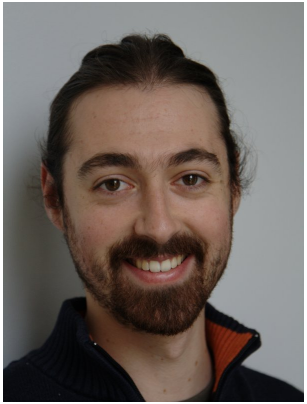
Une aventure de James Bond

Une aventure de James Bond

- Le célèbre agent 007 est dans un hôtel à l'autre bout du monde

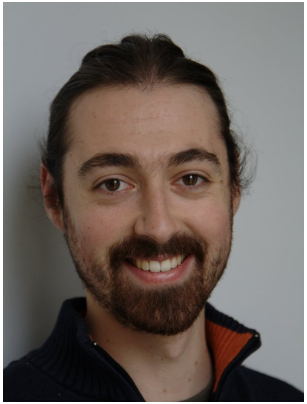
Une aventure de James Bond

- Le célèbre agent 007 est dans un hôtel à l'autre bout du monde
- Miss Moneypenny doit lui faire parvenir la photo d'un agent double



Une aventure de James Bond

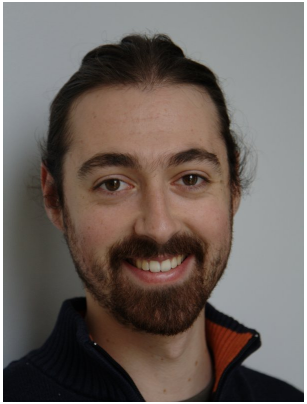
- Le célèbre agent 007 est dans un hôtel à l'autre bout du monde
- Miss Moneypenny doit lui faire parvenir la photo d'un agent double



- Il n'y a qu'un fax à la réception de l'hôtel

Une aventure de James Bond

- Le célèbre agent 007 est dans un hôtel à l'autre bout du monde
- Miss Moneypenny doit lui faire parvenir la photo d'un agent double



- Il n'y a qu'un fax à la réception de l'hôtel
- Mais 007 ne fait pas confiance au réceptionniste

Une aventure de James Bond

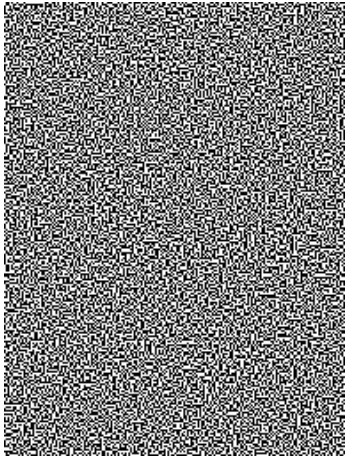
- Le célèbre agent 007 est dans un hôtel à l'autre bout du monde
- Miss Moneypenny doit lui faire parvenir la photo d'un agent double

- Il n'y a qu'un fax à la réception de l'hôtel
- Mais 007 ne fait pas confiance au réceptionniste
- **Comment faire ?**

Cryptographie visuelle (Naor & Shamir, 1994)

Cryptographie visuelle (Naor & Shamir, 1994)

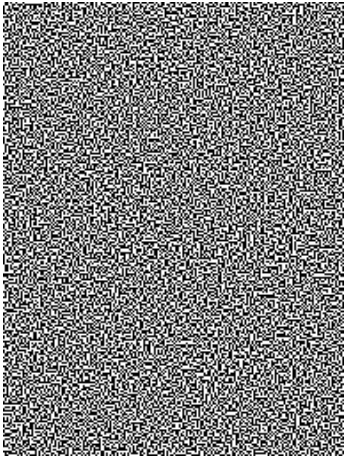
- Avant de partir en mission, Bond avait créé une **clé** de cryptographie visuelle



Clé

Cryptographie visuelle (Naor & Shamir, 1994)

- Avant de partir en mission, Bond avait créé une **clé** de cryptographie visuelle
- Miss Moneypenny peut donc **chiffrer** la photo de l'agent double avec cette clé



