

Introduction à la cryptologie  
TD n° 1 : un peu de cryptanalyse

**Exercice 1.** Décrypter le texte suivant qui a été obtenu en appliquant le chiffrement de César sur un texte en langue française dans lequel les espaces ont été supprimées :

```
vcfgrwqwfbsbhfsntowbsobgfsbhfsnqvsnjcigsghqsoixcif  
rviwtshseicwbsgojsnjcigdogeiscigoihfsgofhwgobgjc  
igbsrsjsnqwfqizsfrobzsgfiszgsgxcifgcijfopzsgoioj  
sqzsggwubsgrsjchfsdfctsggwcbdozfseiszszghhcbashwsf
```

**Note :** comment optimiser votre temps de calcul : déchiffrer le début, puis trouver d'où vient le texte.

**Exercice 2.** Soit  $n > 0$  un entier. Un *carré latin* de rang  $n$  est un tableau de taille  $n \times n$  contenant les entiers  $\{1, \dots, n\}$  tel que chacun de ces  $n$  entiers apparaît une fois sur chaque ligne et chaque colonne.

1. Donner un exemple de carré latin de rang 5.

Étant donné un carré latin  $T$  de rang  $n$ , on lui associe un système de chiffrement où l'espace des clairs, des clés et des chiffrés est l'ensemble  $\{1, \dots, n\}$  et le chiffrement du clair  $m \in \{1, \dots, n\}$  avec la clef  $k \in \{1, \dots, n\}$  (qui a été choisie aléatoirement selon la loi uniforme) est l'élément  $T(k, m)$  placé à l'intersection de la  $k$ -ème ligne de la  $m$ -ème colonne.

2. Montrer que ce cryptosystème est un chiffrement parfait, au sens suivant : en supposant une distribution a priori sur le message clair, soient  $M, C, K$  les variables aléatoires du message, du chiffré, et de la clef, alors  $P(M = m | C = c) = P(M = m)$ .

**Indication :** On peut, ou pas, montrer que la définition précédente est équivalente à : pour tout message  $M$  fixé, la distribution du chiffré correspondant est uniforme (pour une clef uniforme).

3. Montrer que le *one-time pad* est un chiffrement parfait. (*One-time pad* : un message  $M \in \mathbb{Z}_2^k$  est chiffré par la clef  $K \in \mathbb{Z}_2^k$  en  $C = M + K \in \mathbb{Z}_2^k$ .)

**Exercice 3** (Schéma de Feistel).

1. Décrire un moyen pour distinguer un schéma de Feistel à un tour d'une permutation aléatoire (par une attaque à clairs connus).
2. Décrire un moyen pour distinguer un schéma de Feistel à deux tours d'une permutation aléatoire (par une attaque à clairs choisis).
3. Décrire un moyen pour distinguer un schéma de Feistel à trois tours d'une permutation aléatoire (par une attaque à chiffrés choisis).

**Indication :** On pourra demander à l'oracle de chiffrement le chiffré de deux messages  $X_0$  et  $Y_0$  avec  $Y_0^L = X_0^L \oplus \Delta$  et  $Y_0^R = X_0^R$  (avec  $\Delta \neq 0$ ) puis à l'oracle de déchiffrement le clair associé au chiffré  $Z_3$  avec  $Z_3^L = Y_3^L \oplus \Delta$  et  $Z_3^R = Y_3^R$ .

**Exercice 4** (Cryptanalyse de Ladder-DES). Ladder-DES est un schéma de Feistel à 4 tours avec une taille de blocs de 128 bits où la fonction de tour est la permutation DES. Il n'y a pas d'algorithme de diversification de clé et une clé indépendante  $K_i$  de 56 bits est utilisée pour le  $i$ -ème tour de Ladder-DES (pour  $i \in \{1, 2, 3, 4\}$ ).

1. Considérons  $t$  messages de la forme  $(X_{0,i}^L, X_0^R)$  où  $X_0^R$  est constant et les éléments  $X_{0,i}^L$  sont deux à deux distincts pour  $i \in \{1, \dots, t\}$  et notons  $(X_{3,i}^L, X_{3,i}^R)$  pour  $i \in \{1, \dots, t\}$  les messages obtenus à la sortie du troisième tour de Ladder-DES. Montrer que les valeurs  $X_{3,i}^R$  pour  $i \in \{1, \dots, t\}$  sont deux à deux distinctes.
2. Estimer la probabilité pour une fonction aléatoire  $F : \{0, 1\}^n \rightarrow \{0, 1\}^n$  qu'étant donnés  $t$  entrées distinctes  $m_1, \dots, m_t$  de  $\{0, 1\}^n$ , les valeurs  $F(m_1), \dots, F(m_t)$  soient toutes différentes.

3. En déduire une attaque à chiffrés choisis qui permet de déterminer la clé  $K_4$  utilisée lors du quatrième tour.
4. En déduire une attaque sur le chiffrement Ladder-DES.

**Exercice 5** (Cryptanalyse de Magenta). Magenta est un schéma de Feistel à 6 tours qui chiffre des blocs de 128 bits avec une clé de 128 bits. La clé  $K$  est divisée en deux sous-clés  $K_1$  et  $K_2$  de 64 bits chacune et la fonction de tour est notée  $F$ . La clé  $K_1$  est utilisée dans la fonction  $F$  pour les tours 1, 2, 5 et 6 et la clé  $K_2$  est utilisée dans les tours 3 et 4.

Proposer une attaque (indépendamment de la fonction de tour utilisée) à clairs choisis contre le système de chiffrement Magenta qui permet de déterminer la clé  $K_1$  avec un coût algorithmique de  $O(2^{64})$  évaluations de l'algorithme de chiffrement.

**Exercice 6** (Chiffrement Triple-DES avec deux clés indépendantes). Nous considérons le chiffrement d'un bloc  $M$  de 64 bits avec le Triple-DES utilisant seulement deux clés  $(K, K^*) \in \{0, 1\}^{56} \times \{0, 1\}^{56}$  sous la forme :

$$C = \text{DES}_K(\text{DES}_{K^*}^{-1}(\text{DES}_K(M))) .$$

Soit  $\mathcal{L}$  la liste des valeurs  $(K_i, M_i)$  avec  $K_i \in \{0, 1\}^{56}$  et  $M_i = \text{DES}_{K_i}^{-1}(0^{64})$ . Nous supposons connus pour tous les  $M_i$  de cette liste leur chiffrement  $C_i = \text{Triple-DES}_{K, K^*}(M_i)$ . Montrer que pour la clé  $K_{i_0} = K$ , il existe au moins une entrée  $(K_j, \text{DES}_{K_{i_0}}^{-1}(C_{i_0}))$  dans la liste  $\mathcal{L}$  et la clé  $K^*$  est une des clés  $K_j$  ainsi obtenues. En déduire une attaque sur Triple-DES.