Introduction à la cryptographie

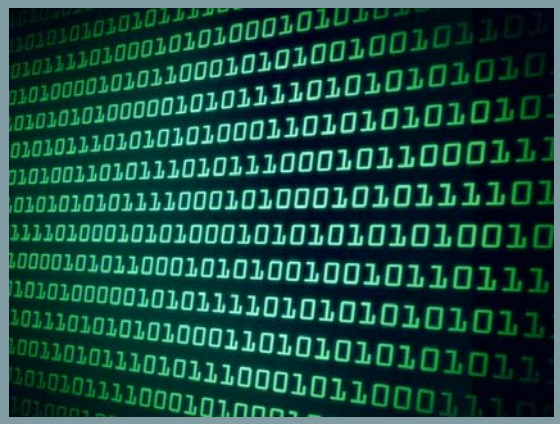
Plan du cours

- **0. Courte introduction.**
- **I. Systèmes à clef publique.**
- **II. Systèmes à clef secrète.**
- **III. Authentification.**
- **IV. Exemples.**

Plan du cours

- **0. Courte introduction.**
- **I. Systèmes à clef publique.**
- **II. Systèmes à clef secrète.**
- **III. Authentification.**
- **IV. Exemples.**

- **Objectif du cours.**
- **Terminologie.**



- Donner une introduction aux techniques de cryptographie moderne, sans trop de mathématiques…

- Décrire les principaux algorithmes de chiffrement utilisés en informatique, dans les réseaux et en particulier dans les réseaux sans fil.

- La cryptologie est la science du secret. Elle regroupe la cryptographie et la cryptanalyse.
- La cryptographie est l'ensemble des techniques de chiffrement de la cryptologie.
- Le but d'un cryptosystème est d'assurer la confidentialité d'un message entre son émetteur et son destinataire.
- Il existe deux grands types d'algorithmes: à clef secrète et à clef publique.

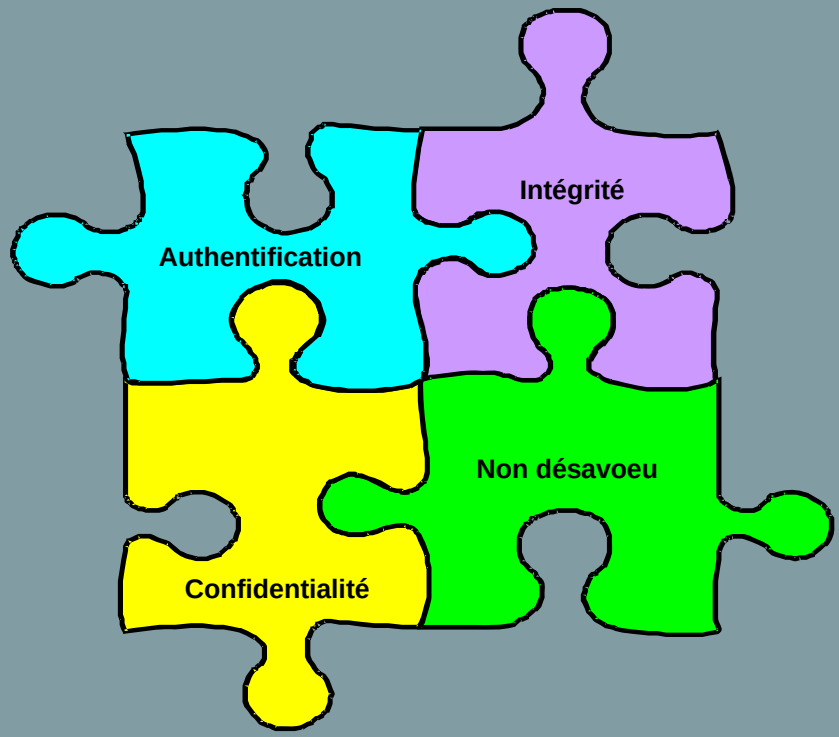
Deux articles fondamentaux sont à l'origine de la cryptographie moderne :

- « The communication theory of secrecy systems » de Claude Shannon (1949) qui définit la notion d'information et d'entropie.
- « New directions in cryptography » de W. Diffie et M. Hellman (1977) qui pose les bases de la cryptographie à clef publique.

