# Atelier 1 : présentation du chiffrement

**Documentation consultée :**

Les articles suivants de Wikipedia (https://fr.wikipedia.org/wiki/) :

- Chiffrement
- Chiffrement du courrier électronique
- Cryptographie asymétrique
- Chiffrement RSA

## Pourquoi chiffrer ses mails

Si la poste ouvrait toutes les lettres, les numérisait et les indexait pour exploiter le contenu à des fins commerciales mais pas que... Que dirions-nous ?

C'est exactement ce que fait Google ! Quand on écrit à une adresse gmail, le mail est numérisé, indexé et tout...

En dehors de cette surveillance de masse, des personnes, les lanceurs d'alerte par exemple, peuvent être mises spécifiquement sous surveillance par la plupart des FAI ou des fournisseurs de mails. Cela à la demande du gouvernement ou plus simplement par leur employeur pour les mails professionnels.

Chiffrer ses mails c'est juste protéger les informations qu'on envoie parce que ces informations sont privées.

## Introduction : un peu de vocabulaire

Le **code** (définition du Petit Robert) : "Le code est un système de symboles destiné à représenter et à transmettre une information".

On connaît tous : le code postal, le code barre, le code morse (échange de texte avant internet) mais aussi le code génétique. Quand le code utilisé peut être connu de tous on parle de **codage**. Quand le code est destiné à protéger l'information, il est secret et on parle de **chiffrement**.

Un code nécessite forcément **une table de conversion** pour passer d'une forme à l'autre. Là, chiffrement et codage sont très proches :

- si la table de conversion est publique, il s'agit de codage
- si la table de conversion n'est connue que des quelques personnes qui l'utilisent, il s'agit de chiffrement. Et on parle plutôt de **clé** que de table de conversion.

Lorsque le contenu du message chiffré est remis en clair en utilisant la clé, on parle de **déchiffrement**.

L'opération qui consiste à essayer d'accéder au contenu sans la clé de chiffrement s'appelle le **décryptage**.

## Le chiffrement symétrique

C'est le premier type de chiffrement inventé, il est utilisé depuis très longtemps, bien avant l'ère chrétienne. L'émetteur et le récepteur commencent par se mettre d'accord sur une méthode de chiffrement, par exemple le remplacement de telle lettre par telle autre lettre, en fait une table de conversion comme on l'a déjà vu.

Le point faible de ce chiffrement est que les personnes doivent d'abord se rencontrer physiquement pour échanger la clé de chiffrement, ce chiffrement n'est sûr que tant que personne d'autre n'a la clé.

Ce chiffrement n'utilise qu'une seule clé, c'est la table de conversion. Elle sert à la fois à chiffrer et à déchiffrer.

Il peut se faire à la main, et les temps de calcul pour le codage et le décodage ne sont pas un problème : ils sont courts.

Il peut être fait à la main, mais cela ne veut pas dire que ce soit simple.

En plusieurs siècles de chiffrement d'informations, les humains ont eu le temps d'imaginer des sytèmes très compliqués de chiffrement, plus de détails amusants sur le site : https://zestedesavoir.com/articles/54/cest-toute-une-histoire-la-cryptographie-partie-1-3/

## Le chiffrement asymétrique

Le chiffrement asymétrique (avec un seul ‘s') est très récent. Le concept a été décrit en 1974, mais la première réalisation pratique a été faite en 1978 par Ronald Rivets, Ali Shamir et Leonard Adleman qui fondèrent la société RSA Security. On parle de chiffrement RSA. (On parle aussi de cryptographie à clé publique.)

Le chiffrement asymétrique utilise 2 clés :

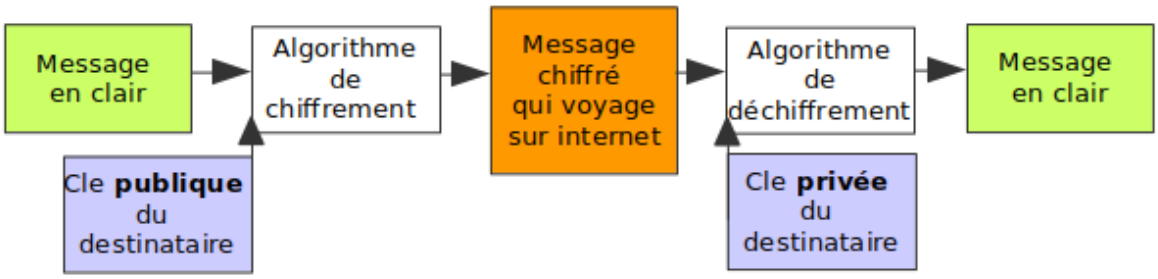
- une clé pour le chiffrement : la clé publique
- une clé pour le déchiffrement : la clé privée

Dans le chiffrement symétrique, la clé joue un rôle symétrique entre le chiffrement et le déchiffrement.

