15.1 Principe

Histoire

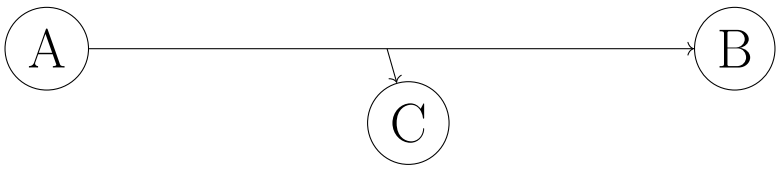
Il faut savoir que l'idée de chiffrer des messages (de les rendre illisibles pour des personnes non autorisées) ne date pas du début de l'ère de l'informatique !
En effet, dès l'antiquité, on cherchait déjà à sécuriser les communications en chiffrant les messages sensibles.
Citons par exemple :

- Le chiffrement de césar : http://www.cryptage.org/chiffre-cesar.html
- Le chiffrement de Vignere : http://mathweb.free.fr/crypto/poly/vigenere.php3
- La machine enigma
  : http://www.irem.unilim.fr/fileadmin/user_ upload/Convergences/tpe_ enigma.pdf

Imaginons que A envoie un message à B :



Si le message est non sécurisé, il pourra être intercepté et lu par C.



Pour ce faire, A va chiffrer le message.

Si C intercepte le message, et si C ne posséde pas le moyen de déchiffrer le message chiffré, il sera impossible pour lui de le lire le contenu.

Définition

Le **chiffrement** d'un message consiste à le modifier et le rendre illisible par une personne qui n'est pas autorisée.

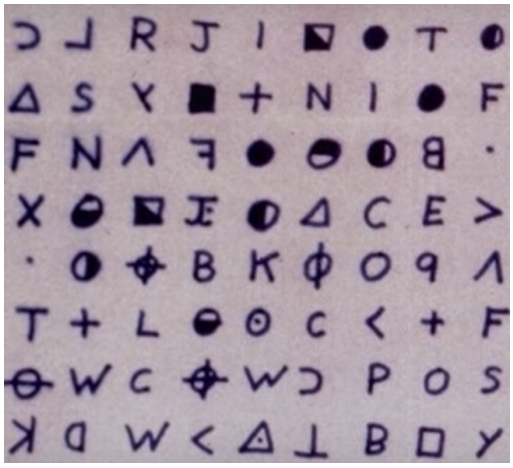
Définition

Le chiffrement (et le déchiffrement) est réalisé en appliquant au message initial une fonction mathématique, basée sur une donnée convenue entre les deux extrémités, appelée **clés de chiffrement**.

Il existe 2 grands types de chiffrement : le chiffrement symétrique et le chiffrement asymétrique.

Nous étudierons ici le chiffrement de message 'informatique'. Comme toute "donnée informatique" peut être vue comme une suite de zéro et de un. Nous chercherons donc à chiffrer une suite de zéro et de un !

Vidéo : Comment déchiffrer n'importe quel message !



https://www.youtube.com/watch?v=z4tkHuWZbRA