Clé

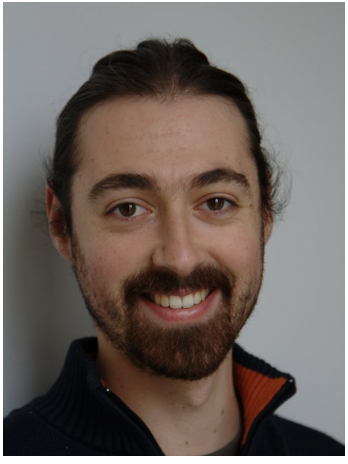
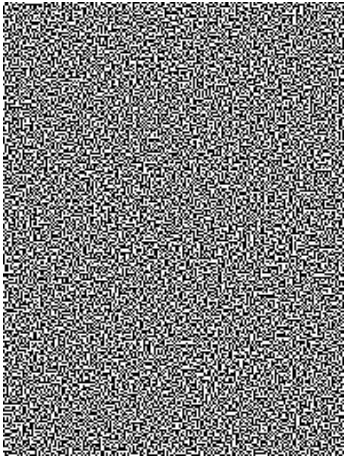


Photo originale

Cryptographie visuelle (Naor & Shamir, 1994)

- Avant de partir en mission, Bond avait créé une **clé** de cryptographie visuelle
- Miss Moneypenny peut donc **chiffrer** la photo de l'agent double avec cette clé

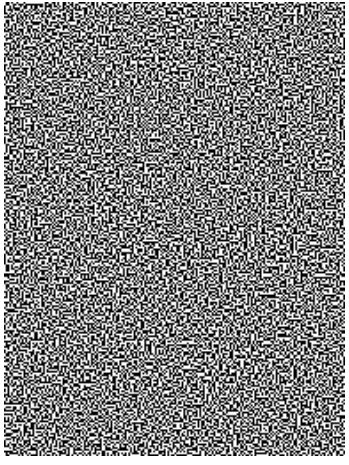


Clé

Photo N&B

Cryptographie visuelle (Naor & Shamir, 1994)

- Avant de partir en mission, Bond avait créé une **clé** de cryptographie visuelle
- Miss Moneypenny peut donc **chiffrer** la photo de l'agent double avec cette clé



Clé

Photo N&B

$\Rightarrow$

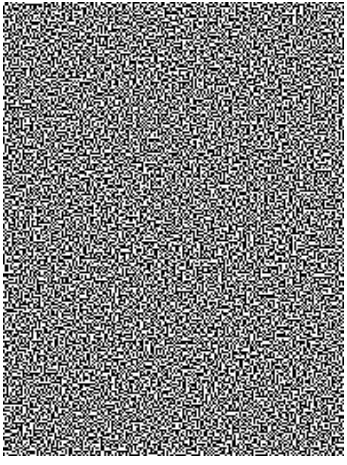
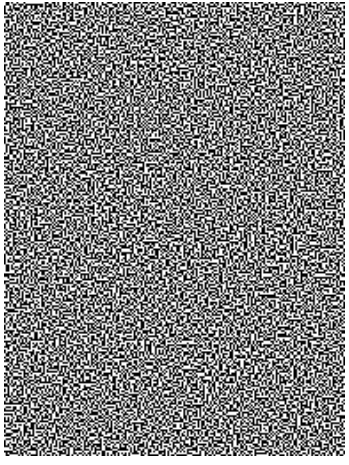


Photo chiffrée

Cryptographie visuelle (Naor & Shamir, 1994)

- Avant de partir en mission, Bond avait créé une **clé** de cryptographie visuelle
- Miss Moneypenny peut donc **chiffrer** la photo de l'agent double avec cette clé



Clé

Photo N&B

$\Rightarrow$

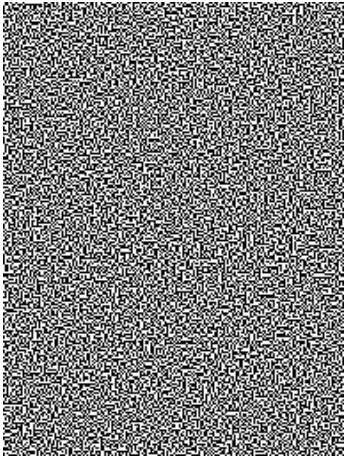


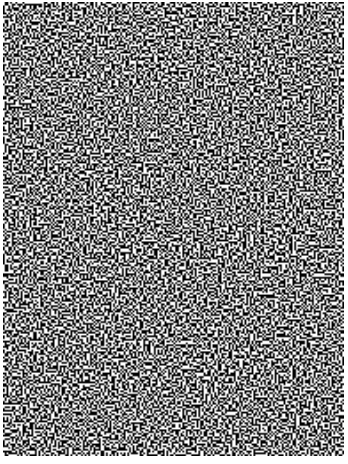
Photo chiffrée

- Miss Moneypenny envoie alors la **photo chiffrée** par fax à Bond

Cryptographie visuelle (Naor & Shamir, 1994)

