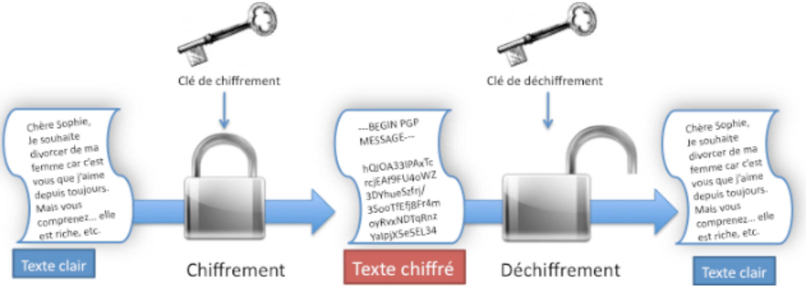
Cryptographie

Anca Nitulescu
anca.nitulescu@ens.fr

Ecole Normale Supérieure, Paris

Cryptosystème



Définition

Un cryptosystème est un dictionnaire entre les messages en clair et les messages chiffrées.

Cryptosystème

Formalisation

Des ensembles finis

- $\mathcal{P}$ les mots en clair
- $\mathcal{C}$ les mots codés
- $\mathcal{K}$ les clefs

Des algorithmes

- $\mathcal{KG} : 1 \to \mathcal{K}$ générateur de clés
- $\mathcal{E} : \mathcal{K} \times \mathcal{P} \to \mathcal{C}$ chiffrement
- $\mathcal{D} : \mathcal{K} \times \mathcal{C} \to \mathcal{P}$ dechiffrement

Cryptosystème

Exemple

Le chiffrement de Caesar peut être représenté en utilisant les congruences sur les entiers.

$$A = 0, B = 1, C = 2, ..., Y = 24, Z = 25$$

Chiffre de Caesar

- $\mathcal{P} = \{0, 1, \ldots 25\}$
- $\mathcal{C} = \{0, 1, \ldots 25\}$
- $\mathcal{K} = \{0, 1, \ldots 25\}$
- Générer la clé = le décalage

$\mathcal{KG}(1) = 3$

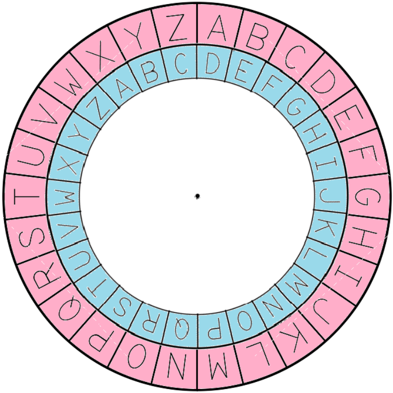
- Le chiffrement = la fonction qui ajoute 3 à chaque lettre du message

$\mathcal{E}(Y) = 24 + 3 = 1 = B \mod 26$

$\mathcal{E}(B) = 1 + 3 = 4 = E \mod 26$

- Le déchiffrement = la fonction qui soustrait 3

$\mathcal{D}(Z) = 25 - 3 = 22 = W \mod 26$



Cryptanalyse de chiffre de Caesar

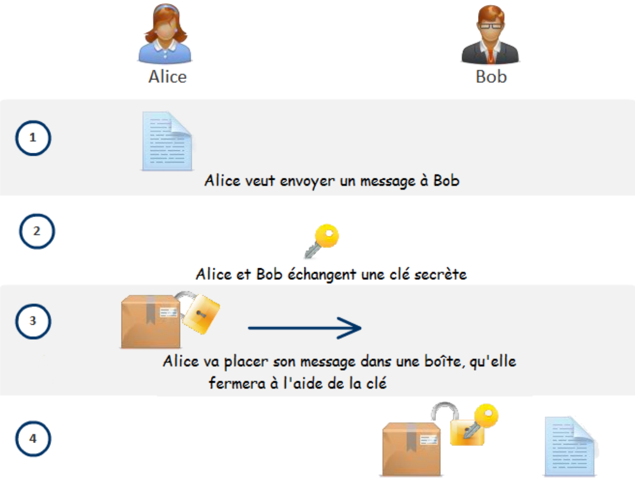
Cryptanalyse

Recherche exhaustive :
Nombre faible de clés possibles (26), on les essaye toutes jusqu'à tomber sur la bonne

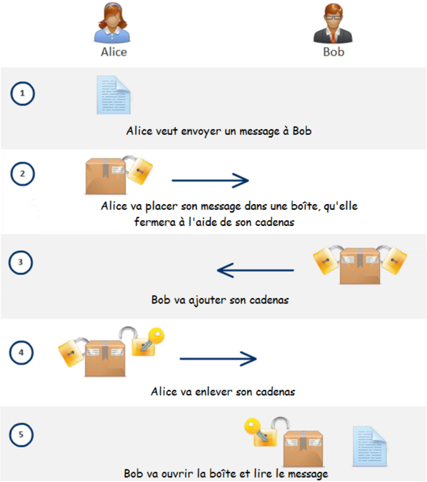
Faiblesse
Chaque lettre est remplacée par une autre, toujours la meme
L'ordre des lettres est conservé

Analyse des fréquences :
L'exploitation des caractéristiques linguistiques (redondances, fréquences) permet de cryptanalyser facilement ce type de schéma

Chiffrement à clé secrète



Chiffrement sans échange de clés ?