On attend d'un système cryptographique qu'il résolve les problèmes de :

- **Confidentialité** : le message transmis ne peut pas être lu par une 3ème personne.
- **Authentification** : Le destinataire doit être certain de l'identité de l'émetteur.
- **Non désavoeu** : L'expéditeur ne doit pas pouvoir nier avoir envoyé le message.
- **Intégrité** : Le message ne doit pas pouvoir être modifié entre son expédition et sa réception.

- **Confidentialité.**
- **Authentification.**
- **Non désavoeu.**
- **Intégrité.**

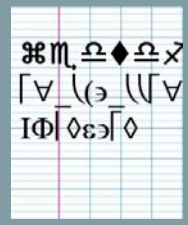


- Chiffrement et déchiffrement.
- Alice, Bernard, Eve & les autres.
- Cryptanalyse.

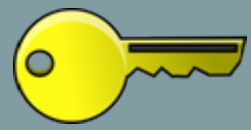
- Un algorithme de chiffrement transforme un message appelé **texte en clair** en un **message chiffré**, à l'aide de **clefs** et d'une **fonction de chiffrement**.
- Le processus qui permet de recouvrer le texte en clair à partir du texte chiffré est la s'appelle **déchiffrement**.
- La fonction qui transforme le texte en clair en texte chiffré est la fonction de **chiffrement**.

- x ou m le texte en clair.

- y le texte chiffré.



- $\mathcal{K}$ l'ensemble des clefs.

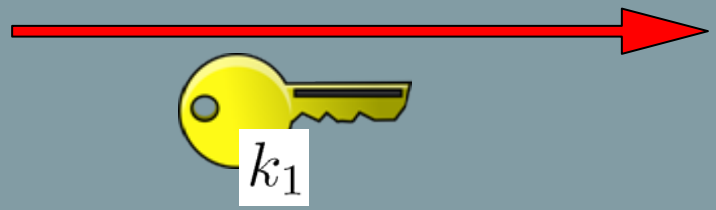


- E la fonction de chiffrement.

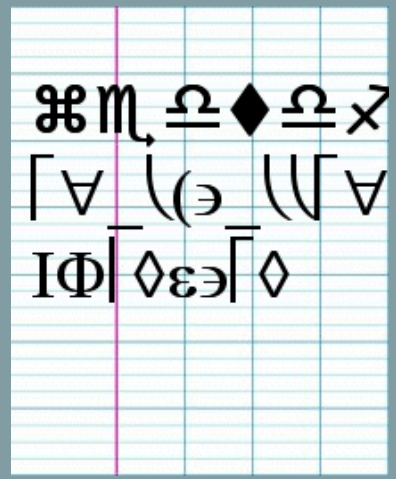
- D la fonction de déchiffrement.

