Devoir Partie 2

Il nous a été demandé de chiffrer et déchiffrer selon des méthodes particulières comme le chiffrement affine et de Hill.

Exercice 1

Chiffrement affine :

Tk vk esme jie ieekb ekxmksn jcsx dcvvkx dke wcvekmhe kl tk hk esme lxcj jcsx kv xkwkzcmx

Déchiffrement affine :

IL FAUT PLUS DE COURAGE POUR VIVRE EN LACHE QUE POUR MOURIR EN HEROS

Chiffrement de Hill :

IM QMI XG KBLFVBLG ZYZOKFTF XCF

Déchiffrement de Hill :

CHAQUE FOU SUIT SON IDEE

Partie programmation :

Pour chiffrer un message selon l’algorithme affine, on prend en input le message et la clé A et B. On pré-traitre le message en enlevant tous les caractères spéciaux. On va faire la boucle qui va de la première lettre de la chaine a la dernière et on associe pour chaque lettre un nombre de 0 à 26. Nous allons ensuite transformer ce nombre selon l’algorithme affine soit ax +b%26 pour chaque lettre puis nous allons refaire une boucle pour chaque nombre et nous allons réassocier ne lettre à ces nombres de A à Z. Toutes les lettres que nous trouvons sont mises dans un tableau et son implosées dans une chaine de caractères qui sont les valeurs finales.

Pour déchiffrer un message selon l’algorithme affine, nous faisons l’inverse. Nous prenons le message chiffré auquel nous recalculons a’\*x-b, a’ étant l’inverse modulaire de a. Cette fonction va réassocier à la lettre un chiffer qui va ensuite être réassocier à la lettre initiale. Par la suite, tous les nombres que nous trouvons sont mises dans un tableau et son implosées dans une chaine de caractères qui sont les valeurs finales.

Pour chiffrer un message selon l’algorithme de Hill, on prend en input le message et la clé A, B, C et D. On pré-traitre le message en enlevant tous les caractères spéciaux. On va faire la boucle qui va de la première lettre de la chaine a la dernière et on associe pour chaque lettre un nombre de 0 à 26. Nous allons ensuite transformer ce nombre selon l’algorithme de Hill soit M.P=C pour chaque lettre, P étant le groupe de matriciel des nombres des deux caractères réunis, M étant la matrice (). Puis, nous allons refaire une boucle pour chaque nombre et nous allons réassocier ne lettre à ces nombres de A à Z. Toutes les lettres que nous trouvons sont mises dans un tableau et son implosées dans une chaine de caractères qui sont les valeurs finales.

Pour déchiffrer un message selon l’algorithme affine, nous faisons l’inverse. Nous rechiffrons le message avec la matrice inverse. Cela va réassocier à la lettre un chiffre qui va ensuite être réassocier à la lettre initiale. Par la suite, tous les nombres que nous trouvons sont mis dans un tableau et son implosés dans une chaine de caractères qui sont les valeurs finales.

Exercice 2 :

Chiffrement avec RSA :

01 01 01 11 45 01 45 01 01 01 01 01 45 01 01 01 45

Déchiffrement avec RSA :

n = p\*q = 3\*13 = 39 et m = (p-1)(q-1)=2\*12=24

Il suffit de montrer que d et m sont premier entre eux

PGCD (39,24) = 3 donc ce n’est pas un nombre premier.

On ne peut donc pas utiliser c=29 et d=5.

Dans l’ensemble, nous ne pensons pas avoir réussi l’exercice 2 car les résultats de coïncidents pas avec vos attentes, de plus nous n’avons pas trouvé d’algorithme de chiffrement pour el Gamal et les seuls trouvés était trop complexe. Le programme de l’algorithme de Hill n’est pas terminé. Le calcul matriciel avec PHP a été difficile.