Cryptographie visuelle (Naor & Shamir, 1994)

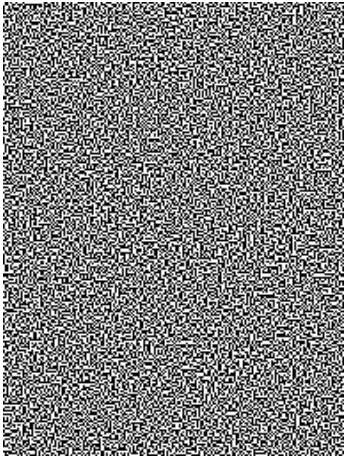
- Bond avait gardé avec lui une copie de la **clé**



Clé

Cryptographie visuelle (Naor & Shamir, 1994)

- Bond avait gardé avec lui une copie de la **clé**
- Il peut alors **déchiffrer** le fax envoyé par Miss Moneypenny



Clé

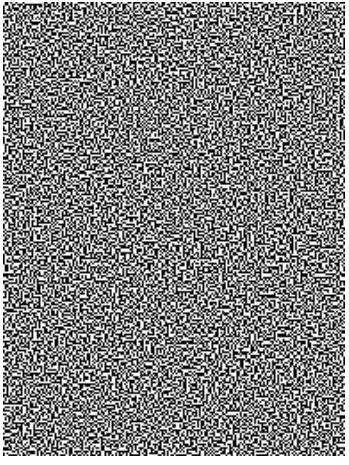
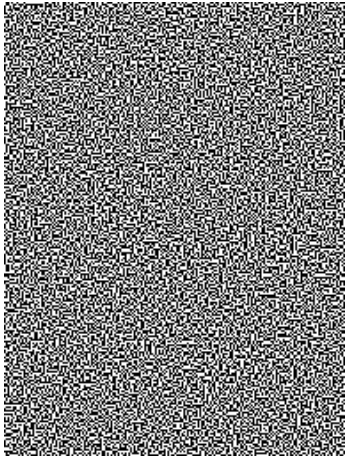


Photo chiffrée

Cryptographie visuelle (Naor & Shamir, 1994)

- Bond avait gardé avec lui une copie de la **clé**
- Il peut alors **déchiffrer** le fax envoyé par Miss Moneypenny



Clé

+

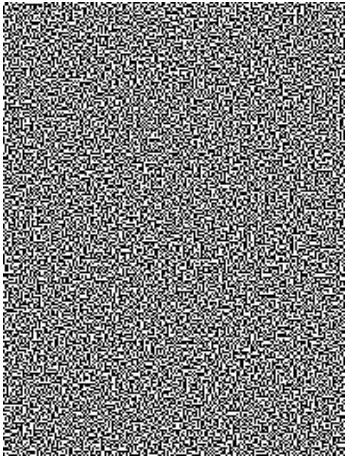


Photo chiffrée

=

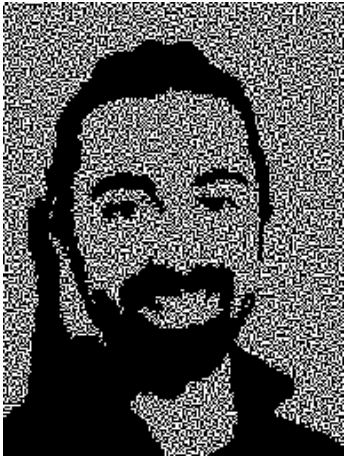


Photo déchiffrée

Cryptographie visuelle (Naor & Shamir, 1994)

Cryptographie visuelle (Naor & Shamir, 1994)

