Université Mohammed V-Agdal
Faculté des Sciences de Rabat

Département d'Informatique

Année Universitaire 2021/2022
Master IPS
Module (Sécurité informatique))

Série de TD n° 1

Exercice1 :

On définit une multiplication $*$ sur les entiers de la manière suivante : pour calcule le produit de deux lettres, on transforme les lettres en entiers, on multiplie ces deu entiers et on réduit le résultat modulo 26, puis on le retransforme en une lettre. Par exemple, pour le produit de G et Y, on a $G = 6$ et $Y = 24$ et 6×2 $\mod 26 = 14$, donc $G * Y = O$.

Le cryptogramme de César multiplicatif consiste à multiplier toutes les lettres d message par un lettre fixé qui sert de clé.

1. Coder en utilisant le cryptogramme de César multiplicatif le message suivar avec la clé N

$$QUOI$$

2. En déduire que certaines clés donnent des messages cryptés non décryptable Déterminer toutes ces mauvaises clés.

3. Coder le message ci-dessus avec une clé, de votre choix, permettant u décryptage.

Exercice 2 : On considère le système de chiffrement suivant :

$$\begin{aligned}\mathcal{M} &= \mathcal{C} = \mathbb{Z}/26\mathbb{Z} = \{0, 1, \ldots, 25\},\\ \mathcal{K} &= (\mathbb{Z}/26\mathbb{Z})^\times \times \mathbb{Z}/26\mathbb{Z},\end{aligned}$$

où l'on a noté $(\mathbb{Z}/26\mathbb{Z})^\times$ l'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/26\mathbb{Z}$ (les entiers de $\{0, 1, \ldots, 25\}$ premiers avec 26).

Un élément $x \in \{0, \ldots, 25\}$ est chiffré grâce à la fonction de chiffrement $e_{(a,b)}$ pour une clef $(a, b) \in \mathcal{K}$ définie par

$$e_{(a,b)}(x) = ax + b \mod 26.$$

Ce système de chiffrement est appelé *chiffrement affine*.

1. En utilisant la correspondance $A \leftrightarrow 0, B \leftrightarrow 1, \ldots, Z \leftrightarrow 25$, numériser le message suivant
$$UNE\ MAISON$$
2. Chiffrer le message numérisé précédent avec le chiffrement affine et la clef $(15, 8) \in \mathcal{K}$.
3. On considère l'entier $a = 15$, calculer $\text{pgcd}(15, 26)$ et déterminer deux entiers u et v tels que $15u + 26v = \text{pgcd}(15, 26)$ en utilisant l'algorithme d'Euclide étendu (on donnera les détails les calculs).
4. Donner l'expression de la fonction de déchiffrement $d_{(15,8)}$ en fonction de $x \in \mathbb{Z}/26\mathbb{Z}$. Et déchiffrez le message $C = (16, 17, 24, 18, 10, 21)$ qui a été chiffré avec la clef $(15, 8)$.
5. Trouvez un couple $(a, b) \in \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$ solution du système d'équations
$$\begin{cases} a \times 8 + b \equiv 21 \mod 26, \\ a \times 19 + b \equiv 14 \mod 26. \end{cases}$$
6. Bob a envoyé à Alice le message chiffré suivant
$$C' = (16, 3, 6, 13, 3, 11, 20, 19, 1, 7)$$
Sachant que ce message a été chiffré avec un chiffrement affine de clef (a, b) et sachant que $e_{(a,b)}(8) = 21$ et $e_{(a,b)}(19) = 14$, trouvez la clef secrète qu'a utilisée Bob.