Exercices Sécurité Informatique
Cryptographie

Exercice1 (César) :

Soit le message : « Ici c'est licence SI »
En appliquant l'algorithme de César et le Code ASCII chiffrer le message avec :
1- un décalage à droite de 4
2- un décalage à gauche de 3
3- un décalage à droite de 3

Exercice2 (RSA) :

On suppose l'algorithme RSA avec : p=5, q=13, e=17, m=123
Question : Chiffrer m.

Exercice3 (Disponibilité):

Soit le système composé de 5 serveurs :
S1 : 99%, S2 : 80%, S3 : 90%, S4 : 95%, S5 : 56%

- Calculer la disponibilité du système dans les cas suivants :
  - Système en parallèle
  - Système en série

Exercice4 : (Sécurité des Bases de Données) :

Soit la matrice suivante :

	T1	T2	T3
Bob	ALL	SELECT *	
Alice	UPDATE *	SELECT*, UPDATE	ALL
Jack		SELECT INSERT * UPDATE	DELETE

1) Pour chacun des cas suivants dire si la requête s'exécute ou non, justifier votre réponse :
a) Jack fait select * from T1
b) Bob fait INSERT INTO T1
c) Alice fait DROP TABLE T2
d) Alice fait SELECT * FROM T3

2) Donner la suite des requêtes SQL permettant de l'attribution de cette matrice

3) Supposons les cas suivants :
-> Bob voulait supprimer le droit de sélection sur T2 de Alice
-> Alice voulait supprimer le droit de INSERT sur T1 de Bob
-> Bob voulait donner le droit de DELETE sur T3 à tout le monde

Pour chaque cas donner
Bob-> T1
Jack -> T3
Alice -> T2

4- Donner le graphe d'action des droits de la matrice saquant que les sujets chacun possible de la table
Ex : Bob -> T1, Jack -> T3, Alice -> T2

Corrigé des exercices :

Exercice1 :

Le message : **« Ici c'est licence SI »**

1) décalage à droite de 4 :

Mgm g'iwx pmgirgi WM

2) décalage à gauche de 3 :

Haf y'zmm dzstbpq DS

3) décalage à droite de 3 :

Lfl f'hvw olfhqfh VL

Exercice2 :

RAPPEL sur RSA :

Soit 2 nbres premiers p et q

n=p*q

$\phi(n) = (p - 1)(q - 1)$

e : $1 < e < \phi(n)$ c'est un nbre premier

d=pgcd(e, $\phi(n)$)=1

clé public : (e, $\phi(n)$)

clé privé : d

Chiffrement :

C=$M^e \bmod(n)$

Déchiffrement de C :

D=$C^d \bmod(n)$

p=5, q=13, e=17, M=123

n=p*q=5*13=64

$\phi(n)$=(p-1)*(q-1)=(5-1)*(13-1)=4*12=48

e est déjà donné =17

On retrouve d tel que :
d= pgcd(e, ϕ(n))=1 => pgcd(17,48) => 3

Clé publique : (17,48)
Clé privée : 3

Chiffrement :
C=M^{e}mod(n)= 123^{17}mod(64) = 59

Déchiffrement :
D=C^{d}mod(n)=59^{3}mod(64)=3

Exercice3 :

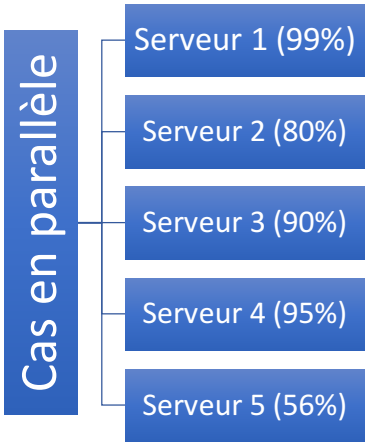
Cas d'un système en **série** :

1)

