Université Batna 2 -Mostefa Ben Boulaïd

- Faculté de Technologie –

Département D'Electronique

3éme Année Licence Télécommunication 2017-2018

Nom :

Prénom :

EXAMEN

Sécurité de l'information

Date : 13 JUIN 2018 - Durée 1.5 heures - Calculatrices permises

Responsable : Dr. Hadef Mahmoud

Exercice 01 (8 points)

Le RSA est une technique de codage asymétrique. Le RSA utilise deux nombres primaires, *p* et *q*, une clé de chiffrement publique **<e,n>** et une clé de déchiffrement privée **<d,n>.**

1) Ecrivez les étapes principales pour générer la clé publique et la clé privée du RSA.
2) Expliquez comment le RSA utilise la clé publique **<e,n>** pour le chiffrement et la clé **<d,n>** pour le déchiffrement.
3) Pour les valeurs de ***p, q*** et ***e*** suivantes : $p = 17, \quad q = 13, \quad e = 7$
    a. Trouvez la valeur positive la plus petite du ***d*** qui fonctionne comme la clé privée de l'algorithme du RSA.
    b. Supposons que le message naturel **M = 9** doit être encodé en utilisant la paire de la clé publique
        i. Trouvez le message chiffré **C** qui correspond au message **M**.
        ii. Vérifiez que le message déchiffré du **C** est le message **M**.
4) Supposons que nous ne connaissons pas *p* et *q* mais on a la clé publique <3,55>, est ce que il est possible de trouver la clé de déchiffrement privée **<d,n>,** dans ce cas justifiez votre réponse.

Exercice 02 (6 points)

1) Expliquez le fonctionnement d'un pont «Bridge» dans un Local Area Network étendu (Extended LAN) et qu'est-ce qu'un VLAN? (Servez-vous d'un schéma pour expliquer).
2) Expliquez le rôle et le fonctionnement d'un pare-feu (firewall) dans la Sécurité des Réseaux Informatiques ? Mentionnez et expliquez trois types des par-feu
3) Dans la technique de cryptographie DES, pourquoi doit-on à chaque tour diviser Le block de 64 bits (permuté) en deux blocks, chacun de 32 bits?

Exercice 03 (6 points)

Votre enseignant du module de Sécurité Informatique vous a envoyé un message très important mais chiffré avec la méthode de chiffrement nommée **Vigenère**. Le message reçus est le suivant :

OEOPTHIGOTBMPSZIAUEEP

Sûrement vous ne pouvez pas comprendre le message sans le déchiffrer. Le problème c'est que vous ne connaissez pas la clé utilisée par l'enseignant mais vous connaissez que la clé contient cinq lettres et les messages de l'enseignant toujours commencent avec le mot ***Hello***. Utilisez le tableau de **Vigenère** ci-dessous pour :

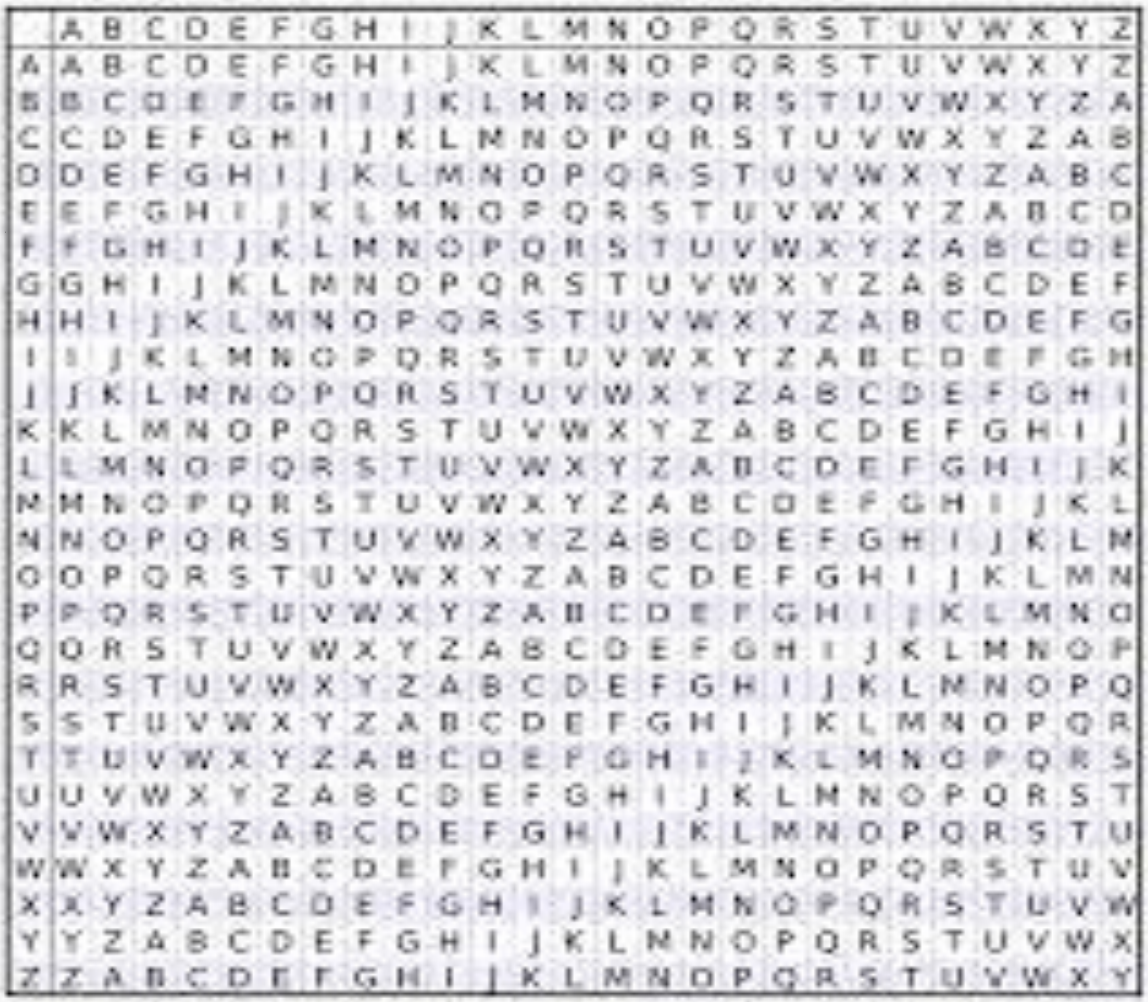
1) Trouver le mot clé utilisé par l'enseignant pour chiffrer le message
2) Déterminer le message initial envoyé par l'enseignant

Rappel

Le système de Vigénère utilise la substitution poly alphabétique. Son principe est relativement simple. Dans un tableau, dit carré de Vigénère, on remplace la lettre du message à chiffrer par la lettre obtenue à l'intersection de la colonne repérée par cette lettre, et de la ligne définie par la lettre de la clé associée à la lettre du message. Exemple :

Message initial →	A	B	A	C	A	**D**
La clé utilisée →	C	L	E	C	L	**E**

Donc la lettre **D** du message initial sera codée avec la lettre **H** (comme montre dans le carré).



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

Bon Courage