Pourquoi a-t-on besoin de sécurité sur Internet ?

- Usurpation d'identité
- Atteinte à l'image ou à la réputation
- Disparition
- Responsabilités juridiques

La sécurité et vous ?

- Comment ai-je choisi mon mot de passe ?
- Mes logiciels sont-ils à jour ?
- Qui utilise mes machines ?
- Ai-je des récentes sauvegardes a ma disposition ?
- A quel réseau me suis je connecté ?
- Portable-Smartphone-Tablette même combat ?
- Ai-je confiance en ma messagerie ?
- Qu'elles sont mes sources logicielles ?
- Paiement sûr ?
- Usages personnels ou professionnels ?
- Comment sont gérées mes données privées ?

Institutions

Réglementations et normes

- **ANSSI** : *Agence Nationale de Sécurité des Systèmes d'Informations*
- **CNIL** : *Commission Nationale de l'Informatique et des Libertés*
- **OWASP** : *Open Web Application Security Project*

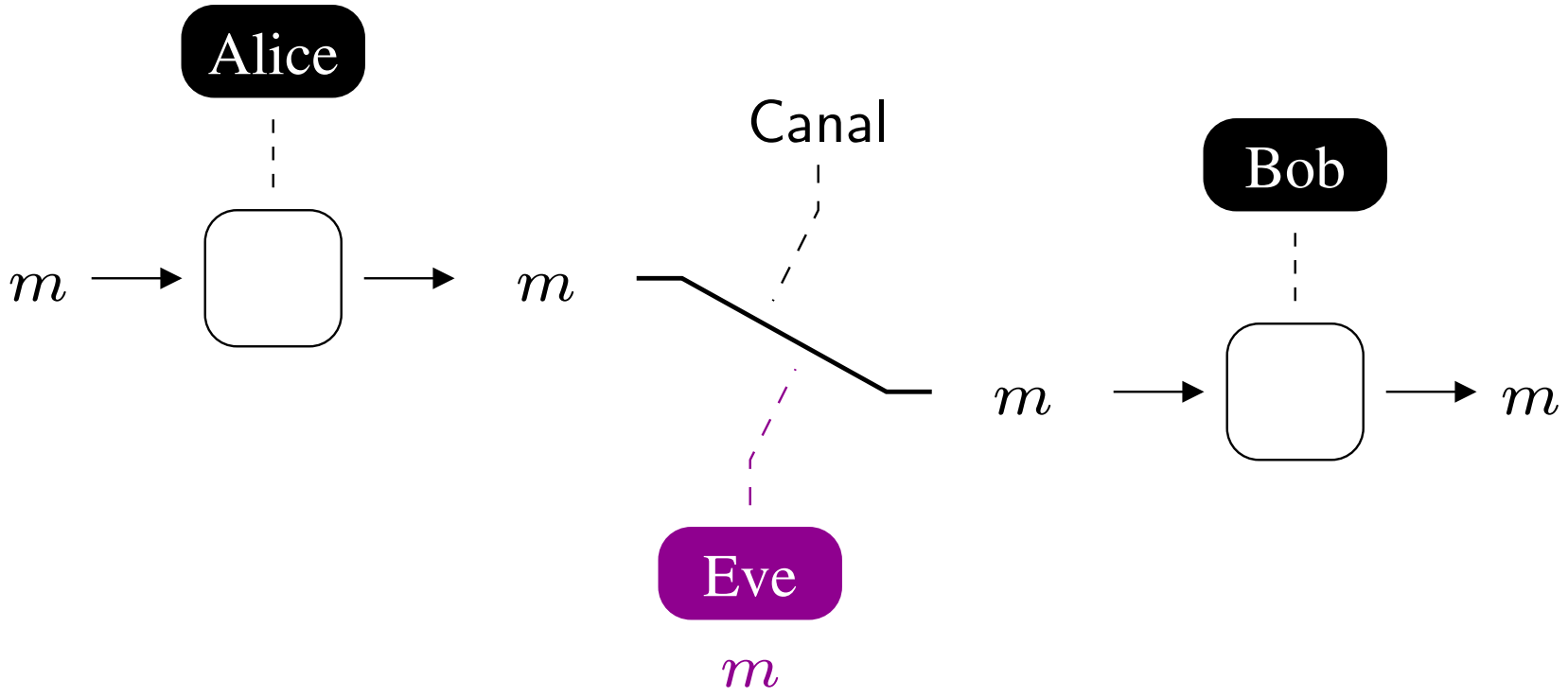
Briques de base en sécurité

- **Confidentialité :** empêcher un attaquant de connaître le contenu des communications.

- **Intégrité :** empêcher la manipulation des données par un attaquant.

- **Accessibilité :** un attaquant ne peut pas monopoliser les ressources afin d'empêcher les autres utilisateurs d'accéder aux services.
- Confidentialité et intégrité = Cryptographie