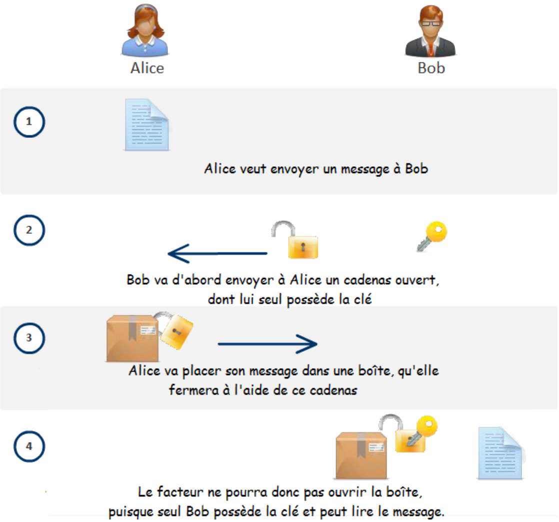
Difficulté

Construction impossible

Des fois les deux clés (cadenas) **NE** commutent **PAS** ! ! !

On peut les voir comme des coffres.
(Faut respecter l'ordre du chiffrement)

Chiffrement à clé publique



Chiffrement à clé publique

Exemples

- **RSA (Rivest-Shamir-Adleman, 1978) :**
  basé sur les racines modulaires et la decomposition en facteurs prémiers
- **ElGamal (1984) :**
  basé sur le logarithme discret
- **McEliece (1978) :**
  basé sur les codes correcteurs
- **Merkle-Hellman (1978) :**
  basé sur des problèmes combinatoires (sac-à-dos)
- **Hidden Field Equation (Patarin, 1996) :**
  basé sur les systèmes multivariables

Chiffrement à clé publique

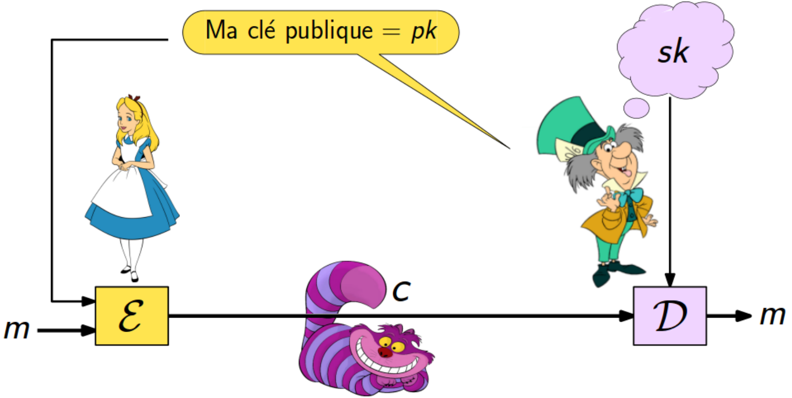
Protocole

- **Algorithme de génération des clés** $\mathcal{KG}(\ell) = (\mathrm{pk}, \mathrm{sk})$
à partir d'un paramètre de sécurité, il produit une paire de clés

- **Algorithme de chiffrement** $\mathcal{E}(\mathrm{pk}, m) = c$
produit le chiffré d'un message m, par la clé publique

- **Algorithme de déchiffrement** $\mathcal{D}(\mathrm{sk}, c) = m$
utilise la clé sécrete/privée sk pour retrouver m à partir de c

Chiffrement à clé publique



Protocole RSA

RSA - Génération des clés

$\mathcal{KG}(\ell) = (\mathsf{pk}, \mathsf{sk})$

- Soit $n = p \cdot q$ (p et q premiers)
- L'ordre du groupe multiplicatif $\mathbb{Z}_n^\star = \varphi(n) = (p-1)(q-1)$
- Soit e un entier premier avec $\varphi(n) = (p-1)(q-1)$
- Soit d un entier qui satisfait $d \cdot e = 1 \pmod{\varphi(n)}$

$$d \cdot e + u\varphi(n) = 1 \qquad \text{(Bézout)}$$

clé publique

- $n = pq$: module public
- e : exposant public

clé secrète

- $d = e^{-1} \pmod{\varphi(n)}$
- les premiers p et q

Protocole RSA

RSA - Chiffrement

$\mathcal{E}(\mathrm{pk} = (e, n), M) = M^e \pmod{\mathrm{n}}$

RSA - Déchiffrement

$\mathcal{D}(\mathrm{sk} = \mathrm{d}, C) = C^d \pmod{\mathrm{n}}$

Vérification

$$(M^e)^d = M^{ed} = M^{1-u\varphi(n)} = M \cdot 1 = M \quad (mod \;\; n)$$

(Théorème d'Euler)

Protocole ElGamal

ElGamal - Génération des clés

$\mathcal{KG}(\ell) = (\mathsf{pk}, \mathsf{sk})$

- Soit un premier p et le groupe cyclique $\mathbb{Z}_p^\star$
- Soit $g \in \mathbb{Z}_p^\star$ un élément d'ordre q, un diviseur de $(p-1)$.
- Soit une clé secrète $\mathsf{sk} = x$.
- Soit $y = g^x \pmod{p}$.

clé publique

- p et g : paramètres publiques
- $\mathsf{pk} = y = g^x$: clé publique

clé secrète

- $\mathsf{sk} = x$
  exposant sécret

Protocole ElGamal

ElGamal - Chiffrement

$\mathcal{E}(\mathrm{pk} = y, M) = (C, D)$

Pour un aléa r on calcule une paire (C, D) (le chiffré de M)

$$C = g^r \pmod{p}$$
$$D = M \cdot y^r \pmod{p}$$

ElGamal - Déchiffrement

$\mathcal{D}(\mathrm{sk} = x, (C, D)) = D \cdot C^{-x} \pmod{p}$.

Vérification

$D \cdot C^{-x} = M\ y^r\,(g^r)^{-x} = M\,(g^x)^r\,(g^r)^{-x} = M \ \ (mod\ \ p)$