TD 1 : Introduction

Exercice 1. *Chiffrement par décalage*

Le chiffrement de César s'applique sur des messages sur l'alphabet latin de 26 lettres. Il consiste à remplacer D par A, E par B, …, Z par W, A par X, B par Y, C par Z.

1. En quoi le chiffrement de César ne respecte pas les principes de Kerckhoffs ?

Le chiffrement par décalage est une généralisation, avec une clef k qui décrit le décalage de l'alphabet. Le chiffre de César correspond à la clef $k = -3$.

2. Décrire l'espace des messages et celui des clefs, et écrire les algorithmes Gen, Enc et Dec.
3. Montrer que le chiffrement par décalage n'est pas inconditionnellement sûr.

Exercice 2. *Chiffrement par substitution*

Le chiffrement par permutation (sur l'alphabet de 26 lettres) utilise comme clef une permutation des 26 lettres. On peut décrire la clef par un mot k de 26 lettres différentes : pour chiffrer, on remplace A par $k_{[0]}$, B par $k_{[1]}$, …, Z par $k_{[25]}$.

1. Chiffrer ALGORITHME avec la clef OTMWYECQKGVAURNZISHJDLFBPX. Déchiffrer MSPZJN avec la même clef.
2. Décrire l'espace des clefs et calculer sa taille.
3. **i.** On suppose qu'on dispose d'un chiffré, dont on sait qu'il est le chiffré d'un texte écrit en français. Comment utiliser la fréquence des lettres pour attaquer ce chiffré ?
   ii. Formellement, de quelle information (sur $\mathcal{K}$ ou $\mathcal{M}$) s'est-on servi ?

Exercice 3. *Chiffrement de Vigenère*

Le chiffrement de Vigenère s'applique sur les mots écrits sur l'alphabet latin. La clef est un mot k sur l'alphabet. Chaque lettre de la clef représente un entier, qui est sa position dans l'alphabet : A représente 0, B représente 1, …, Z représente 25. Pour chiffrer un message m avec une clef k, on applique à la première lettre $m_{[0]}$ le décalage correspondant à la première lettre $k_{[0]}$ de la clef, à $m_{[1]}$ le décalage correspondant à $k_{[1]}$, etc. Si la clef est trop courte, on la répète. Par exemple, si on chiffre ALGORITHME avec la clef CAFE, le A subit un décalage de 2 et devient C, le L aucun décalage, etc. et à nouveau le R est décalé de 2, le I n'est pas décalé, etc. On obtient CLLSTIYLOE.

1. Décrire l'espace des clefs, et écrire les algorithmes Gen, Enc et Dec.
2. Décrire une attaque contre ce chiffrement étant donné la longueur de la clef.
3. On veut maintenant une attaque qui se passe de la longueur de la clef. On suppose que le message chiffré est bien plus long que la clef.
   i. Supposons que dans le message, une suite de lettre revient (au moins) deux fois. À quelle condition cette suite est chiffrée de la même façon les deux fois ?
   ii. En français (et dans la plupart des langues), les suites de lettres ne sont pas du tout aléatoires mais des suites de lettre reviennent fréquemment (QUE par exemple en français). Comment utiliser cette information et la question précédente pour tenter de deviner la longueur de la clef ?
4. Que peut-on dire de ce chiffrement si on prend une clef aussi longue que le message ?

Exercice 4. *Vernam pour des messages de tailles variables*

On considère l'espace $\mathcal{M} = \{0,1\}^{\leq \ell}$ des messages binaires de longueur au plus ℓ.

1. On considère le schéma de chiffrement suivant : Gen produit une clef aléatoire uniforme de $\mathcal{K} = \{0,1\}^{\ell}$ et $\mathsf{Enc}_k(m)$ renvoie $k_{[0,|m|[} \oplus m$ où $k_{[0,t[}$ désigne les t premiers bits de k. Montrer que ce schéma n'est pas inconditionnellement sûr.
2. Proposer un schéma de chiffrement inconditionnellement sûr pour $\mathcal{M}$.