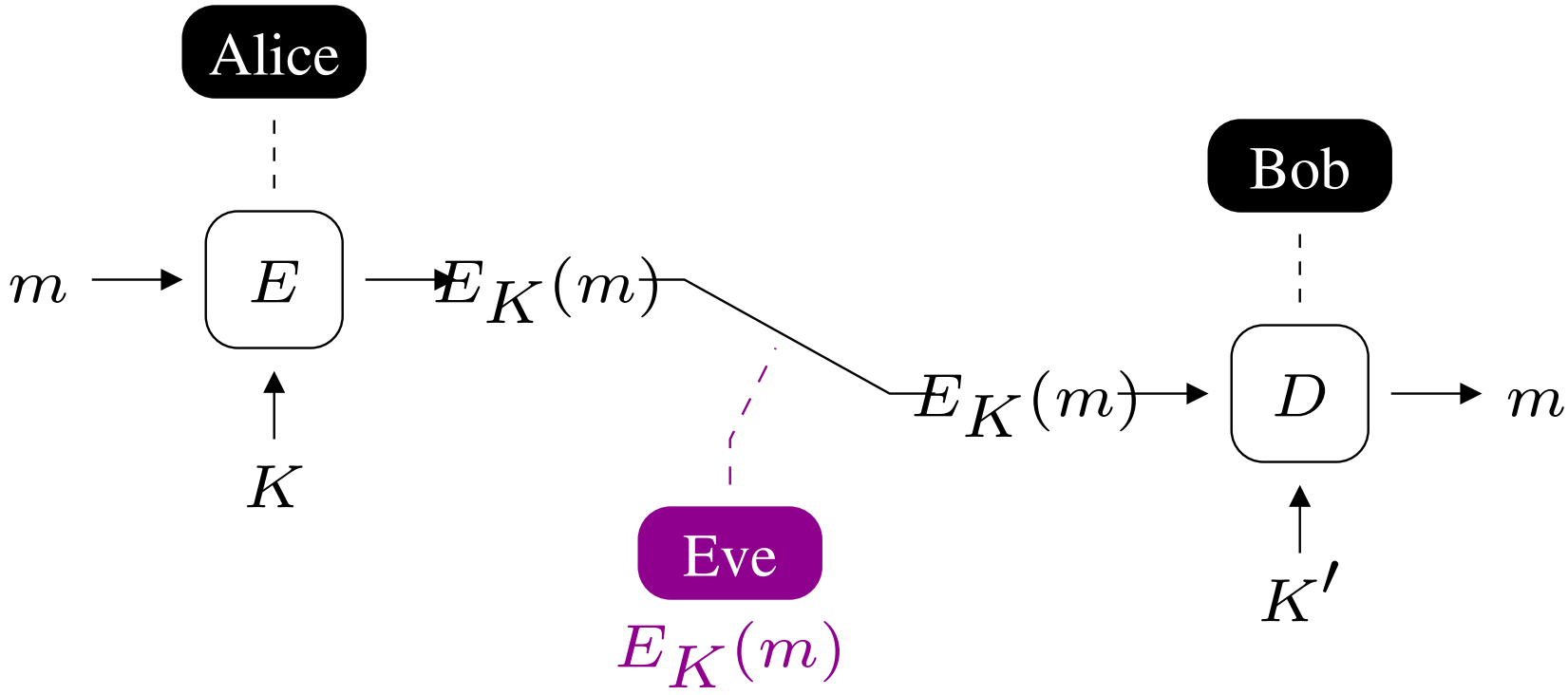
Confidentialité



- Comment préserver la confidentialité des messages entre Alice et Bob ?

Solution

Chiffrement



Chiffrement

- E est un **algorithme de chiffrement** : $c = E_K(m)$;
- D est un **algorithme de déchiffrement** : $m = D_{K'}(c)$;
- K est la **clef de chiffrement** (Alice) ;
- K' est la **clef de déchiffrement** (Bob).
- m est le texte clair ;
- c est le texte chiffré (ou simplement chiffré).

Symétrique ou asymétrique

- $K = K'$, on parle de **chiffrement symétrique** :
  - ◇ Alice et Bob doivent échanger la clef K ;
  - ◇ Il y a autant de clefs que de correspondants pour Bob.
- $K \neq K'$, on parle de **chiffrement asymétrique** :
  - ◇ K est la clef publique de Bob ;
  - ◇ K' est la clef secrète de Bob ;
  - ◇ La clef K est commune a tous les correspondants de Bob ;
  - ◇ Une autorité de confiance certifie $(K,\ \mathrm{Bob})$;

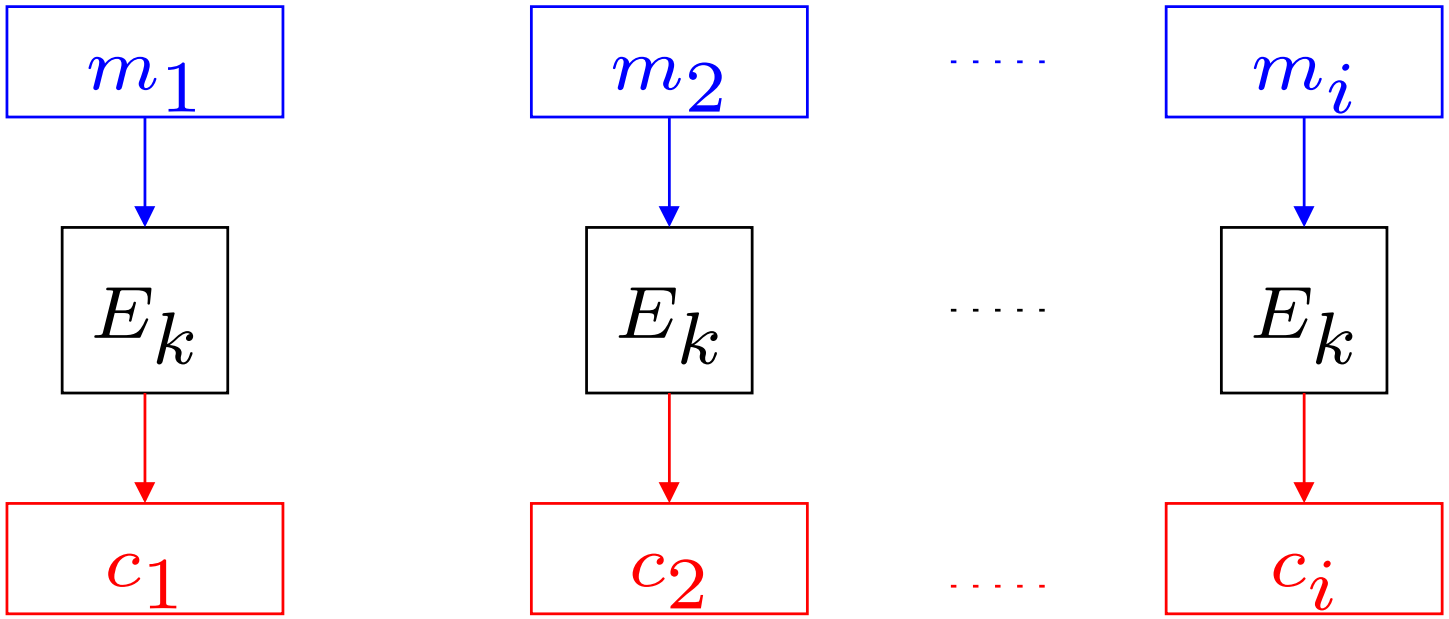
Principe

- La sécurité d'un système de chiffrement repose uniquement sur le secret de la clef. . .
- . . . et jamais sur le secret de l'algorithme.

