ENSA
ÉCOLE NATIONALE DES SCIENCES APPLIQUÉES
KHOURIBGA

Examen de Cryptographie

Durée : 2H

NB. *0,5 point pour la qualité de la rédaction et la présentation. BON COURAGE !*

Question de cours. (3 pts) Expliquer chacune des qualités suivantes d'un cryptosystème ?

- Confidentialité: ……

……

- Authenticité: ……

……

- Intégrité: ……

……

Exercice 1. (Masque jetable) (2 pts) On utilise la méthode du masque jetable pour chiffrer un message écrit en binaire, et en faisant appel à la fonction XOR.

a) Chiffrer le message en clair A = 0101011101 à l'aide de la clé K=0100101011.

……

……

……

b) Expliquer la méthode de déchiffrement tout en la justifiant. Déchiffrer alors le message déjà chiffré.

……

……

……

……

……

……

Exercice 2. (Chiffrement de Hill) (4,5 pts)

On cherche à chiffrer le mot « ENSA » à l'aide du chiffrement de Hill (26 caractères), et en utilisant la matrice suivante :

$$A = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$$

On remplace chaque lettre par son rang à l'aide du tableau suivant :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

1) La matrice A est-elle inversible dans Z/26Z ? Justifier votre réponse.

……

……

……

2) Chiffrer puis déchiffrer le mot « SOS ».

……

……

……

……

……

……

……

……

……

……

……

……

Exercice 3. (Code RSA) (5 pts) On cherche à chiffrer avec le code RSA. On prend n = 85.

1) Trouver parmi les exposants de chiffrement suivants ceux qui sont valides. Justifier.

e = 2; e = 10 et e = 15.

……

……

……

2) On prend e=9.

a) Préciser la clé privée et la clé publique.

……

……

……

……

b) Supposons qu'on veuille envoyer la lettre « K » que l'on écrira « 10 » sous forme numérique. Quel est alors le chiffré de « K » sous forme numérique pour ces paramètres ?

……

……

……

……

c) Déchiffrer la valeur numérique obtenue pour le chiffré de « K » et montrer qu'on retrouve la valeur numérique associée à « K ».

……

……

……

……

……

……

Exercice 4. (Protocole de Diffie et Hellman) (2 pts)

Alice et Bob veulent s'échanger une clé K, mais ils ne disposent pas de canal sécurisé pour cela. Ils utilisent le protocole de Diffie et Hellman. Alice et Bob ont choisi un nombre premier p=19 et une base a=7. Alice choisit un nombre secret $x_1 = 9$ et Bob choisit à son tour un nombre secret $x_2 = 13$. Quelle est la clé d'échange ?

……

……

……

……

……

……

……

……

Exercice 5. (Analyse fréquentielle) (3 pts)

Déchiffrer la célèbre citation suivante chiffrée par substitution mono-alphabétique:

HYUD DU IU FUHT HYUD DU IU SHUU JEKJ IU JHQDIVEHCU

Fréquences d'apparition des lettres en Français

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%

……

……

……

……

……

……

……

……

……

……

……