# TAN

05/10/2020

## Cryptographie

Concept d'un cryptosystème
- symétrique (< 1976)
- à clé publique
  - RSA
  - ElGamal

Définition. Un cryptosystème est un application (ou une famille d'applications):

$$\mathcal{E} : \mathcal{K} \times \mathcal{M} \longrightarrow \mathcal{C}$$

(et

$$\mathcal{D} : \mathcal{K} \times \mathcal{C} \longrightarrow \mathcal{M})$$

où

$\mathcal{K}$ = espace (= ensemble) de clés
$\mathcal{M}$ = espace de messages
$\mathcal{C}$ = espace de textes chiffrés.

N.B. espace = ensemble, équipé éventuellement d'une structure de probabilité (espace de proba).

On écrit $E_K = \mathcal{E}(K, \cdot) : \mathcal{M} \longrightarrow \mathcal{C}$,
et on peut identifier
$\mathcal{E}$ avec l'ensemble $\{K\} \times \mathcal{M}$
$\{E_K : \mathcal{M} \longrightarrow \mathcal{C} \mid K \in \mathcal{K}\}$.
L'appli $E_K$ s'appelle un chiffrement.
Pour continuer la définition...
L'application $\mathcal{E}$ est telle que

$$\mathcal{D}(K, \mathcal{E}(K, M)) = M. \quad (*)$$

En écrivant $D_K = \mathcal{D}(K, \cdot) : \mathcal{C} \to \mathcal{M}$,
on écrit $(*)$ comme :

$$D_K \circ E_K = id_{\mathcal{M}}.$$

L'appli $D_K$ s'appelle un déchiffrement.
De la même manière on peut identifier $\mathcal{D}$ avec

$$\{D_K : \mathcal{C} \longrightarrow \mathcal{M} \mid K \in \mathcal{K}\}$$

$\mathcal{K} \ni K \mapsto D_K$

Kerkhoff (fin du XIX$^e$)

Le principe de Kerk- (~1883)
hoff exprime que la sécurité d'un cryptosysteme ne doit se reposer que sur le secret de la clé.

Selon le principe de Kerkhoff, tous les autres paramètres sont supposés d'être publiquement connus $(\mathcal{K}, \mathcal{M}, \mathcal{C}, \mathcal{E}, \mathcal{D})$.
Formulation 20e: "Maxime de Shannon": "l'adversaire connaît le système".
Remarque: Souvent $\mathcal{M} = \mathcal{C}$, mais il sont distingués par leurs fonction de probabilités.
Un élément $M \in \mathcal{M}$ s'appelle un message ou texte clair.

## Cryptosystème asymétrique

Pareil, mais on distingue
$\mathcal{K}$ = espace de clés publiques
$\mathcal{K}'$ = espace de clés privées
avec fonctions
$\mathcal{E} : \mathcal{K} \times \mathcal{M} \longrightarrow \mathcal{C}$ et
$\mathcal{D} : \mathcal{K}' \times \mathcal{C} \longrightarrow \mathcal{M}$.

(1976) Introduit par Diffie & Hellman

On suppose l'existence d'une application $\chi \hookrightarrow \mathcal{K} \times \mathcal{K}'$ telle que (inclusion) $\chi = \{(K, K')\}$ $D_K \circ E_K = id_{\mathcal{M}}$
pour couple $(K, K') \in \chi$.

1976 : Échange de clé de Diffie-Hellman

1977 : Rivest-Shamir-Adelman = protocole RSA

1985 : Cryptosystème de ElGamal

Protocoles

Échange de clé de Diffie-Hellman

- A (= Alice) et B (= Bob) choisissent un premier $p$ et un élément primitif $a \in \mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$.

Défn Un élément primitif de $\mathbb{F}_p^*$ est un générateur.

