Université Paris DESCARTES - UFR de mathématiques et Informatique

Réseaux, Performance et Sécurité

Examen partiel du 05 Mars 2014 – Licence L3

Durée 1h30 - Sans documents

Exercice 1 (3 points)

On considère un système de chiffrement symétrique avec une clé de 64 bits. Vous cherchez à casser le système sans aucune connaissance de la clé: vous essayez de manière exhaustive toutes les clés. On suppose que vous avez à votre disposition un ordinateur puissant capable de tester une clé (et de dire si c'est la bonne !) en une femtoseconde (1 femto=10^{-15}sec).

1. Combien de clés y-a-t-il ? Combien de clés en moyenne essaierez-vous ?
2. Combien de temps en moyenne vous faudra-t-il pour trouver la bonne clé ?
3. Donner deux solutions pour lutter contre la cryptanalyse par force brute ?

Exercice 2 (1 point)

Vous avez intercepté ce message chiffré avec l'algorithme de César. Utiliser les spécificités de ce message pour le déchiffrer.

```
BQIUSKHYJUTUBYDVEHCQJYEDUIJKDFHESUIIKILYIQDJQFHEJUWUHTUITEDDUUI
```

Expliquer la démarche pour trouver la clé de déchiffrement et donner le texte lisible (texte en clair écrit en Français).

Exercice 3 (4 points)

Vous avez intercepté le message suivant:

```
CTTVHGZCVVUSZGWGPJMTFZGVVHAEUGIBSKXGEHVVBSEXWITUFCXZSWEIAVADVC
WJIHRHILTDHJWTWGJTVVCGLKWRJSLUACSWJHAVRDVHKVJDCT
EFNWESWCTXRXJVPWMDDLT
```

Sachant que le texte en clair est écrit en Français, et l'algorithme de chiffrement est Vigenère. En regardant par-dessus l'épaule de l'émetteur, vous avez réussi à voir uniquement la taille de la clé "3" (3 caractères). Déchiffrer le message et donner le texte en clair.

Exercice 4 (1 point)

Le texte suivant a été chiffré avec l'algorithme de Rail Fence et une clé de chiffrement égale à 3. Déchiffrer le texte et expliquer la démarche :

```
SIMAITDNOAORIESNREATNRERTUVARSNEEER
```

Exercice 5 (3 points)

Ce message a été chiffré avec un système de PlayFair :

```
NDQLLTUFPCVPNLLREICPLBLIBGLOOLFZNDENPI
```

Déchiffrer le message, sachant que la lettre double (parasite) est W et partage la même case que la lettre X.

Saurez-vous trouver la clé cachée dans ce sujet ?

Université Paris DESCARTES - UFR de mathématiques et Informatique

Réseaux, Performance et Sécurité

Examen partiel du 05 Mars 2014 – Licence L3

Durée 1h30 - Sans documents

Exercice 6 (2 points)

Indiquer les services de sécurité fournis par les schémas suivants ? Sachant que "k" est la clé de chiffrement partagée entre Alice et Bob, E (resp. D) est la fonction de chiffrement (resp. déchiffrement), H est la fonction d'hachage, T représente le texte en clair et TC représente le texte chiffré. Justifier vos réponses et donner l'expression représentant le message qui circule dans le réseau.

