Série 4

Exercice 1

Le chiffrement affine est une méthode de chiffrement par substitution mono-alphabétique. Elle permet de remplacer une lettre d'un texte par une autre en appliquant la transformation suivante :

$y = ax + b\ (mod\ 26)\ a, b \in \mathbb{Z}_{26}$

- x est le rang dans l'alphabet de la lettre à chiffrer
- y est le rang dans l'alphabet de la lettre obtenue
- (a, b) est la clé de chiffrement

La clé de chiffrement doit être valide. C'est-à-dire, elle doit permettre le décodage (le déchiffrement) : a et 26 doivent être premiers entre eux.

1. Écrire une fonction qui permet de vérifier si une clé est valide ou non pour un chiffrement affine
2. Écrire une fonction qui permet de prendre en entrée un texte et une clé et produit le texte chiffré correspondant
3. Écrire une fonction qui permet de trouver, à partir d'une clé valide, la clé de déchiffrement
4. Écrire une fonction qui permet de prendre en entrée un cryptogramme (texte chiffré) et la clé de déchiffrement et fournit en sortie le texte en clair correspondant

Exercice 2

Le chiffre de Vigenère est une méthode de chiffrement par substitution poly-alphabétique. Elle permet de remplacer une lettre d'un texte par une autre en fonction de sa position dans le texte en clair :

Principe :

- Les lettres sont identifiées à des nombres
  - A ↔ 0, B ↔ 1, … Z ↔ 25 ;
- La clé est une séquence de lettres (un mot clé) ;
- Le chiffrement consiste à additionner la lettre du texte en clair avec la lettre correspondante de la clé (mod 26)
- Une lettre sera cryptée en fonction de sa position dans le texte en clair ;

Exemple

- La Clé = SESAME
- Message T H I S I S A T E S T M E S S A G E

- La clé est répétée : S E S A M E S E S A M E S E S A M E

T	**H**	**I**	**S**	**I**	**S**	**A**	**T**	**E**	**S**	**T**	**M**	**E**	**S**	**S**	**A**	**G**	**E**	•	•
S	**E**	**S**	**A**	**M**	**E**	**S**	**E**	**S**	**A**	**M**	**E**	**S**	**E**	**S**	**A**	**M**	**E**	•	•
L	**L**	**A**	**S**	**U**	**W**	**S**	**X**	**W**	**S**	**F**	**Q**	**W**	**W**	**K**	**A**	**S**	**I**	•	•

1. Écrire une fonction qui permet de produire, à partir d'un texte en clair et une clé, le cryptogramme correspondant
2. Écrire une fonction qui permet de produire, à partir d'un cryptogramme et une clé, le texte en clair correspondant