École normale supérieure **2019-2020**
Département d'informatique

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 :

```
vcfgrwqwfsbhfsntowbsobgfsbhfsnqvsnjcigsghqsoixcif
rviwtshseicwbsgojsnjcigdogeisjcigoihfsgofhwgobgjc
igbsrsjsnqwfqizsfrobgzsgfisgzsgxcifgcijfopzsgeioj
sqzsggwubsgrsjchfsdfctsggwcbdofzseiszsghhcbashwsf
```

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 $\{1, \ldots, n\}$ 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 n.

Étant donné un carré latin T de rang n, on lui associe un système de chiffrement où l'espace des clairs, des clefs et des chiffrés est l'ensemble $\{1, \ldots, n\}$ et le chiffrement du clair $m \in \{1, \ldots, n\}$ avec la clef $k \in \{1, \ldots, n\}$ (qui a été choisie alétoirement 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 alétoires du message, du chiffré, et de la clef, alors $P(M = m|C = c) = P(M = m)$.
3. On joue au jeu suivant. Un Adversaire A choisit librement deux messages m_1 et m_2. Un *Challenger* C choisit $b \in \{0, 1\}$ et $k \in \{1, \ldots, n\}$ uniformément, et donne à l'adversaire le chiffré $E(k, m_b)$. L'adversaire gagne le jeu s'il devine b (intuitivement : il parvient à deviner quel message a été chiffré). Si, quelle que soit la stratégie de l'adversaire, la probabilité qu'il gagne est $1/2$ (intuitivement : il n'a aucune idée de quel message a été chiffré), on dit que le chiffrement est indistinguable. Montrer qu'un chiffrement parfait est indistinguable.
   Indication : il suffit de montrer : l'information observée par l'adversaire est indépendante de b.
4. 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 $C = M + K \in \mathbb{Z}_2^k$.)
5. Soit $E : M \times K \to C$ un chiffrement parfait. Le chiffrement consistant à chiffrer deux messages, formellement $E^2 : K \times M^2 \to C^2$ défini par $E^2(k, m_1, m_2) = (E(k, m1), (k, m_2))$, est-il nécessairement parfait ? Bonus : argumenter en utilisant la question 3.

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 $Y_0^L = X_0^L$ et $Y_0^R = X_0^R \oplus \Delta$ (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 $i \in \{1, \ldots, t\}$ et notons $(X_{3,i}^L, X_{3,i}^R)$ pour $i \in \{1, \ldots, t\}$ les messages obtenus à la sortie du troisième tour de Ladder-DES. Montrer que les valeurs $X_{3,i}^R$ pour $i \in \{1, \ldots, t\}$ sont deux à deux distinctes.
2. Estimer la probabilité pour une fonction aléatoire $F : \{0,1\}^n \longrightarrow \{0,1\}^n$ qu'étant donnés t entrées distinctes $m_1, \ldots, m_t$ de $\{0,1\}^n$, les valeurs $F(m_1), \ldots, F(m_t)$ 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 clefs indépendantes)**.** Soit i_0, tel $K_{i_0} = K$. On calcule $\mathsf{DES}_K^{-1}(C_{i_0}) = \mathsf{DES}_K^{-1}\left(\mathsf{DES}_K\left(\mathsf{DES}_{K^*}^{-1}\left(\mathsf{DES}_K\left(\mathsf{DES}_K^{-1}\left(0^{64}\right)\right)\right)\right)\right) = \mathsf{DES}_{K^*}^{-1}(0^{64})$
On en déduit l'existence d'une paire, dans notre ensemble, dont la deuxième coordonnée correspond à $\mathsf{DES}_K^{-1}(C_{i_0})$.