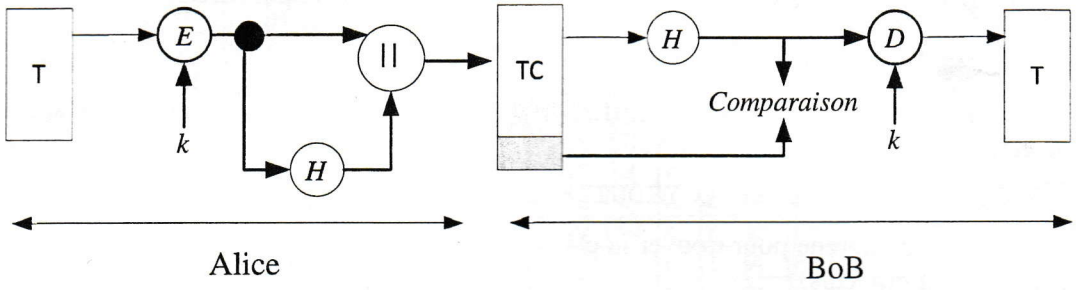


Figure 6.A

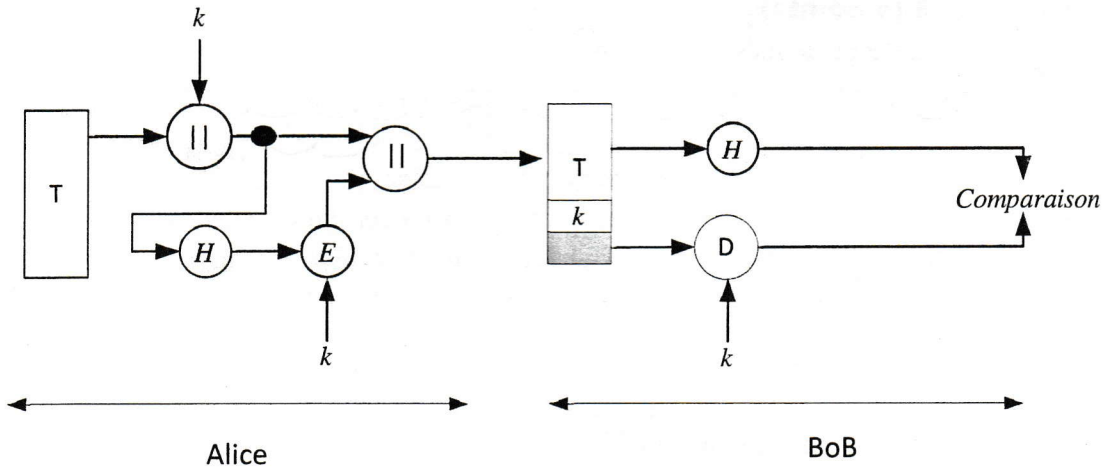


Figure 6.B

Exercice 7 (1 point)

7.1 Expliquer "la collision" dans une fonction d'hachage ? Existe-t-il une fonction d'hachage qui ne possède aucune collision ? Donner son nom.

7.2 Est-ce que le protocole d'authentification CHAP (Challenge Handshake Authentication Protocol) est vulnérable à l'attaque Man In The Middle ? Justifier.

Exercice 8 (5 points)

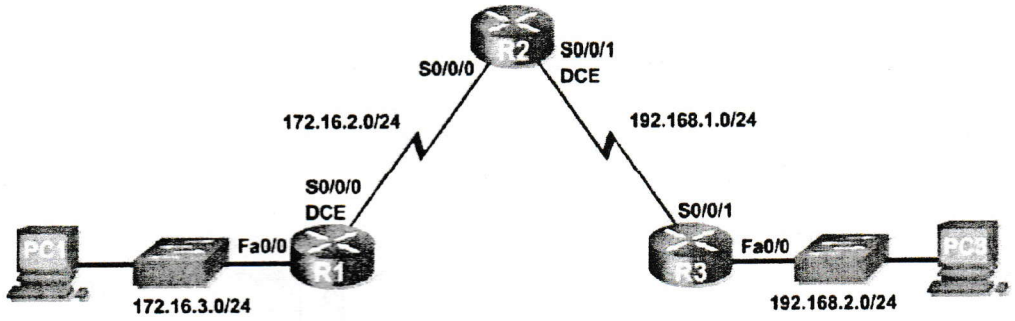
On considère la topologie suivante :

Université Paris DESCARTES - UFR de mathématiques et Informatique

Réseaux, Performance et Sécurité

Examen partiel du 05 Mars 2014 – Licence L3

Durée 1h30 - Sans documents



8.1) 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
4. Sécuriser l'accès local et à distance
5. Configurer correctement et activer les interfaces:
   a. Fa 0/0 @IP : 172.16.3.1 Masque : 255.255.255.0
   b. S 0/0/0 @IP : 172.16.2.1 Masque : 255.255.255.0

8.2) Dans la suite de cet exercice, on suppose que toutes les interfaces des routeurs et des ordinateurs ont été configurées correctement avec les adresses IP suivantes :

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	Fa0/0	172.16.3.1	255.255.255.0	s/o
	S0/0/0	172.16.2.1	255.255.255.0	s/o
R2	Fa0/0	172.16.1.1	255.255.255.0	s/o
	S0/0/0	172.16.2.2	255.255.255.0	s/o
	S0/0/1	192.168.1.2	255.255.255.0	s/o
R3	FA0/0	192.168.2.1	255.255.255.0	s/o
	S0/0/1	192.168.1.1	255.255.255.0	s/o
PC1	Carte réseau	172.16.3.10	255.255.255.0	172.16.3.1
PC2	Carte réseau	172.16.1.10	255.255.255.0	172.16.1.1
PC3	Carte réseau	192.168.2.10	255.255.255.0	192.168.2.1

1. Donnez le contenu de la table de routage de chaque routeur.
2. Donner la suite des commandes pour la configuration du routage statique sur chaque routeur afin que tous les ordinateurs puissent communiquer ensemble.
3. Donner le nom du fichier (et le nom de la mémoire) contenant la configuration courante d'un routeur ? et le nom du fichier contenant la configuration permanente ?
4. Donner la commande pour enregistrer les modifications dans la configuration.

Université Paris DESCARTES - UFR de mathématiques et Informatique

Réseaux, Performance et Sécurité

Examen partiel du 05 Mars 2014 – Licence L3

Durée 1h30 - Sans documents

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