Cryptographie – Feuille d'exercices 2

Introduction à la cryptographie

M1 Informatique – 2014-2015

1 Exercice

On cherche à chiffrer un message $M \in \{0, 1, 2\}$ au moyen d'une clé aléatoire partagée $K \in \{0, 1, 2\}$.

1. Supposons qu'on procède de la façon suivante : on représente K et M en utilisant deux bits (00, 01 ou 10), puis en XORant les deux représentations. Est-ce que ce protocole vous paraît bon ? Expliquer.
2. Donner un bon schéma de chiffrement dans ce contexte.

2 Chiffrement de Hill

Le schéma de chiffrement symétrique suivant a été inventé en 1929 par Lester S. Hill.

Soit m un entier strictement positif.
- L'ensemble des messages clairs est $\mathcal{P} = (\mathbb{Z}/26\mathbb{Z})^m$, et l'ensemble des messages chiffés est $\mathcal{C} = (\mathbb{Z}/26\mathbb{Z})^m$.
- L'ensemble des clés est $\mathcal{K} = \{\text{matrices } m \times m \text{ inversibles dans } \mathbb{Z}/26\mathbb{Z}\}$.
- Pour toute clé $K \in \mathcal{K}$, on définit la fonction de chiffrement $\mathcal{E}_K$ par $\mathcal{E}_K(x) = x \cdot K$, et la fonction de déchiffrement par $\mathcal{D}_K(y) = y \cdot K^{-1}$, où toutes les opérations sont faites dans $\mathbb{Z}/26\mathbb{Z}$.

Supposons que l'on sache que le texte clair

`conversation`

donne le texte chiffré

`HIARRTNUYTUS`

par le chiffrement de Hill (où m n'est pas spécifié). Déterminer la clé utilisée.

3 Chiffrement par transposition

$\mathcal{A}$ est l'alphabet romain et $\mathcal{B} = \mathcal{A}$. Soit σ une permutation (*i.e.* une bijection) sur $\{1, \ldots, n\}$ où n est la longueur du clair. L'opération de chiffrement d'un message $m = m_1 \ldots m_n$ est :

$$c = \mathcal{E}_\sigma(m) = m_{\sigma(1)} \ldots m_{\sigma(n)}.$$

La clé secrète est σ.

1. Montrer comment, connaissant cette clé, on peut déchiffrer.

2. Montrer qu'il existe une matrice A_σ telle que :

$$c = m \times A_\sigma.$$

   Expliciter la matrice A_σ.

3. Supposons que l'attaquant dispose de n paires clair-chiffré. Montrer qu'il peut, avec une probabilité non négligeable, retrouver la clé.
4. Calculer la probabilité de succès de l'attaque, ainsi que sa complexité.