Dans le chiffrement asymétrique, le chiffrement et le déchiffrement n'utilisent pas la même clé. Ces deux opérations ne sont donc pas symétriques.

Pour envoyer un message chiffré à un destinataire, il doit d'abord vous avoir donné sa clé publique, donc un accord préalable est indispensable.

**Déroulement de la transaction :**




Il est important de garder en tête qu'un courriel se chiffre **avec la clé publique du destinataire**.

La sécurité de ce système de chiffrement réside sur le secret des clés et non sur celui de l'algorithme. Le point fondamental est l'impossibilité, par calcul, de déduire la clé privée de la clé publique.

Ce chiffrement utilise des fonctions à sens unique et à brèches secrètes : c'est à dire des fonctions difficiles à inverser, à moins de posséder une information particulière : la brèche secrète.

Les calculs utilisent la représentation des nombres dans les machines; il n'est pas réaliste d'envisager de le faire à la main. Les calculs sont longs... pour une machine, et inaccessibles aux humains, pas que pour des raisons de temps de calcul.

## Essai d'analogie

Si le chiffrement, c'est mettre une serrure pour fermer un texte et empêcher qu'il soit lu par tout le monde :

- dans le cas du chiffrement symétrique : la serrure ne possède qu'un modèle de clé. Cette clé permet d'ouvrir et de fermer le texte.
- dans le cas du chiffrement asymétrique : la serrure possède un jeu de 2 clés :
    - une clé qui ferme : la clé publique
    - une clé qui ouvre : le clé privée

Les deux clés ont un rôle symétrique : un texte fermé par une clé est ouvert par l'autre clé, et uniquement par l'autre clé.

## Utilisation du chiffrement asymétrique

**A** décide de chiffrer ses courriels à destination de **B**, pour cela il lui faut :

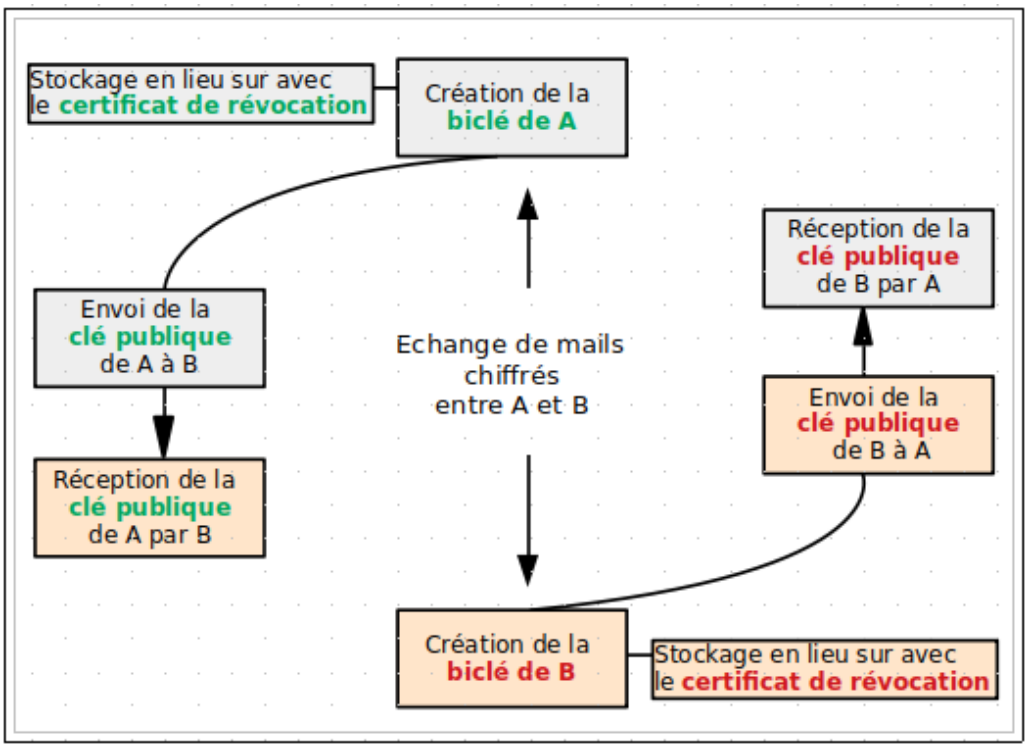
1. Créer un jeu de 2 clés :
    - une clé publique qui sera donnée à ses correspondants
    - une clé privée qui sera gardée précieusement. Personne ne doit avoir accès à cette clé.
2. Envoyer sa clé publique à **B** pour faire un premier test. **B** va pouvoir envoyer à **A** un courriel chiffré (avec la clé publique de **A**). Lorsque **A** reçoit ce courriel, sa clé privée lui permet de le déchiffrer. Comme **B** en a profité pour lui envoyer sa clé publique, chacune a :
    - sa propre clé privée,
    - la clé publique de l'autre.