Standard pour le chiffrement

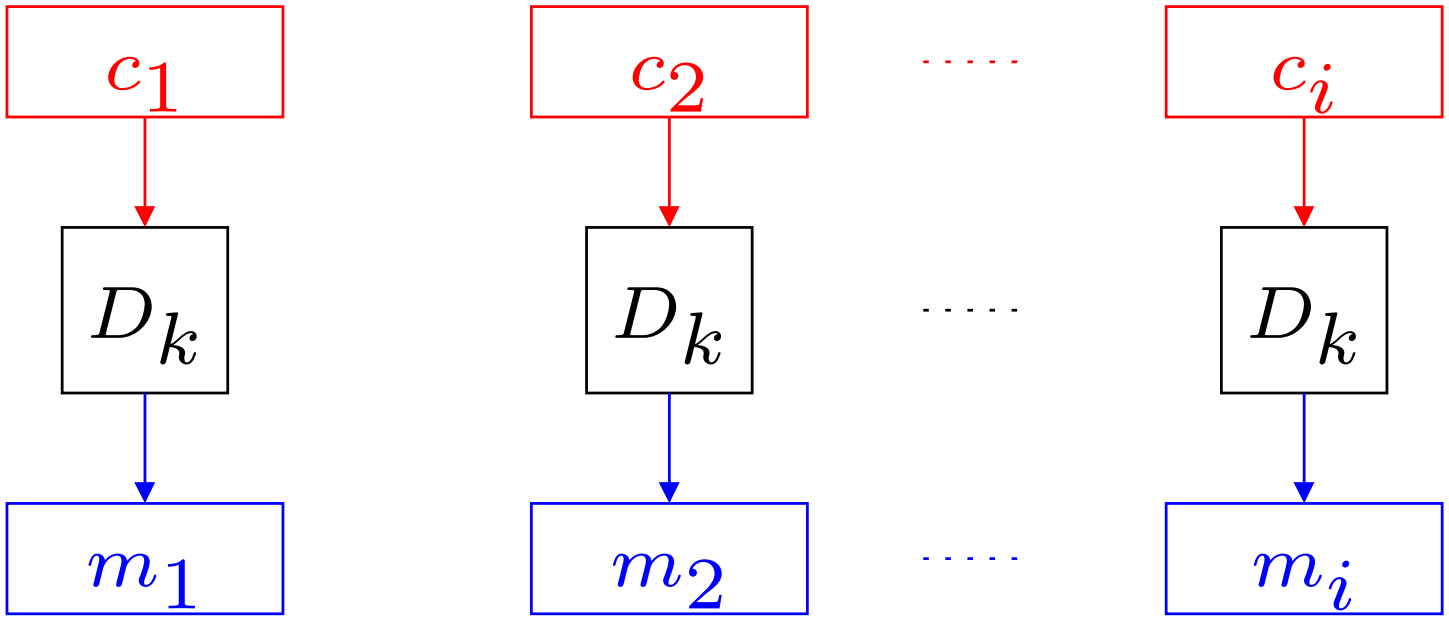
- **Symétrique : AES**
  - publié en 2001.
  - taille des blocs est de 128 bits (16 octets).
  - $\ell = 128$ bits (16 octets).
- **Asymétrique : RSA et courbes elliptiques**
  - publié en 1977 et 1985.
  - $\ell = 2048$ bits et 256 bits.

Electronic CodeBook (ECB)



Chiffrement

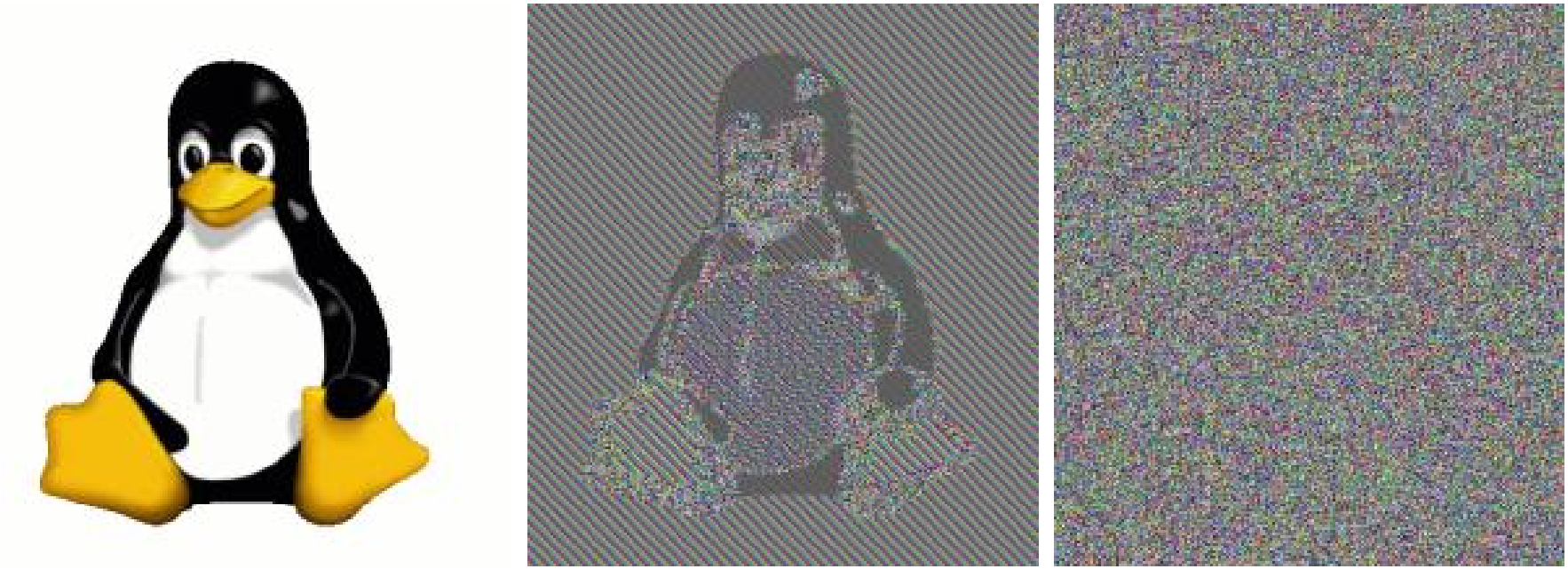
Electronic CodeBook (ECB)