- Le réceptionniste (qui était effectivement un espion ennemi) n'a que le fax

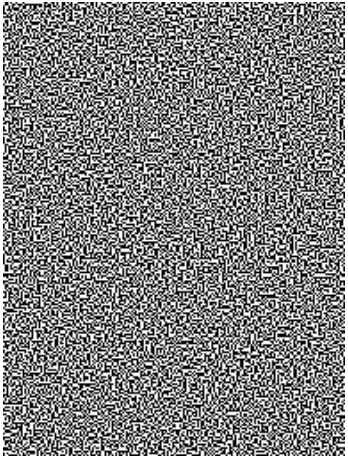
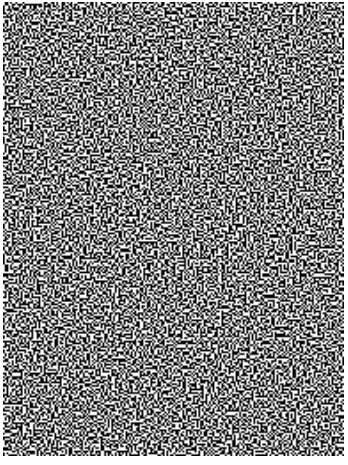


Photo chiffrée

Cryptographie visuelle (Naor & Shamir, 1994)

- Le réceptionniste (qui était effectivement un espion ennemi) n'a que le fax
- Il peut alors essayer de deviner une clé valide



Mauvaise clé

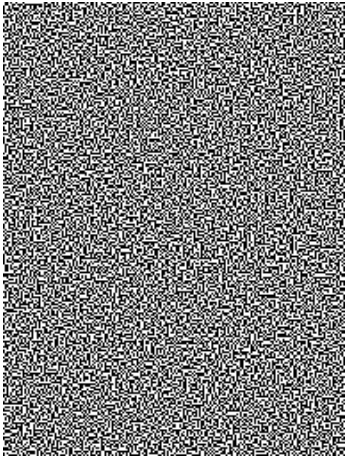
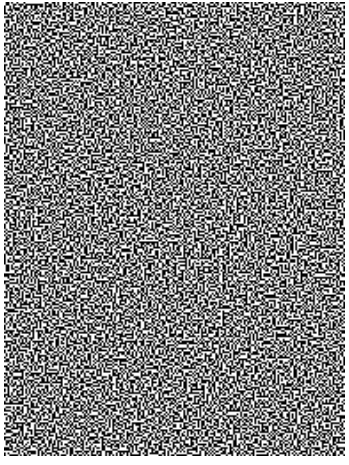


Photo chiffrée

Cryptographie visuelle (Naor & Shamir, 1994)

- Le réceptionniste (qui était effectivement un espion ennemi) n'a que le fax
- Il peut alors essayer de deviner une clé valide



Mauvaise clé

+

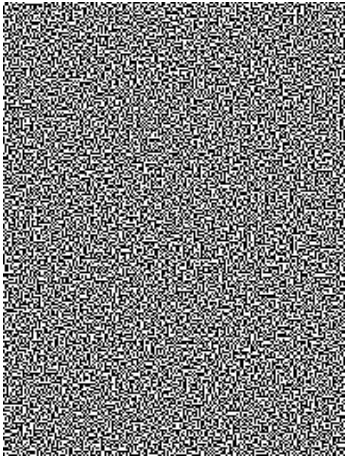


Photo chiffrée

=

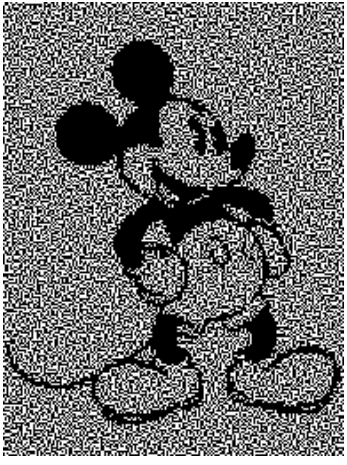


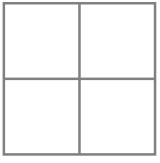
Photo déchiffrée

- Mais cela est aussi difficile que de deviner la photo originale

Comment ça marche ?

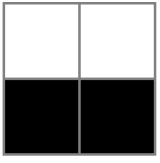
Comment ça marche ?