$$y = E_{k_1}(x)$$

x



chiffrement



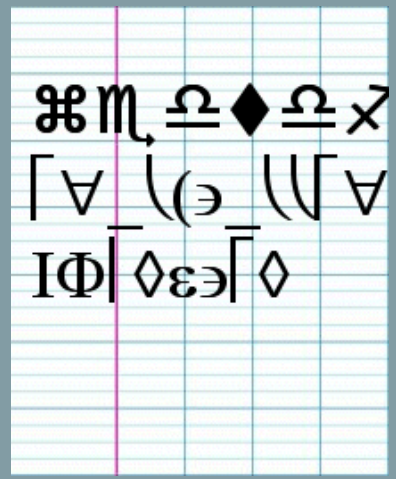
y

$$x = D_{k_2}(y)$$

x

k_2

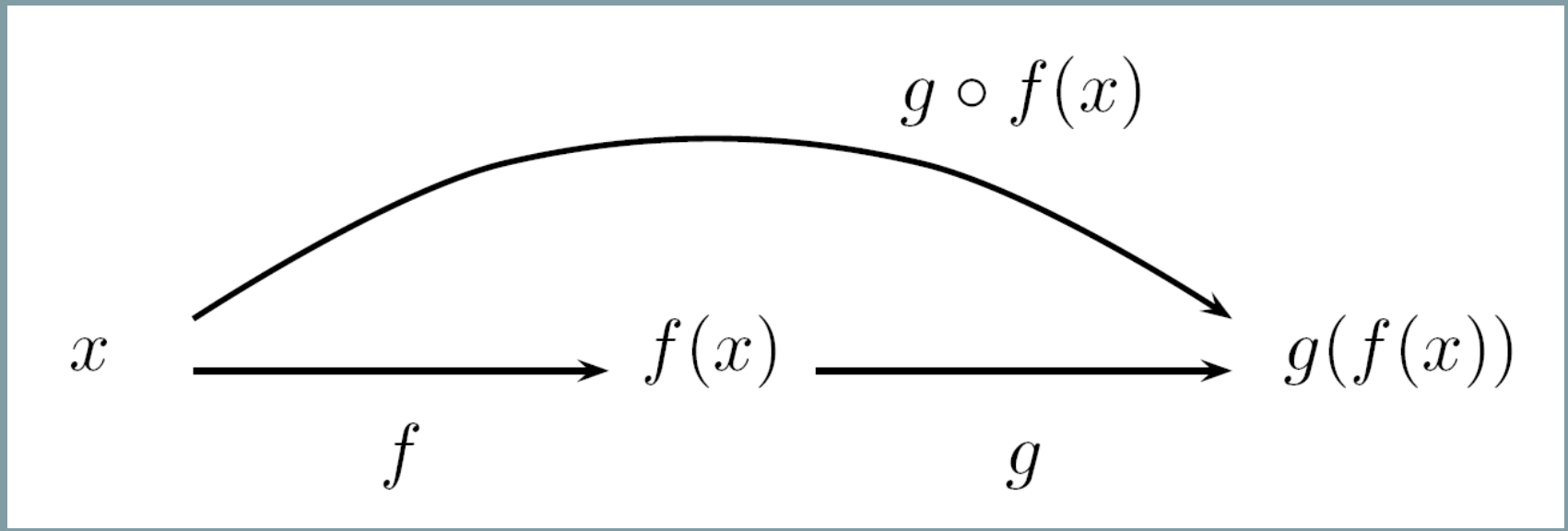
déchiffrement



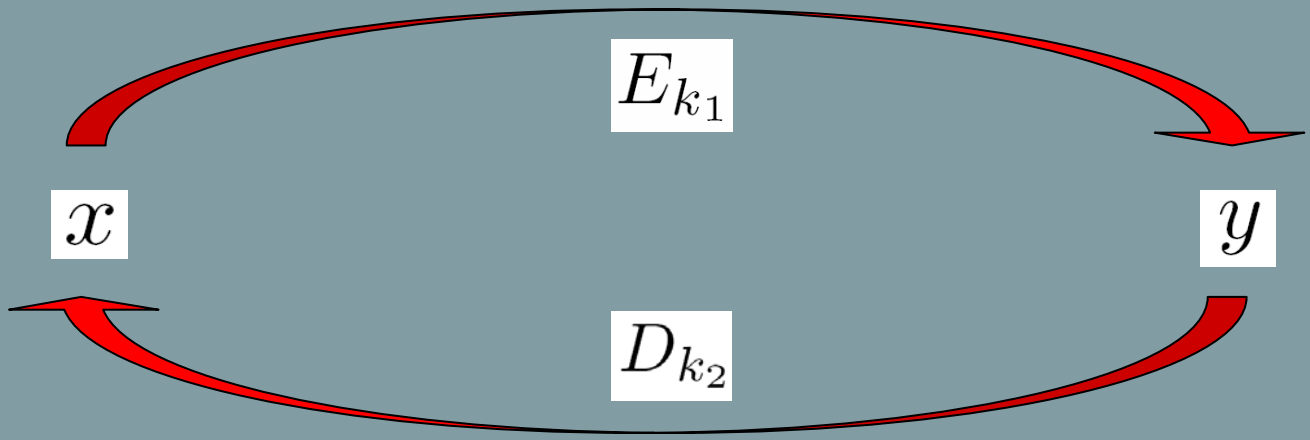
y

La composée de deux fonctions applique successivement à un nombre (ou un texte) l'action de chaque fonction.