Déchiffrement

Resultat

Source : Wikipedia



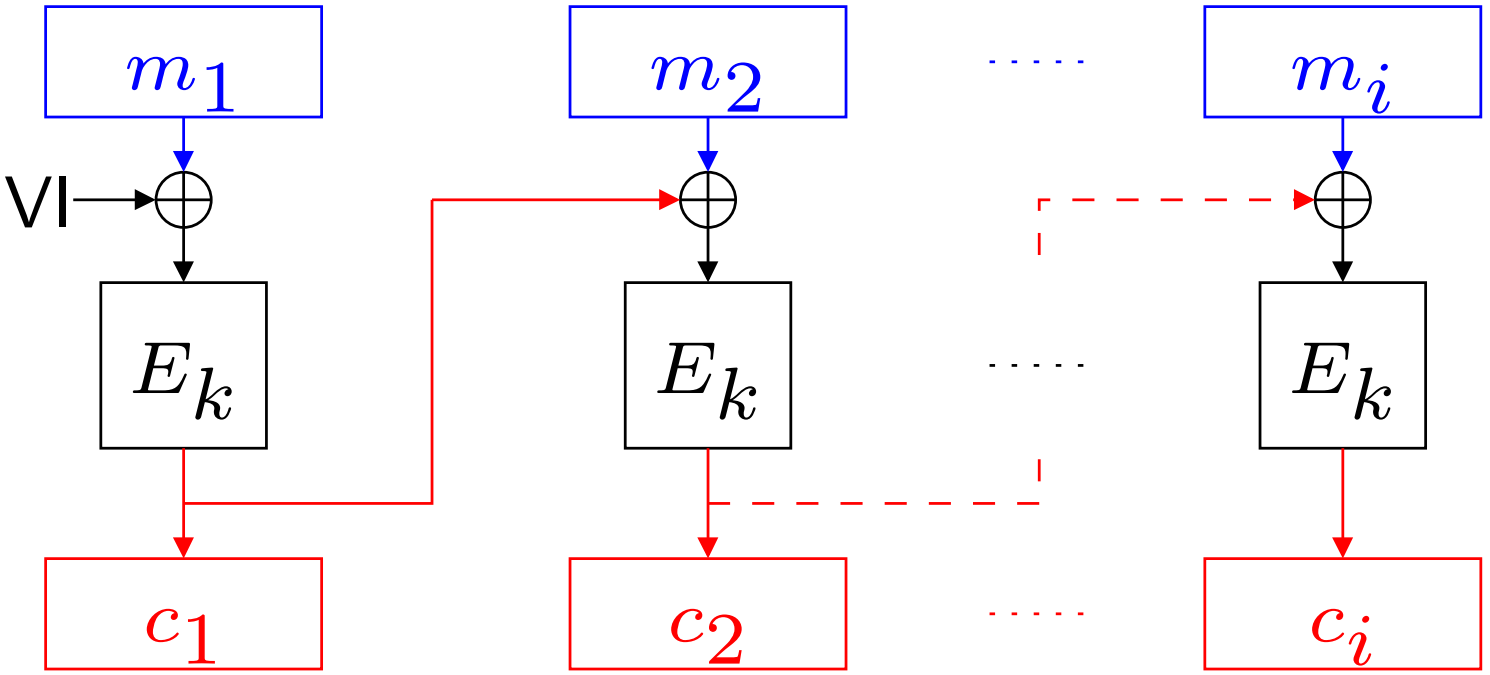
- Le mode ECB ne permet pas de cacher la structure des données qui sont chiffrées !

Chiffrement rendu aléatoire

- On introduit un $nonce$ dans le chiffrement. **Comment implémenter un $nonce$?**
  - avec un compteur ;
  - avec un $timestamp$;
  - avec un nombre aléatoire ;
  - combinaison des 3 précédents.