- La clé et la photo chiffrée sont composées uniquement de
  - blocs de 2×2 pixels



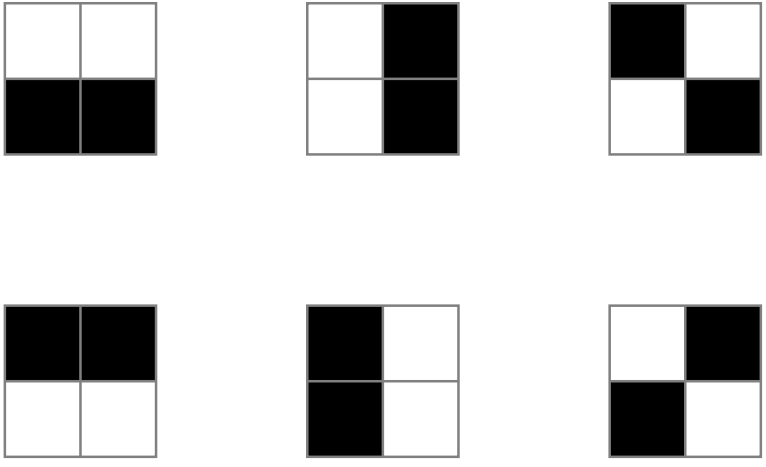
Comment ça marche ?

- La clé et la photo chiffrée sont composées uniquement de
  - blocs de 2×2 pixels
  - avec exactement 2 pixels noirs et 2 pixels blancs (transparents)



Comment ça marche ?

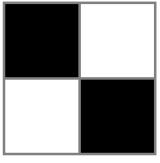
- La clé et la photo chiffrée sont composées uniquement de
  - blocs de 2×2 pixels
  - avec exactement 2 pixels noirs et 2 pixels blancs (transparents)
- Il y a 6 blocs possibles



Comment ça marche ?

Comment ça marche ?

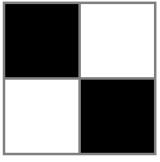
- Pour chaque bloc de la clé, le bloc correspondant de la photo chiffrée est



Clé

Comment ça marche ?

- Pour chaque bloc de la clé, le bloc correspondant de la photo chiffrée est
  - soit identique



Clé

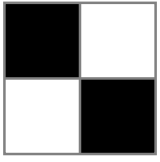
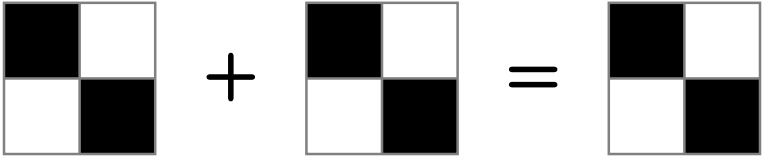


Photo chiffrée
(bloc identique)

Comment ça marche ?

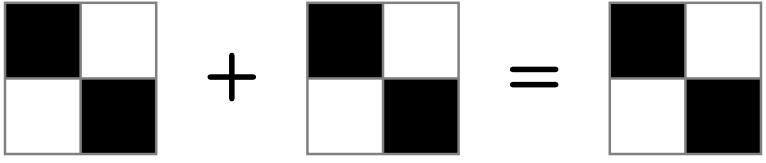
- Pour chaque bloc de la clé, le bloc correspondant de la photo chiffrée est
  - soit identique ⇒ bloc gris (mi-noir, mi-blanc)



Clé + Photo chiffrée (bloc identique) = Résultat

Comment ça marche ?

- Pour chaque bloc de la clé, le bloc correspondant de la photo chiffrée est
  - soit identique ⇒ bloc gris (mi-noir, mi-blanc)
  - soit complémentaire

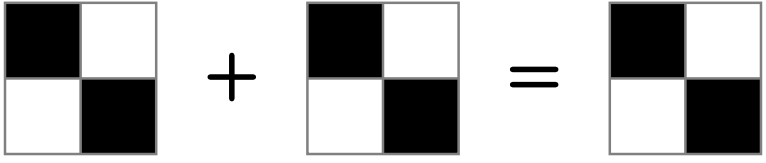


Clé + Photo chiffrée (bloc identique) = Résultat

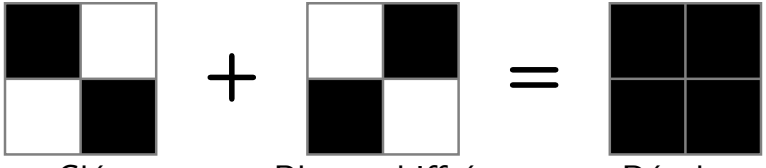
Clé Photo chiffrée (bloc complémentaire)

Comment ça marche ?

