement construite à cet effet.

Cela a représenté une **augmentation importante de la sophistication** des outils mathématiques qui ont été utilisés. Depuis, les mathématiques ont joué un rôle de plus en plus important dans la cryptologie.

Une grande impulsion semble être venue à la suite de l'apparition de la communication par radio au début du XX^e siècle. Ce développement technologique a mené à la croissance du trafic militaire, diplomatique, et commercial.

Il était nécessaire de protéger un tel trafic, contre l'interception, et cela a mené à la recherche d'une amélioration des méthodes de chiffrement.

Le **développement des applications civiles** menaient au des problèmes tels que la gestion des clés et les signatures numériques, qui auparavant n'avaient pas été perçues comme importantes dans les communications militaires et diplomatiques qui sont des domaines plus petits et soumis à un contrôle plus strict. En même temps, les développements en technologie offraient des possibilités sans précédent pour mettre en application des algorithmes compliqués.

Les **mathématiques** se sont avérées fournir les outils qui ont été utilisés pour relever le défi. C'était un exemple de ce qu'Eugene Wigner a appelé "l'efficacité peu raisonnable des mathématiques," des techniques développées pour des buts abstraits s'avèrent être étonnamment efficaces confrontées à de vraies applications.

Lorsque l'on crypte une information avec une **clé secrète**, le destinataire utilisera la même clé secrète pour décrypter. C'est la **cryptographie symétrique**. Il est nécessaire que les deux interlocuteurs se soient mis d'accord sur une clé privée auparavant, par courrier, par téléphone ou lors d'un entretien privé.

La **cryptographie à clé publique** a été inventée par Whitfield Diffie et Martin Hellman en 1976 pour éviter ce problème d'échange de clé secrète préalable. C'est à dire que pour crypter un message, on utilise la clé publique (connue de tous) du destinataire, qui sera à priori le seul à pouvoir le décrypter à l'aide de sa clé privée (connue de lui seul). Les algorithmes à clé publique sont aussi appelés algorithmes asymétriques.

Mais la cryptographie à clé publique **demande plus de temps de chiffrement** et utilise **des clés de longueur plus importante**.