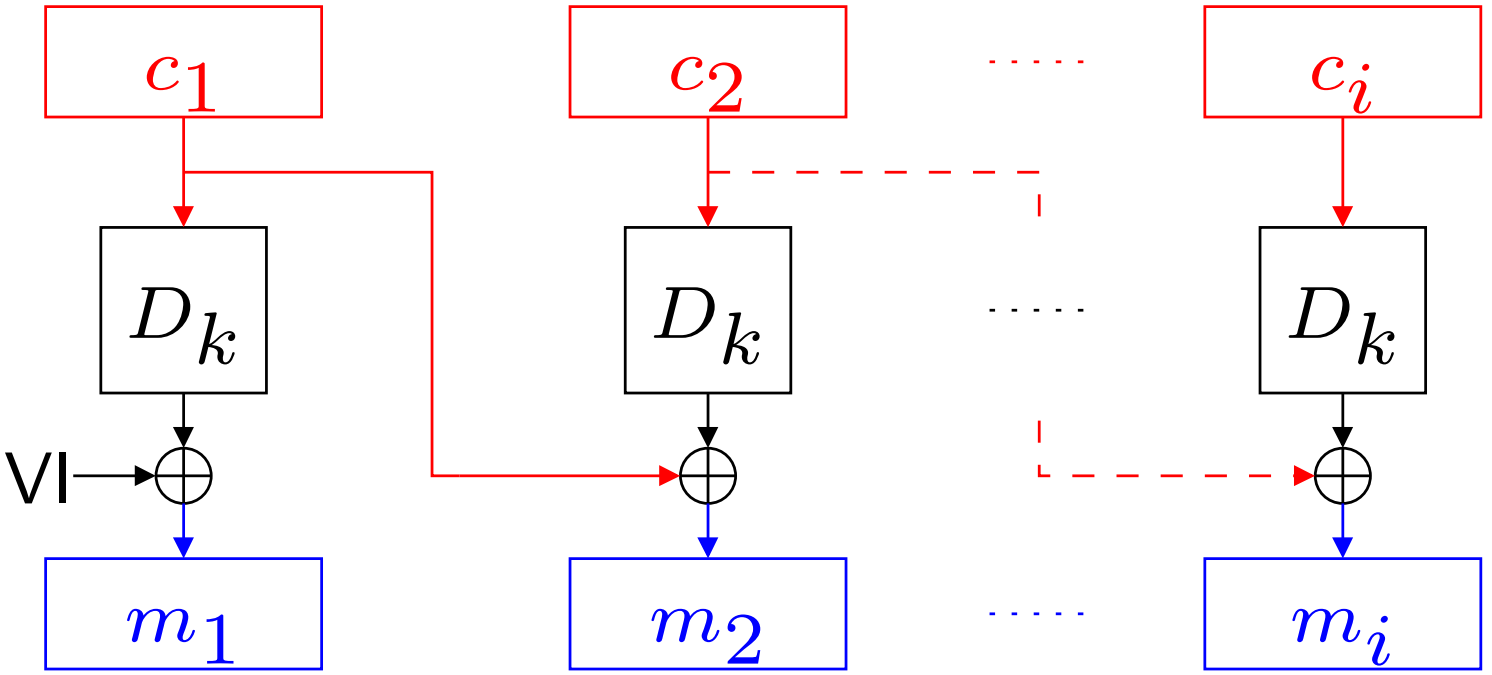
- **Comment introduire l'aléa ?**

Cipher-Block Chaining (CBC)



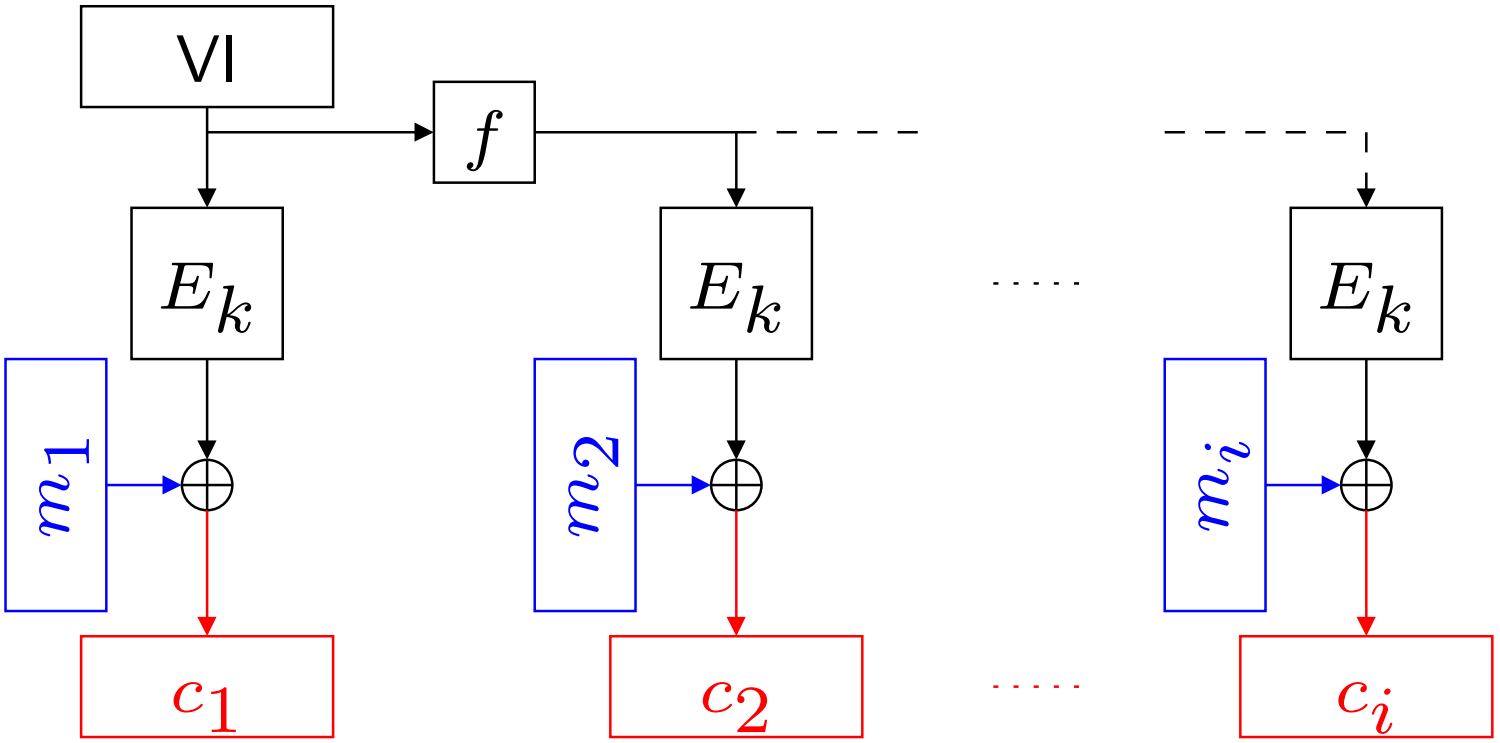
Chiffrement

Cipher-Block Chaining (CBC)



