Introduction à la Cryptographie

BUT Informatique

Présentation

Ce module est une introduction à la cryptographie dont il s'agit de présenter différentes techniques.

Présentation

- Rappels d'arithmétique
- Cryptographie symétrique (César, Vigenère, Hill, AES)
- Cryptographie asymétrique (Chiffrement RSA, Diffie-Hellman, El Gamal)

Présentation

Évaluation

- Examen final semaine du 20 janvier (2h)
- Une partie sous forme de QCM.
- Une partie sous forme d'exercices à résoudre.

La cryptologie, cryptographie, cryptanalyse I

Définition :

La *cryptologie* (étymologiquement la *science du secret*) englobe la cryptographie ET la cryptanalyse.

- La **cryptographie** est l'ensemble des principes et méthodes dont l'application assure le *chiffrement* et le *déchiffrement* des données, afin d'en préserver la confidentialité, l'intégrité, l'authenticité et la non-répudiation.
- La **cryptanalyse** est l'ensemble des techniques utilisées pour tenter de retrouver un message chiffré sans posséder la clé de déchiffrement.

Où se trouve la cryptographie?

Armée, banque, console de jeux, vote électronique, paiement en ligne, ...

La cryptologie, cryptographie, cryptanalyse II

Objectifs de la cryptographie

- **Confidentialité** : le contenu du message chiffré ne peut être lu par une tierce personne (non destinataire).
- **Intégrité** : garantie le contenu du message reçu. Le message n'a pas été modifié durant sa transmission par un tiers.
- **Authenticité** : garantie l'identité de l'émetteur. Pas d'usurpation d'identité.
- **Non-répudiation** : l'émetteur ne doit pas pouvoir nier l'envoi du message.

La cryptologie, cryptographie, cryptanalyse III

Terminologie

- L'**émetteur** désire envoyer un message.
- Le **récepteur** le reçoit.
- Le message passe par un **canal de transmission** public.
- Le **message clair** est le message original.
- Une méthode de **chiffrement** est utilisée pour dissimuler le contenu.
- Ce qui donne un **message chiffré**.
- Une méthode de **déchiffrement** est utilisée pour retrouver le contenu.
- Les protagonistes utilisent une **clé** de chiffrement/déchiffrement.