- Pour chaque bloc de la clé, le bloc correspondant de la photo chiffrée est
  - soit identique ⇒ bloc gris (mi-noir, mi-blanc)
  - soit complémentaire ⇒ bloc noir



Clé + Photo chiffrée (bloc identique) = Résultat



Clé + Photo chiffrée (bloc complémentaire) = Résultat

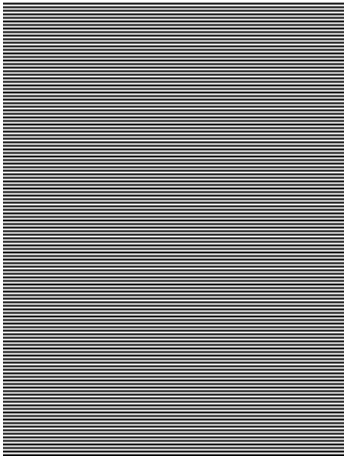
Attention au choix de la clé

Attention au choix de la clé

- La clé doit être choisie **aléatoirement** : chaque bloc choisi **au hasard**

Attention au choix de la clé

- La clé doit être choisie **aléatoirement** : chaque bloc choisi **au hasard**

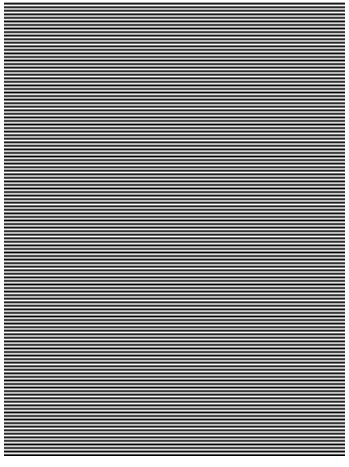


Clé uniforme

Photo N&B

Attention au choix de la clé

- La clé doit être choisie **aléatoirement** : chaque bloc choisi **au hasard**



Clé uniforme

Photo N&B

$\Rightarrow$

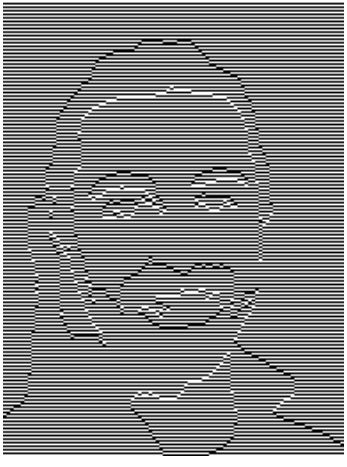


Photo chiffrée

Cryptographie

Cryptographie

Science de la **protection des messages**

Cryptographie

Science de la **protection des messages**

- La cryptographie permet d'assurer

Cryptographie

Science de la **protection des messages**

- La cryptographie permet d'assurer
  - la confidentialité (qui peut lire le message)

Cryptographie

Science de la **protection des messages**

- La cryptographie permet d'assurer
  - la confidentialité (qui peut lire le message)
  - l'authenticité (qui a envoyé le message)

Cryptographie

Science de la **protection des messages**

- La cryptographie permet d'assurer
  - la confidentialité (qui peut lire le message)
  - l'authenticité (qui a envoyé le message)

- On l'utilise tous les jours

Cryptographie

Science de la **protection des messages**

- La cryptographie permet d'assurer
  - la confidentialité (qui peut lire le message)
  - l'authenticité (qui a envoyé le message)

- On l'utilise tous les jours
  - dans nos téléphones portables

Cryptographie

Science de la **protection des messages**

- La cryptographie permet d'assurer
  - la confidentialité (qui peut lire le message)
  - l'authenticité (qui a envoyé le message)

- On l'utilise tous les jours
  - dans nos téléphones portables
  - dans les cartes bancaires

Cryptographie

Science de la **protection des messages**

- La cryptographie permet d'assurer
  - la confidentialité (qui peut lire le message)
  - l'authenticité (qui a envoyé le message)

- On l'utilise tous les jours
  - dans nos téléphones portables
  - dans les cartes bancaires
  - sur Internet `https://mail.google.com/`

Cryptographie

Science de la **protection des messages**

- La cryptographie permet d'assurer
  - la confidentialité (qui peut lire le message)
  - l'authenticité (qui a envoyé le message)

- On l'utilise tous les jours
  - dans nos téléphones portables
  - dans les cartes bancaires
  - sur Internet `https://mail.google.com/`
  - ...