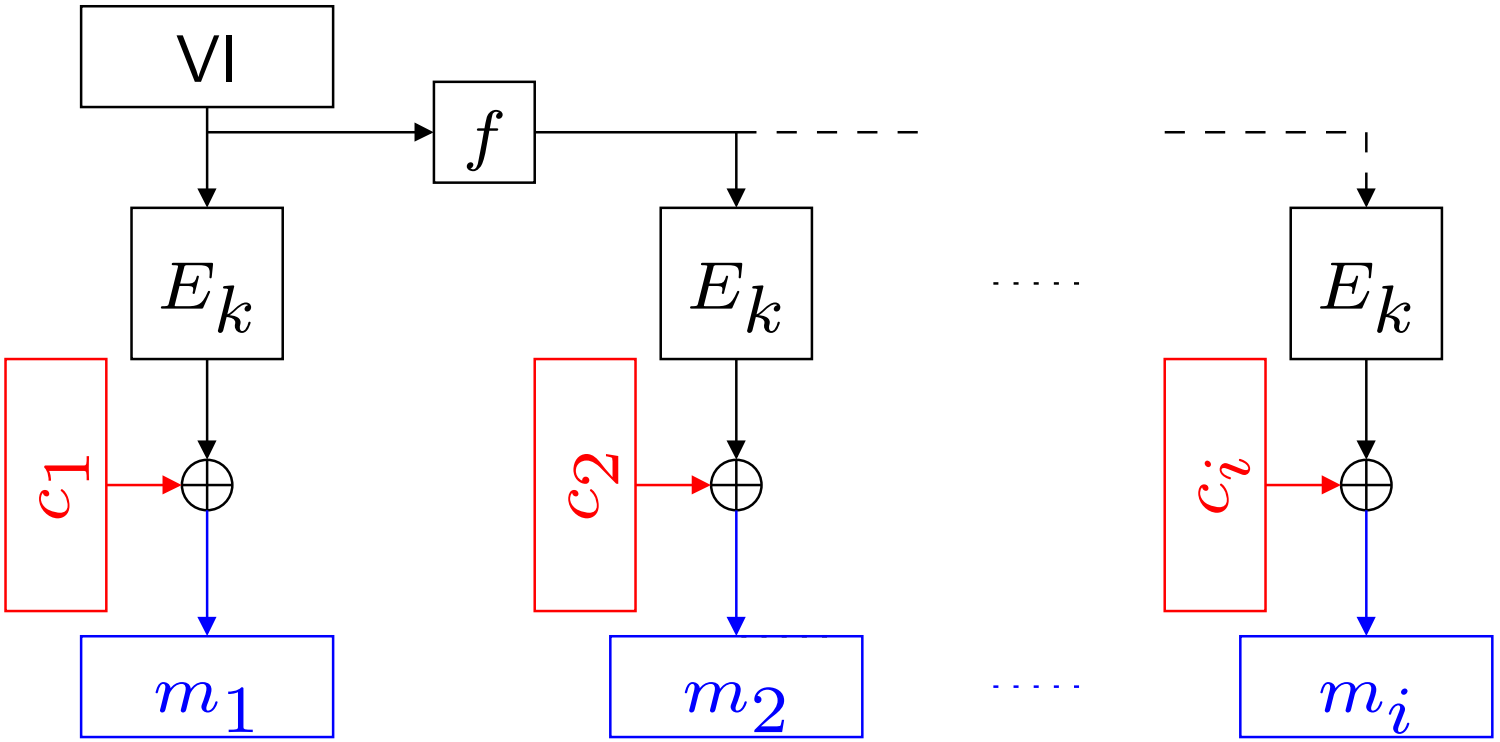
Déchiffrement

CounTeR (CTR)



Chiffrement

CounTeR (CTR)



Déchiffrement

Intégrité=Hachage

- **Applications** :
  — Intégrité.
  — Authentification.
  — Création d'identifiant et mot de passe.

- **Définitions et propriétés** :
  — Paradoxe des anniversaires.
  — Rré-image, 2^{eme} pré-image et collisions.

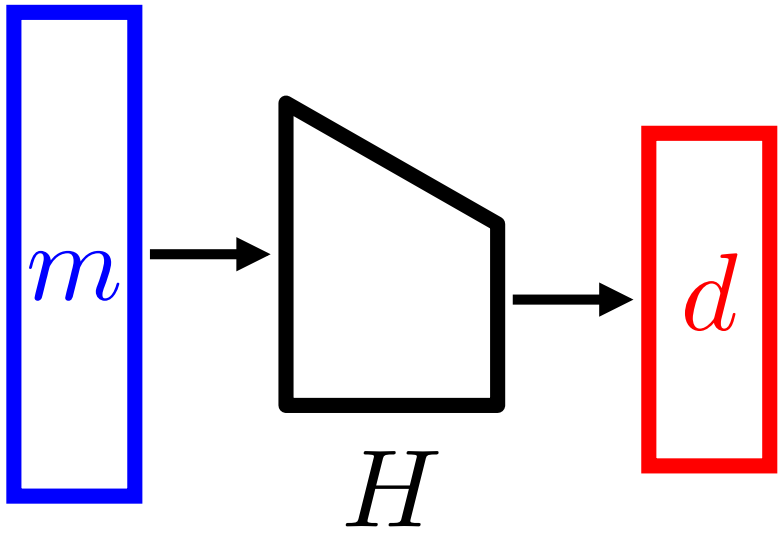
- **Exemples** :
  — MAC.

Hachage

Définition. *Une fonction de hachage H a les propriétés suivantes :*

— *H est facilement calculable.*

— $H : \{0,1\}^\star \to \{0,1\}^\ell$.