Cryptosystème

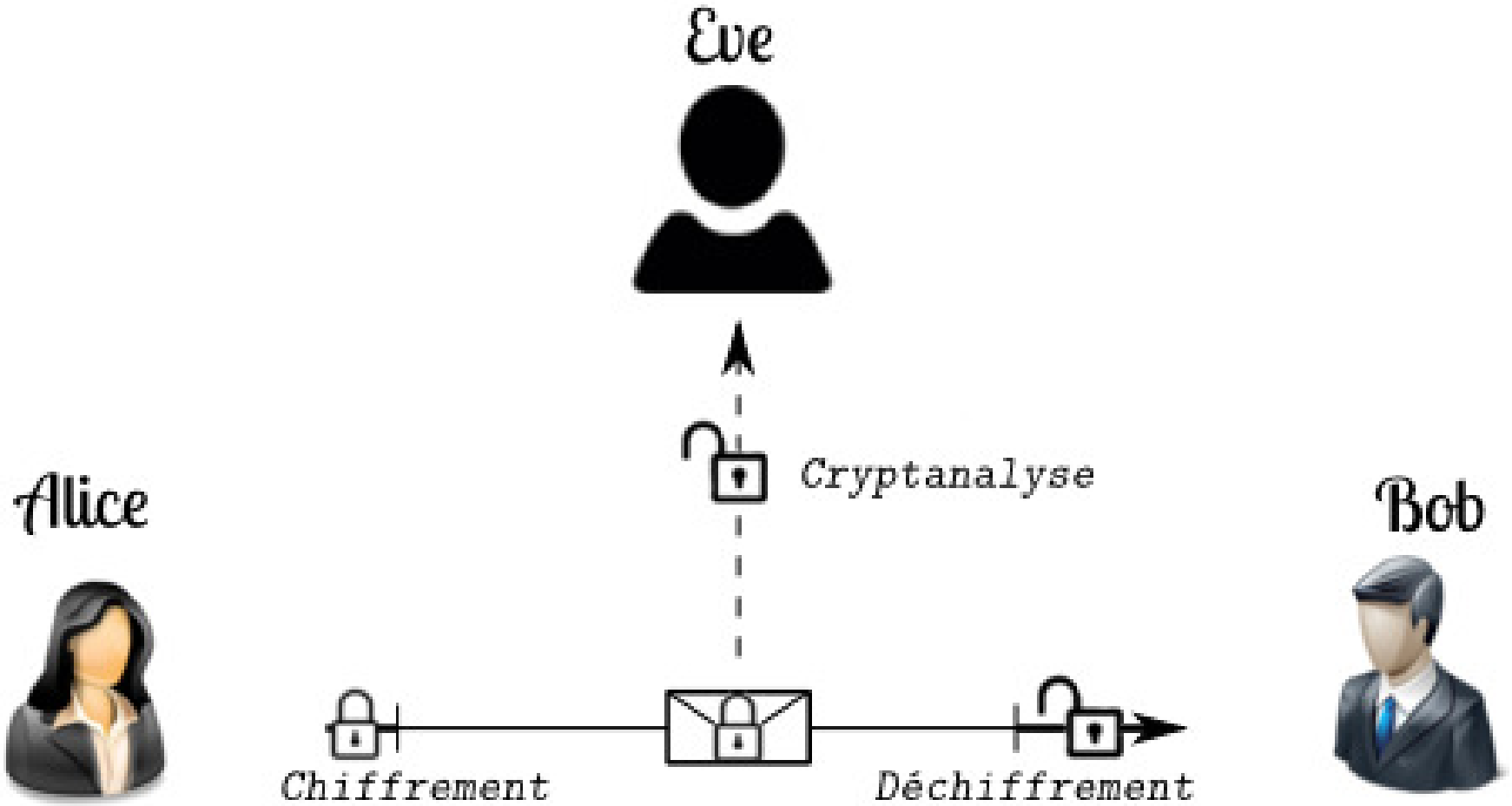
Définition

Un *cryptosystème* est un ensemble $\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}$ tel que:

- $\mathcal{P}$: espace des messages clairs,
- $\mathcal{C}$: espace des messages chiffrés,
- $\mathcal{K}$: espace des clés,
- $\mathcal{E}$: les fonctions de chiffrement

  $ie : \mathcal{E} = \{E_k, k \in \mathcal{K}\}$ avec $E_k : \mathcal{P} \to \mathcal{C}$
- $\mathcal{D}$: les fonctions de déchiffrement

  $ie : \mathcal{D} = \{D_k, k \in \mathcal{K}\}$ avec $D_k : \mathcal{C} \to \mathcal{P}$
- Chaque clé $e \in \mathcal{K}$ est associée une clé $d \in \mathcal{K}$ telle que $D_d(E_e(m)) = m$.


Eve
Cryptanalyse
Alice
Bob
Chiffrement
Déchiffrement

Cryptanalyse I

Définition

L'*attaquant* est celui qui cherche à obtenir des informations protégées qui ne lui sont pas destinées.

Différents niveaux de connaissance pour l'attaquant

- Texte **chiffrés connus**:
  - connaît un ou plusieurs textes chiffrés c_i.
- Texte **clair connu**:
  - connaît plusieurs couples (m_i, c_i) fixées et c_{n+1}, avec $c_i = E_k(m_i)$ pour $i = 1, \ldots, n$.
- Texte **clair choisi**:
  - peut faire chiffrer autant de message qu'il désire.
- Texte **chiffré choisi**:
  - peut faire déchiffrer tous les textes chiffrés de son choix.

Principe de Kerchoffs (19ème siècle)

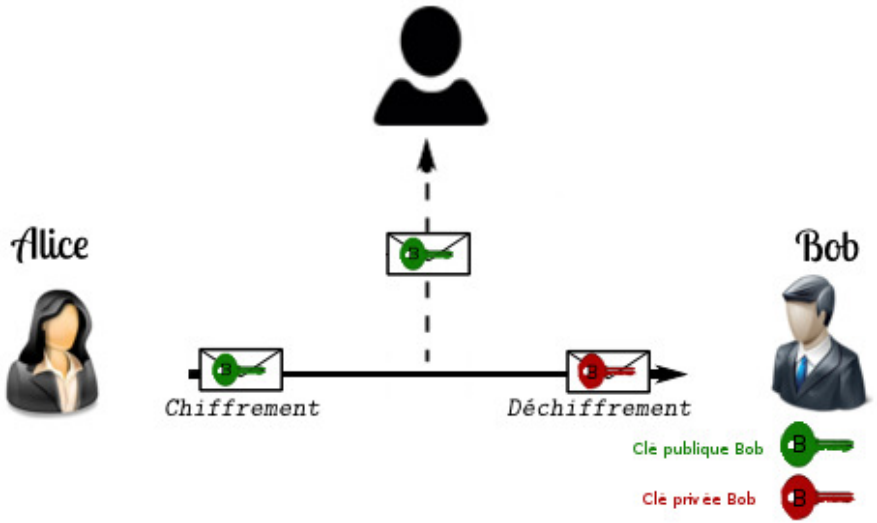
La sécurité d'un système de chiffrement ne doit résider que dans la clé et non dans le procédé de chiffrement.

Chiffrements symétriques

Chiffrement symétrique

- Alice et Bob partage la même clé,
- Deux familles de chiffrement symétriques : blocs et flot,
- Rapide,
- Mais :
  - Comment échanger la clé?
  - Une clé pour chaque correspondant.