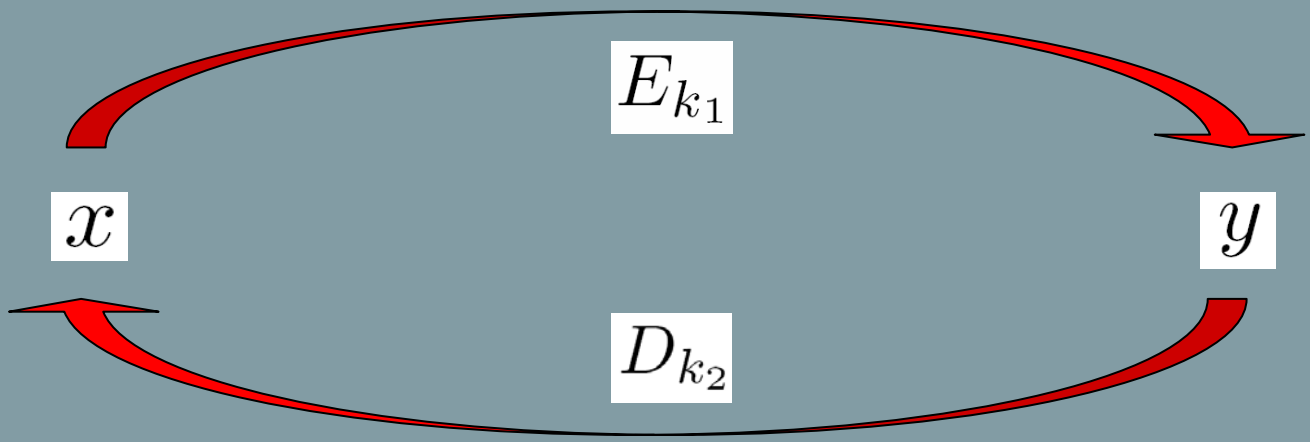
$$f \circ g(x) = f\left(g(x)\right)$$



Lien entre tous ces éléments (chiffrement et déchiffrement).



$$\left.\begin{array}{l} x = D_{k_2}(y) \\ y = E_{k_1}(x) \end{array}\right\} \Rightarrow D_{k_2}(E_{k_1}(x)) = x$$



$$D_{k_2}(E_{k_1}(x)) = x \quad \Longrightarrow \quad D_{k_2} \circ E_{k_1} = \mathrm{Id}$$

Les fonctions de chiffrement et déchiffrement sont réciproques l'une de l'autre.

- Si $k_1 = k_2$ on parle de chiffrement symétrique. C'est souvent le cas dans les algorithmes à clef secrète.
- Sinon, on parle de chiffrement asymétrique.
- Les algorithmes à clef publique sont asymétriques.

- Dans tout protocole, il y aura un expéditeur et un destinataire, que nous appellerons Alice et Bernard comme cela est souvent l'usage en cryptographie.
- Il y aura souvent aussi un espion qui tentera d'intercepter le message et que nous appelerons Eve.
- Martin sera également un espion malveillant qui tentera des attaques actives contre les protocoles.

- Camille sera l’autorité de certification et représentera une personne en laquelle on peut avoir confiance (une sorte ce notaire, en fait) et qui sera chargé de diverses transactions.

- C’est le processus qui permet de déterminer le texte en clair à partir du texte chiffré sans posséder la clef.

- Lorsqu’on effectue une cryptanalyse, on attaque le protocole cryptographique.

- Il existe différents types d’attaques.

- Attaque à texte chiffré: si on ne dispose que d'un texte chiffré sans avoir le texte en clair correspondant.
- Attaque à texte en clair connu: si l'on possède au moins un texte en clair et le texte chiffré correspondant .
- Attaque à texte en clair choisi: si l'on peut envoyer des textes en clair et récupérer les textes chiffrés correspondants.

- La taille des clefs est un paramètre très important des algorithmes.
- L'attaque exhaustive est l'attaque qui teste toutes les clefs possibles.
- Il faut donc avoir un ensemble de clefs $\mathcal{K}$ très grand pour que cette attaque soit impossible.

« La sureté d'un algorithme cryptographique ne doit pas reposer sur le secret de l'algorithme mais sur sa robustesse et sa clef. Comme l'histoire l'a montré à de très nombreuses reprises, il est impossible de garder un algorithme secret très longtemps; c'est juste une question de temps ou d'argent avant qu'il ne soit volé ou dévoilé. Les meilleurs algorithmes sont ceux qui ont été publiés, attaqués par tous les spécialistes et qui ont résisté à ces attaques. Garder un algorithme secret n'augmente pas sa sécurité, au contraire. »

- Photo de couverture: © Adi Shamir.
- Dessin du puzzle: © Haykel Mejri.
- Photo nombres binaires: © Westwood Schools.
- Autres sources d’inspiration:
  - Cryptographie appliquée de Bruce Schneier, éditions Vuibert.
  - L’art du secret, in « dossier pour la science ».
  - Histoire des codes secrets, de Simon Singh, éditions livre de poche.