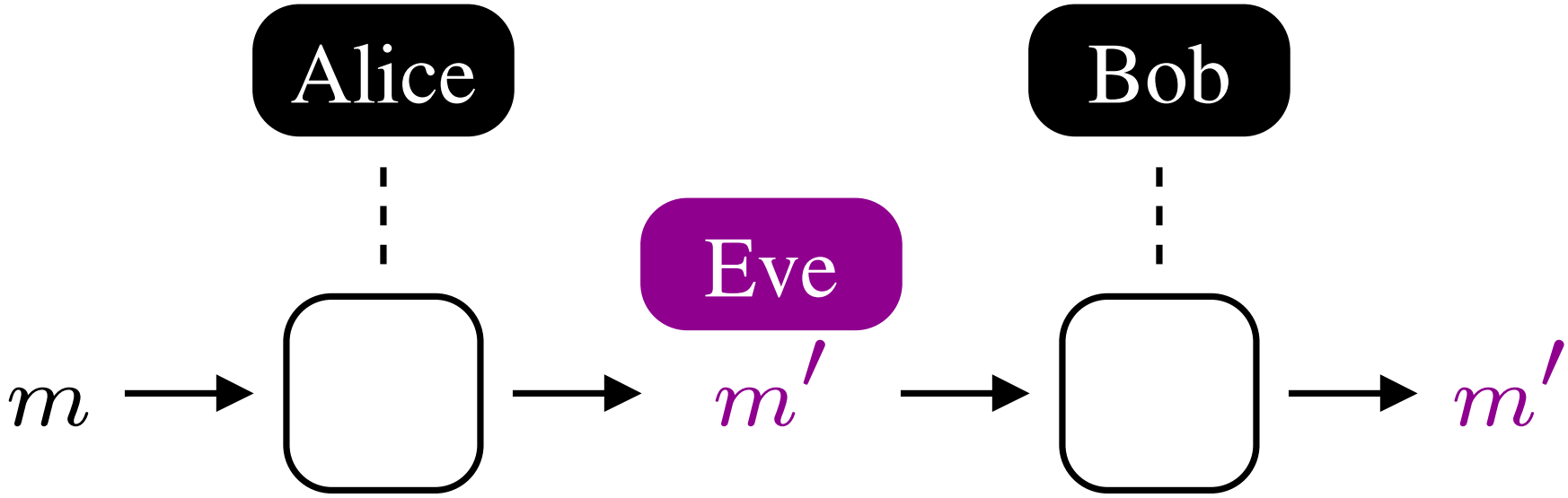


Termes

- m est un message de $longueur\ arbitraire$
- d est le condensée (ou empreinte).
- Si on trouve $x \neq x'$ tel que $H(x) = H(x')$, alors on parle de collision entre x et x'.
- Il existe $toujours\ des\ collisions$ pour une fonction de hachage.

Applications en sécurité

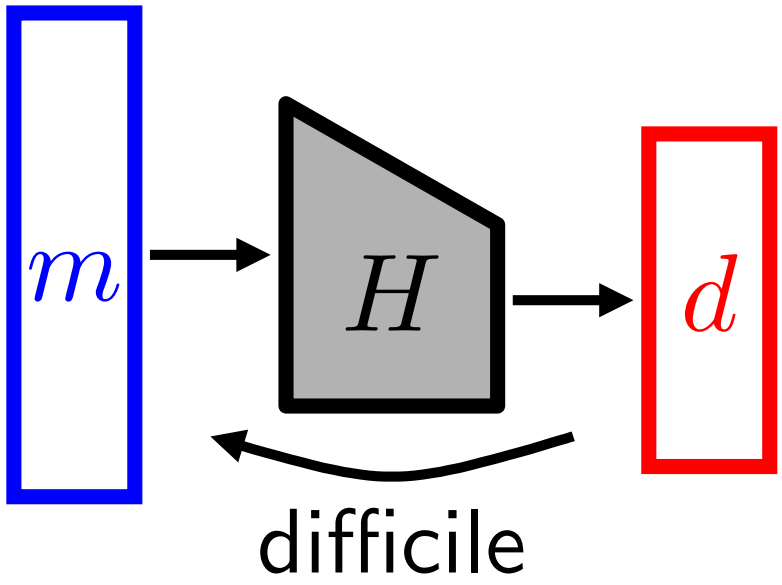
Intégrité



- Alice et Bob veulent *détecter les modification* d'Eve.
- **Solution** : hachage cryptographique + canal sécurisé.