3. Au fur et à mesure que leur réseau d'échange en courriels chiffrés s'agrandira, chacune aura :

    - toujours uniquement sa clé privée,
    - de plus en plus de clés publiques.

Avec les bons logiciels, cela se fait tout seul : Enigmail reconnaît si vous avez ou non, la clé publique du destinataire du courriel et vous propose de chiffrer, ou pas.

L'envoi d'un courriel chiffré par Dom à Claude peut se schématiser :




**Remarque de sécurité**
Il est préférable de ne pas envoyer sa clé publique par un mail. Le destinataire doit être sur que c'est bien votre clé qu'il reçoit. Il est possible de :

- déposer la clé publique sur un serveur de clés
- échanger ses clés publique en utilisant une clé USB
- déposer sa clé dans un espace privé commun aux deux personnes

## Aspects légaux

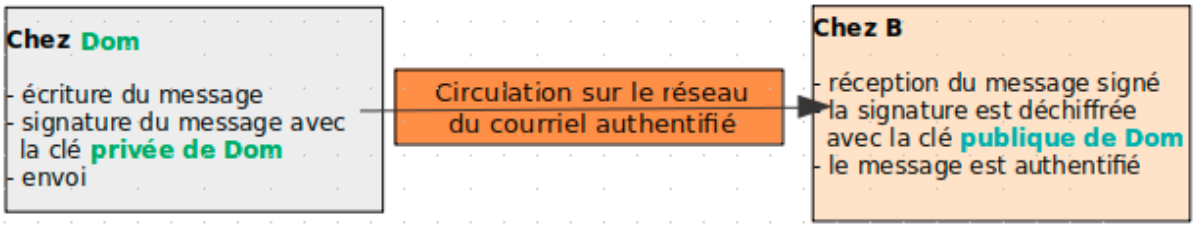
Après avoir été interdit jusqu ‘en 1996, puis autorisé avec des limites jusqu'en 2004, la Loi pour la Confiance dans l'Économie Numérique du 21 juin 2004 a totalement libéré l'utilisation ds moyens de cryptologie, et donc le chiffrement des courriels. La signature numérique, dans un cadre légal, donne une valeur juridique à un courrier électronique.

-> voir les aspects juridiques

## Signature numérique

Le fait que les 2 clés aient un fonctionnement symétrique l'une par rapport à l'autre est utilisé pour la signature numérique : ce qui est chiffré avec la clé privé de l'expéditeur pourra être déchiffré par sa clé

publique.




## Conséquence pratique de ce fonctionnement

Le chiffrement et déchiffrement se font dans l'interface utilisateur du service de messagerie, c'est donc à ce niveau que sont stockées les clés. Le stockage des clés ne peut se faire que sur l'ordinateur de l'utilisateur qui chiffre. Ce n'est pas possible et si c'était possible il ne serait pas raisonnable de stocker sa clé privée sur un serveur géré par Google !!! ou par n'importe qui d'autre, du reste. Et donc on ne peut pas chiffrer ses courriels en utilisant un webmail.

Donc :

- on ne chiffre ses courriels qu'à partir de sa propre machine
- il est indispensable de sauver ses clés quelque part... ailleurs

---


*Dernière édition le jeudi 24 septembre 2020 à 15:44*