Université KASDI Merbah Ouargla

Année universitaire : 2013/2014 Niveau : 1ère Master RCS

Module : Sécurité informatique

Exercice N°1 :

Quelle est le nombre de clés possibles :

1. Pour un chiffrement de décalage (César) ?
2. Pour un chiffrement affine ?
3. Pour un chiffrement de substitution (substitution arbitraire caractère par caractère) ?
4. Pour un chiffrement de vigenère (avec une clé de longueur m) ?

Exercice N°2 : Calculez :

$2^{256} \bmod 128$

$529^{436} \bmod 66$

$1023^{4096} \bmod 1024$

$15^{362} \bmod 26$

$51447^{21} \bmod 17$

Exercice N°3 : Le chiffrement affine est défini par la règle suivante :

$e_k(x) = (ax+b) \bmod 26$ pour chaque caractère $x \in \mathbb{Z}_{26}$ avec pgcd(a,26)=1

1. Montrez que résoudre $ax + b \equiv y (\bmod 26)$ est équivalent à résoudre $ax \equiv y (\bmod 26)$.

2. Si a^{-1} est l'inverse de a, en déduire que $d_k(y) = a^{-1}(y-b) \bmod 26$

3. Montrez que k=(7,3) induit un chiffrement affine dans $\mathbb{Z}_{26}$.

Quelle est sa fonction de déchiffrement ?

Exercice N°4 :

Dans le chiffrement de Hill, chaque lettre de l'alphabet est représentée par un entier compris entre 0 et 25. L'algorithme est un chiffrement par bloc de m lettres, qui transforme un bloc $(x_1, x_2, ...x_m)$ en un bloc $(y_1, y_2, ..., y_m)$ défini par la relation algébrique : $(y_1, y_2, ..., y_m) = (x_1, x_2, ..., x_m).A$

Où A est une matrice carrée d'ordre m à coefficients dans $\mathbb{Z}_{26}$, tous les calculs étant faits modulo 26.

Par exemple : avec m=2 et $A=\begin{pmatrix} 5 & 1 \\ 12 & 3 \end{pmatrix}$ le message (10,21) est chiffré en (10,21).A=(10*5+21*12, 10*1+21*3)=(16,21) modulo 26

Le déchiffrement d'un bloc se fait en multipliant le bloc chiffré par la matrice inverse de A.

1. Quelle est la formule donnant la matrice inverse lorsque m=2 ?
2. Calculer la matrice inverse de celle donnée en exemple.
3. Décrire une méthode permettant d'attaquer le chiffrement de Hill « à texte clair connu »
4. Application : On dispose des couples ((2,9),(11,11)) et ((7,3), (11,23)).

Exercice N°5 :(RSA)

1. Décrypter le message reçu y=18, chiffré avec la clé (e=11, n=35) c à d ($y = x^{11} \bmod 35 = 18$)
2. Chiffrer le message x=10 avec la clé publique (e=7,n=55). Calculer *p, q,* et *d* et déchiffrer y=35.

Exercice N°6 :

Dans un cryptosystème RSA, on suppose que la clé publique d'Alice est

composé du module n = 28829 et du plus petit exposant publique e possible.

1. Factoriser n et montrer que e = 5.
2. Donner la signature numérique d'Alice pour le message M = 11111, puis vérifier cette signature.

Exercice N°7 :

Deux documents d_1, égal à 12, et d_2 égal à 13 sont signés numériquement par 363 pour d_1 et par 227 pour d_2. Ces deux signatures sont produites à l'aide d'un schéma RSA dont le module est 1833 et l'exposant publique est 3.

1. Les signatures de ces deux documents sont-elles correctes?
2. Le choix de e = 3 est-il valable?

Exercice N°8 :

Alice se sert du cryptosystème RSA pour signer un document. Les paramètres sont p = 541, q = 1223 et e = 159853.

1. Déterminer la clé privée d'Alice.
2. Alice signe le document électronique M = 630579. Calculer la signature.