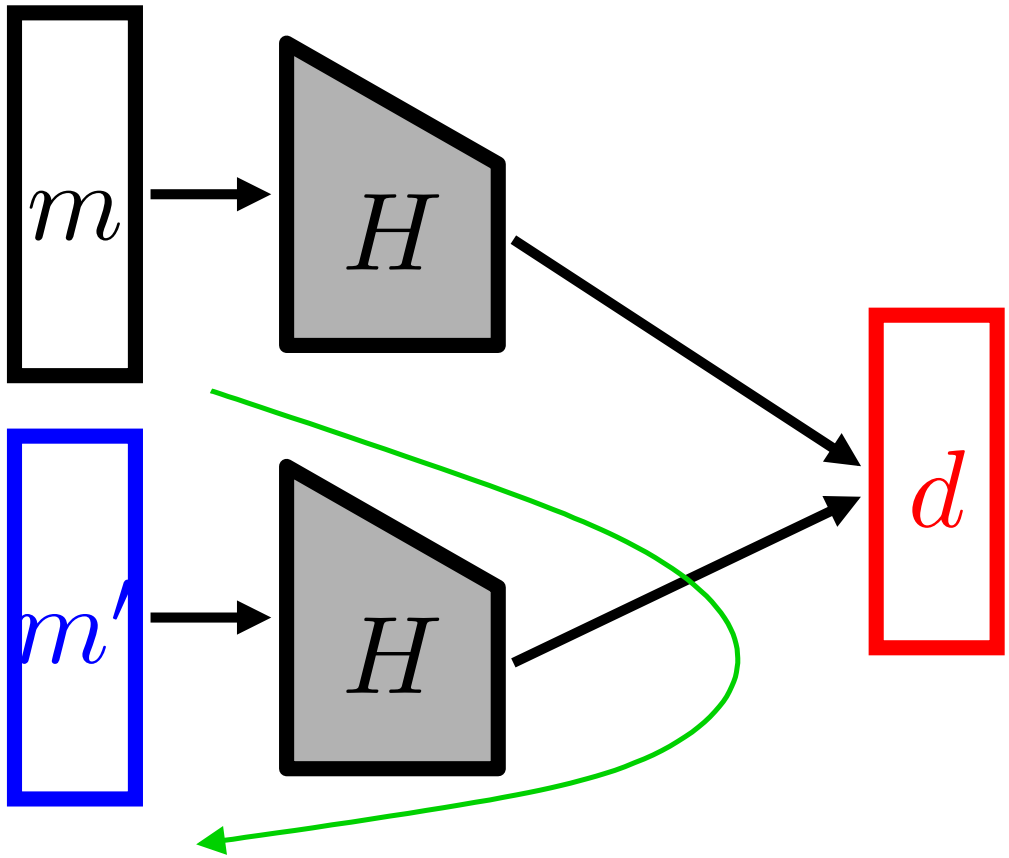
Pré-image

- Etant donné $d = H(m)$, retrouver m.
- 2^ℓ calculs de condensé pour retrouver m.



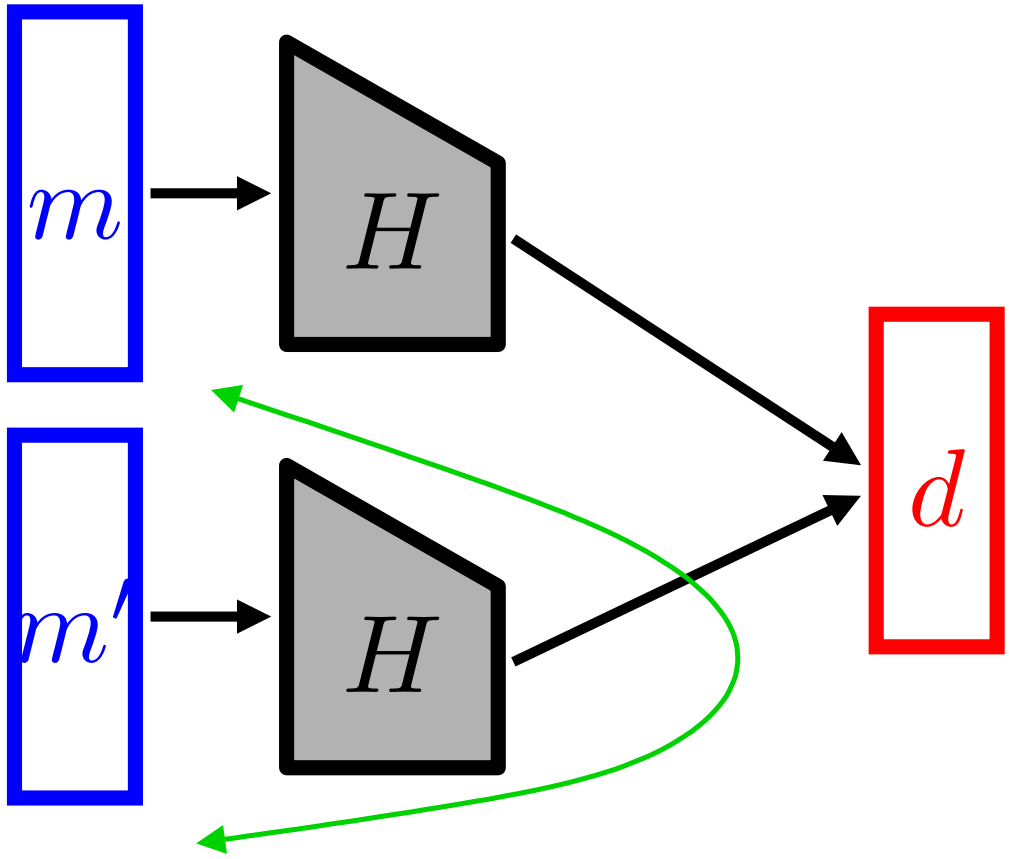
$2^{\text{ème}}$ Pré-image

- Etant donné m, trouver m' tel que $H(m) = H(m')$.
- 2^{ℓ} calculs de condensé pour trouver m'.



Collision

- Trouver m et m' tel que $H(m) = H(m')$.
- $2^{\ell/2}$ calculs de condensé pour trouver une collision.



Classification

- **Fonction de hachage à sens unique :**
  — Résistance à la pré-image.
  — Résistance à $2^{\text{ème}}$ pré-image.

- **Fonction de hachage résistante aux collisions :**
  — Résistance à $2^{\text{ème}}$ pré-image.
  — Résistance aux collisions.

Paradoxe des anniversaires

Définition 1. *Dans une assemblée de 23 personnes, la probabilité qu'au-moins 2 d'entre-elles aient leur anniversaire le même jour est supérieure à* $\frac{1}{2}$.

- **Problème général** : on tire k valeurs aléatoires de ℓ bits ($n = 2^\ell$). Qu'elle est la probabilité d'avoir au moins une collision ?

Paradoxe des anniversaires

- Soit P_k la probabilité d'avoir des tirages tous $\neq$.

$$\begin{aligned} P_2 &= \frac{n-1}{n}, \\ P_3 &= \left(\frac{n-1}{n}\right) \cdot \left(\frac{n-2}{n}\right), \\ P_k &= \left(\frac{n-1}{n}\right) \cdot \left(\frac{n-2}{n}\right) \cdots \left(\frac{n-k+1}{n}\right). \end{aligned}$$

- On a :

$$P_k = \prod_{i=1}^{k} \left(1 - \frac{i}{n}\right).$$

Paradoxe des anniversaires

- La probabilité d'avoir au moins une collision :

$$1 - P_k = 1 - \prod_{i=1}^{k} \left(1 - \frac{i}{n}\right).$$

- On a : $1 - P_k \approx 1 - e^{\frac{k(k-1)}{2n}}$.
- On a : $k \approx \sqrt{2n \cdot \ln\left(\frac{1}{1-P_k}\right)}$.
- **On retiendra que si $k > 2^{\ell/2}$ alors $1 - P_k > \frac{1}{2}$.**