Donnée $\langle a \rangle = \{a^0, a^1, \dots\} = \mathbb{F}_p^*$ (publique)

- A choisit $x \in \mathbb{Z}/(p-1)\mathbb{Z}$ et calcule $c = a^x$.
- B choisit $y \in \mathbb{Z}/(p-1)\mathbb{Z}$ et calcule $b = a^y$

- A envoie $c$ à B. (publique)
- B envoie $b$ à A. (publique)
- A et B calculent $a^{xy}$ :

$$a^{xy} = b^x = c^y.$$

(Alice) (Bob)

Le résultat est un secret commun

Échange de clé (ou établissement de clé) permet de déterminer/établir un secret commun. Ce secret s'utilise pour déterminer une clé secrète, utilisé dans un cryptosystème symétrique (ou classique <1976). Cela donne la motivation d'étudier deux problèmes computionnels:

Problème de Diffie Hellman (DHP)
Soit donnés $a, a^x, a^y$ ($a \in \mathbb{F}_p^*$), déterminer $a^{xy} \in \mathbb{F}_p^*$.
N.B. Pas évident, $a^x a^y = a^{x+y} \neq a^{xy}$.

Problème du log discret (DLP)
Soit donnés $a, a^x$ ($a \in \mathbb{F}_p^*$), déterminer $x \in \mathbb{Z}/(p-1)\mathbb{Z}$.
N.B. Une solution (= algorithme) du DLP implique une solution du DHP.
En général on ne connaît pas de meilleur algo pour le DHP.

Problème: DDH = "decision Diffie-Hellman":
Soit donnés $a, a^x, a^y, a^z$ dans $\mathbb{F}_p^* = \langle a \rangle$. Déterminer si $a^{xy} = a^z$.
N.B. Il n'est pas évident à vérifier si une réponse au DHP est correcte.

RSA (1977)

Protocole pour envoyer un message de A à B, avec la connaissance de la clé publique $(n,e)$ de B.
Remarque. Bob construit sa clé publique $(n,e)$ et sa clé privée $(n,d)$ à partir d'un couple $(p,q) \in \mathcal{X} = \mathcal{P} \times \mathcal{P}$, où $\mathcal{P}$ = premiers. Alors le couple $((n,e),(n,d)) \in \mathcal{K} \times \mathcal{K}'$ est déterminé par $(p,q) \in \mathcal{X}$.
On a une application

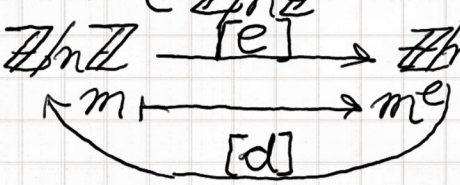
$$\mathcal{X} \longrightarrow \mathcal{K} \times \mathcal{K}'.$$

La clé publique RSA $(n, e)$ sert comme identité de B. On peut dire que c'est équivalente de son identité (avec la clé privée derrière pour déchiffrer).
Une autorité de certification est nécessaire pour gérer les identités valables.

## Sécurité de RSA

### Problème de RSA

Soit donné $n, e$ et $c \in \mathbb{Z}/n\mathbb{Z}$, déterminer $m$ tel que $m^e = c$.




Si $n = pq$,

$d \equiv e^{-1} \bmod$
$\equiv e^{-1} \bmod (p-1)(q-1)$

### Problème de factorisation

Soit donné $n$ composé.
Déterminer $p \mid n$, $p \neq 1, n$.

$n = pq$

Une solution de ce problème donne une solution au problème RSA.

# Algorithmes pour factorisation

**Divisions successives** :
$2 \mid n ?$, $3 \mid n ?$, $5 \mid n ?$, $7 \mid n ?$, etc.,
jusqu'à $p < \sqrt{n}$.

**Complexité** : $\sqrt{n}$ opérations de division (en temps polynôme en $\log n$)

On va discuter d'autres, ...

**ElGamal** ($\Leftarrow$ Diffie-Hellman)
= un autre cryptosystème asymétrique

Construction d'un couple de clé publique et privée :

- B choisit un premier $p$,
  - un élément $x \in \mathbb{Z}/(p-1)\mathbb{Z}$,
  - sa clé publique est : $(p, a, b = a^x)$
  - sa clé privée est : $x$.

  un élément primitif $a$,
- Alice envoie un message $m$ à B en choisissant $y \in \mathbb{Z}/(p-1)\mathbb{Z}$ elle calcule $(r, s)$
- B : $m = r^x s \setminus = (a^y, m b^y)$.