Chiffrements asymétriques



Chiffrement asymétrique

- Alice et Bob ont respectivement 2 clés: k_{public} et k_{prive},
- Pas d'échange de clé préalable,
- Pas d'augmentation exponentielle du nombre de clé,
- Lent.

RSA - 1978 (Rivest, Shamir and Adleman) I

Cryptosystème basé sur le problème de factorisation des nombres.

Comment choisir les clés?

La clé privée : (p, q, d)

- Deux grands nombres premiers p et q,
- Un nombre d premier avec $(p-1)(q-1)$

La clé publique : (n, e)

- Calcul de $n = p \times q$
- Calcul de e l'inverse de d mod $(p-1)(q-1)$
  - $e \times d \equiv 1 \bmod (p-1)(q-1)$

RSA - 1978 (Rivest, Shamir and Adleman) II

Hypothèse : Bob veut envoyer un message m à Alice.

Chiffrement

- Bob récupère la clé publique d'Alice (n, e),
- Il calcule $c = m^e \bmod n$ où m est le message,
- Il envoie c à Alice.

Déchiffrement

- Alice reçoit c et calcule $c^d \bmod n$ pour retrouver m

Diffie-Hellman I

Cette technique permet de construire une clé entre Alice et Bob sans jamais la transmettre sur le réseau.

- On choisit un générateur g d'un groupe G qui peut être connu de tous.
- Alice tire au hasard un entier a et Bob tire au hasard un entier b.
- Alice envoie à Bob le nombre g^a, Bob envoie à Alice le nombre g^b.
- Alice et Bob peuvent tous deux calculer la clef $K = g^{ab}$, mais un adversaire qui intercepterait la communication ne pourrait pas le faire.

Diffie-Hellman II

Alice

Bob

- Un nombre aléatoire a
- Calcule : g^a
- Envoie du résultat à Bob

g^a →

← g^b

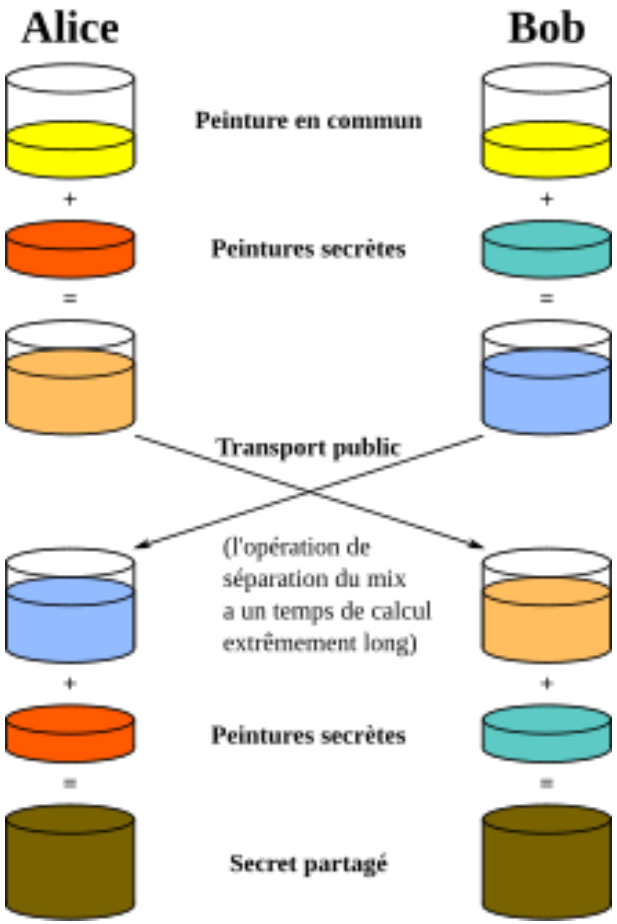
- Un nombre aléatoire b
- Calcule : g^b
- Envoie du résultat à Alice

- Réception de g^b
- Calcule de $g^{ab} = (g^b)^a$

- Réception de g^a
- Calcule de $g^{ab} = (g^a)^b$

Alice et Bob ont une clé secrete en commun

Diffie-Hellman III



Chiffrement El-Gamal I

Alice

Bob

Génération des clés :

- Un nombre aléatoire k_a
- Calcule : $K_a = g^{k_a}$
- Envoie du résultat à Bob

K_a →

Bob veut envoyer un message m

← (g^k, mK_a^k)

- Un nombre aléatoire k
- envoie : (g^k, mK_a^k)

- Reception de (g^k, mK_a^k)
- Calcule : $m = \frac{mK_a^k}{(g^k)^{k_a}}$

Chiffrement El-Gamal II

Paramètres publiques :

- un groupe G,
- un élément g de G d'ordre ℓ,

Remarques :

- $k_a \in [1, \ell - 1]$, c'est une clé privée,
- K_a est une clé publique,
- $k \in [1, \ell - 1]$ est une clé privée temporaire,
- Alice et Bob n'ont pas un rôle symétrique.