

✓ **Exercice 1 (1 point)**

Voici un texte chiffré avec l'algorithme de César :

JCBPJKPXHPGGPCVTBTCIKPJIBXTJMFJJJCQDCEGDRTH

Utiliser les spécificités de ce message pour le déchiffrer. Expliquer la démarche pour trouver la clé de déchiffrement et donner le texte lisible (texte en clair écrit en Français).

✓ **Exercice 2 (2 points)**

Le texte suivant a été chiffré avec l'algorithme de Vignère :

VLIXVMJCEAVNYIEHFLYVLFKERGEYV

En regardant par-dessus l'épaule de l'émetteur, vous avez réussi à voir la première lettre de la clé "F", et la dernière "A". Déchiffrer le texte sachant que la longueur de la clé est 3.

✓ **Exercice 3 (3 points)**

Vous avez intercepté le message suivant :

WEUIEOSRWHEGHXMPWAYVSNYGRMSVYXTDTCEE

Et vous cherchez à le déchiffrer, sachant qu'il s'agit d'un auto-chiffrement. La clé est de longueur 3 et commence par la lettre "C" et se termine par la lettre "I". Donner la clé, le texte en clair et expliquer la démarche pour déchiffrer le message.

✓ **Exercice 4 (2 points)**

Le texte suivant a été chiffré avec l'algorithme de Rail Fence et une clé de chiffrement égale à 4. Déchiffrer le texte et expliquer la démarche sachant que la première lettre du texte est "L":

LRITALSEUSUVENRSBEASOSSETEESMNPJENSET 47

✓ **Exercice 5 (4 points)**

Ce message a été chiffré avec un système de PlayFair :

YJ BE CS JO GB CZ FH JG AC LS QF TI JU SC OS DJ QT

Déchiffrer le message, sachant que la lettre double (parasite) est W.

Saurez-vous trouver la clé cachée dans ce sujet ? Comment s'appelle cette technique ?

✓ **Exercice 6 (2 points)**

Indiquer les services de sécurité fournis par les schémas suivants ? Sachant que "E" est la clé de chiffrement partagée entre Alice et Bob, C (resp. D) est la fonction de chiffrement (resp. déchiffrement), H est la fonction d'hachage, M représente le message en clair et TC représente le texte chiffré. Justifier vos réponses et donner l'expression représentant le message qui circule dans le réseau.

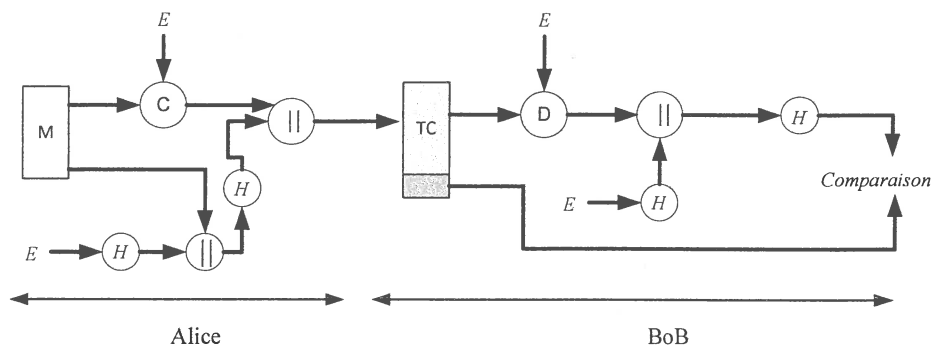


Figure 6.A

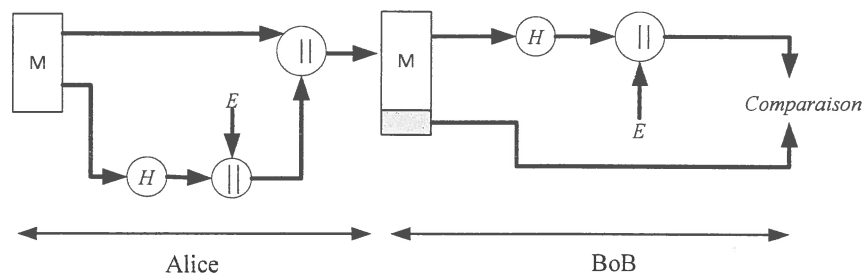


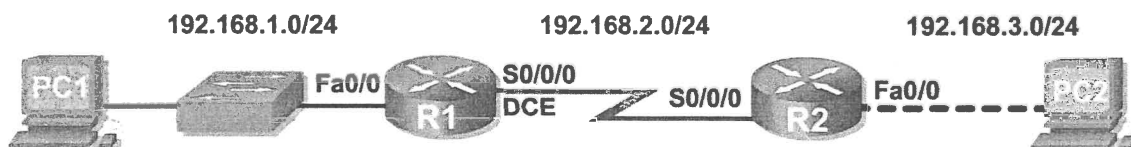
Figure 6.B

Exercice 7 (2 points)

- 7.1 Donner le nom de l'algorithme de chiffrement symétrique utilisé par les spartiates.
- 7.2 Donner le nom du scientifique Arabe qui a découvert l'idée de l'utilisation de la fréquence d'apparition des lettres dans la cryptanalyse au IX^e siècle.
- 7.3 Donner le nom de la machine à rotors utilisée par l'Allemagne nazie et de ses alliés pendant la seconde guerre mondiale.
- 7.4 Donner le nom du service de sécurité qui consiste à empêcher un émetteur de nier qu'il a envoyé un message.

Exercice 8 (4 points)

On considère la topologie suivante :



Donner les commandes pour configurer le routeur R1 uniquement:

1. Changer le nom du routeur à R1

2. Désactiver la recherche DNS
3. Sécuriser l'accès au mode privilégié (mode d'exécution)
4. Sécuriser l'accès en local et à distance
5. Configurer et activer les interfaces:
 - a. Fa 0/0 @IP : 192.168.1.1 Masque : 255.255.255.0
 - b. S 0/0/0 @IP : 192.168.2.1 Masque : 255.255.255.0
6. Activer le protocole RIPv2 sur les deux interfaces
7. Donner la commande pour afficher la table de routage
8. Enregistrer les modifications dans la mémoire NvRAM

Annexe :

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Tableau I : Table de Vigenère