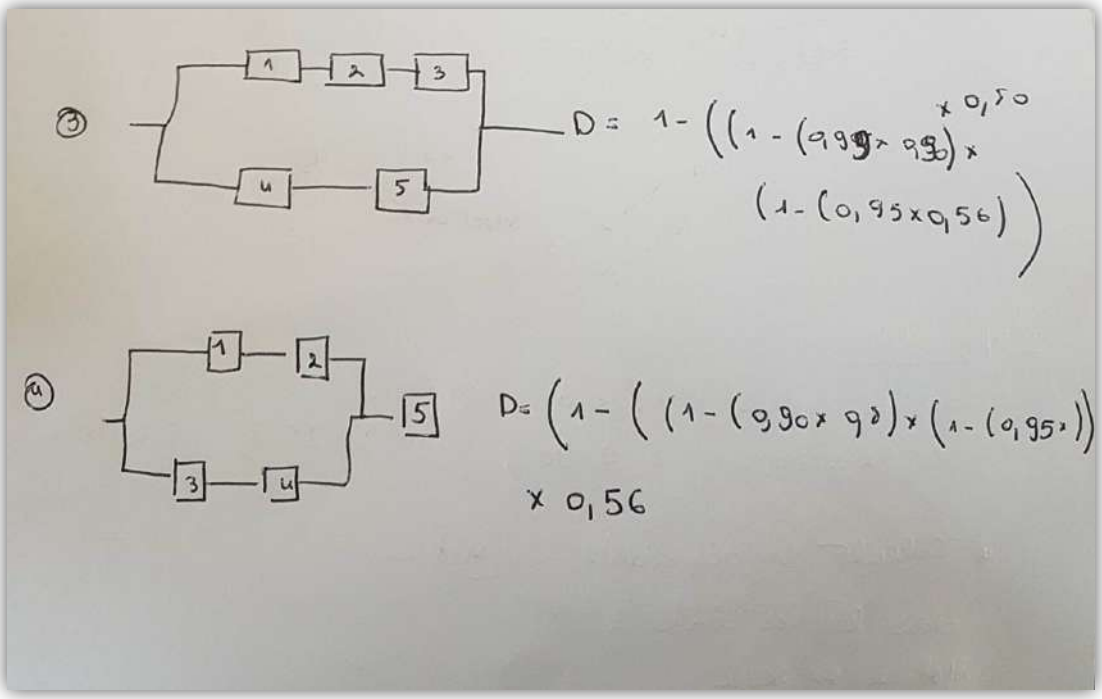
$$\prod_{i=1}^{n}(di) = 0{,}99 * 0{,}8 * 0{,}9 * 0{,}95 * 0{,}56 = 0{,}37$$

Cas d'un système en parallèle :

2)



$$1-\prod_{i=1}^{n}(1\text{-di}) = 1\text{-}((1\text{-}0{,}99)*(1\text{-}0{,}8)*(1\text{-}0{,}9)*(1\text{-}0{,}95)*(1\text{-}0{,}56) = 0{,}99$$



Exercice4 :

1)

a) refusé, il n'a aucun droits (y compris le droit de SELECT)

b) accepté (il a le droit de select)

c) refusé (elle n'a pas le droit de supprimer une table)

d) accepté (elle a le droit de select sur le table T2)

2) les requêtes :

GRANT ALL on T1 to Bob

GRANT SELECT on T2 to Bob with GRANT OPTIONS

GRANT SELECT on T2 to Alice with GRANT OPTIONS

GRANT UPDATE on T2 to Alice

GRANT ALL on T3 to Alice

GRANT UPDATE on T1 to Alice with GRANT OPTIONS

GRANT SELECT, INSERT, UPDATE on T2 to JACK

GRANT DELETE on T3 to Jack

3)
- REVOKE GRANT OPTIONS SELECT on T2 FROM Alice
- Impossible car Alice n'a pas le droit sur T1
- Impossible car Bob n'a aucun droit sur T3

4-