Université Abderrahmane Mira de Bejaia
Faculté des Sciences Exactes
Département d'informatique

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Module : Cryptographie
Niveau : L3 RN option RS
2023 - 2024

Fiche TD N° 1
Cryptographie Classique

Questions de cours

1. Quelle est la différence entre le chiffrement et la stéganographie ?
2. Quelle est la différence entre la stéganographie moderne et classique ?
3. Est-il toujours nécessaire de cacher l'algorithme de chiffrement ?
4. Pourquoi combiner la stéganographie avec la cryptographie ?

Exercice 1. César

On considère le crypto-système de césar récursif. La procédure de chiffrement est la suivante : notons $m_1, m_2, \dots m_n$ les lettres du message avec la correspondance usuelle entre lettre et entiers modulo 26. La clé est une lettre K. le message chiffré est alors donné par les lettres $c_1, c_2, \dots c_n$ avec

$$C_1 = m_1 + K \text{ et pour } i >= 2, C_i = m_i + c_{i-1}$$

1. Chiffrer le message « MESSAGE » avec la clé « C »
2. Déchiffrer le message « PNAAMUKEI » chiffré avec la clé « M »
3. Que peut-on dire de la sécurité de ce crypto-système ?

Exercice 2. Affine

1. Calculer l'image du message « BONE » par la fonction affine a=2, b=5. Que peut-on en conclure ?
2. Le texte suivant a été chiffré à l'aide du principe de chiffrement définit ci-dessus : « J U H K W J Q J E T W ». Les deux premières lettres du texte en clair sont R et A. Donnez deux équations (mod 26) qui vous permettra de trouver la clé de chiffrement. Retrouver la clé de chiffrement.

Exercice 3. Vigènère

Chiffre de Vigenère en auto-clé : c'est le même principe que le chiffre de Vigenère sauf que lorsque la clé est épuisée, on utilise le clair lui-même comme clé (au lieu de reprendre la clé à son début).

1. Avec la clé = « SECRET », chiffrer le message « ENCORE PLUS ETONNANT CELA ».

Exercice 4. Playfair

1. Donnez la grille de chiffrement Playfair correspondante à « WORSHIP ».
2. Chiffrez le message : M= « you can do it just try ».
3. Donnez la grille de chiffrement Playfair correspondante à la clé COVID.
4. Chiffrez le message M = « pandemie ».

Exercice 5. Hill

1. Peut-on appliquer le chiffrement de Hill avec la clé k= $\begin{pmatrix} 7 & 10 \\ 3 & 6 \end{pmatrix}$? Expliquer pourquoi ?
2. Résoudre l'équation diophantienne : 37x - 27y = 1
3. Chiffrer le message en clair M= « EXAM » en utilisant la clé k= $\begin{pmatrix} 9 & 5 \\ 7 & 8 \end{pmatrix}$
4. Déchiffrer le cryptogramme C= « KWVB » en utilisant la même clé k.

Exercice 6. Cryptanalyse

1. Décrypter le message C (chiffré avec le système par décalage) par force brute.
   C= « *JBCRCLQRWCRVNBJENBWRWN* ».

2. L'analyse des fréquences d'apparition des lettres dans un message codé montre que ceux sont les lettres H et F les plus fréquentes dans ce message. Dans un texte en français, les lettres les plus rencontrées sont dans l'ordre :

« E S A I N T R U L O D C P M V Q G F H B X J Y Z K W »

Avec les fréquences (souvent proches et dépendant de l'échantillon utilisé) :

E	S	A	I	N	T	R	U	L	O	D
14,69%	8,01%	7,54%	7,18%	6,89%	6,88%	6,49%	6,12%	5,63%	5,29%	3,66%

Sachant que le message est en français, codé en utilisant le chiffrement par décalage sur les 26 lettres de l'alphabet, déterminer la clé et déchiffrer le début du message :

« *LHLZ HFQ BC HFFPZ WH YOUPFH MUPZH* **»**

3. Décoder le message suivant encodé par le chiffrement de Vigenère avec une clé de longueur 2

« OSFFBDWCJFDAPSGSYWJSQSUSQSVHSZXGFCQ
GLRHFHRHBRGMCXFVQRAPSXBSFRHRQRZHGXF »

(Note : les espaces et signes de ponctuation ont été supprimés.)

Exercice 7. Transposition

1. Soit n=6 et la permutation (6,5,4,3,2,1). Chiffrer le message "CRYPTOGRAPHIE PAR TRANSPOSITION".
2. Déchiffrez le message C en utilisant la méthode de transposition complexe par colonnes avec le clé k= « WATER ».

C= « AAAMNTOHDEGIESNPOELGRER »