Université M'hamed Bougara Boumerdes / Faculté des Sciences / Département d'Informatique

Module : Sécurité informatique | **Niveau :** L3 ISIL/SI (S6) | **Date :** 27.04.2023
Examen : ETCD | **Documents :** non autorisés | **Durée :** 30 min

Matricule : Nom : Prénom : Groupe :

Questions de cours (3 points) : Cochez la ou les bonnes réponses

1. Soit un groupe de N personnes souhaitant utiliser un système cryptographique symétrique pour s'échanger trois à trois des informations confidentielles. Quel est le nombre minimal de clés symétriques nécessaires ?
   - ☐ N(N-1)/2
   - ☐ N(N-1)(N-2)/3
   - ☐ N(N-1)(N-2)/3!
   - ☐ N(N-1)(N-2)(N-3)!/3

2. Une entreprise utilise le chiffrement symétrique. Quel(s) sont les raisons valide pour migrer vers le chiffrement asymétrique ?
   - ☐ Le chiffrement symétrique est plus rapide que le chiffrement asymétrique
   - ☐ Le chiffrement symétrique fournit l'authenticité.
   - ☐ Le chiffrement symétrique peut rendre l'administration des clés difficile
   - ☐ Le chiffrement asymétrique est plus long que le chiffrement symétrique

3. Que se passe-t-il si vous chiffrer un message confidentiel avec votre clé privée ?
   - ☐ Personne ne pourra le déchiffrer
   - ☐ Vous seul pourrez le déchiffrer
   - ☐ Il est impossible de chiffrer avec sa clé privée
   - ☐ Le monde entier pourra le déchiffrer

Exercice 01 (12 points):

Considérant un chiffrement de César où l'alphabet est constitué des 20 premières lettres de l'alphabet français, c'est-à-dire les lettres de **A** à **T**.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

1. Chiffrer le Message M = **CONFIANCE** sachant que la clé = **13.** Détaillez votre réponse

M =	C	O	N	F	I	A	N	C	E
Encodage	2	14	13	5	8	0	13	2	4
Clé	13	13	13	13	13	13	13	13	13
$E_K(M) = M + K \bmod 20$	15	27≡7	26≡6	18	21≡1	13	26≡6	15	17
C =	P	H	G	S	B	N	G	P	R

2. Déchiffrer le Message C = **KLJOPMMELE SL TLFFHNL.** Détaillez votre réponse.
Sachant que le message clair est fait en utilisant l'alphabet choisi. Et que la fréquence d'apparition des lettres des mots construits à partir de cet alphabet est représentée par la table suivante.

Lettre	E	S	I	A	…
Fréquence	18.4%	12.2%	8.5%	6.3%	…

Cryptanalyse : Analyse de fréquence
H0 : Chiffrement de César(monoalphabétique)
H1 : Langue française

1- Calcule des fréquences des lettres :

Lettre	**G**	**S**	**M**	**O**	**A**	**Q**
Fréquence	**1**	**3**	**4**	**2**	**1**	**1**

2- H2 : On suppose que la lettre la plus fréquente M du message chiffré correspond à la lettre la plus fréquente S de la langue française.

3- $D_k(M) = S$ => M - K = S => 12 – k = 18 => k = 12 – 18 mod 20 => k = -6 mod20 => k = 14 = "O"

4- Déchiffrer le message :

C =	G	S	M	M	O	A	S	Q	O	M	M	S
Encodage	6	18	12	12	14	0	18	16	14	12	12	18
Clé	14	14	14	14	14	14	14	14	14	14	14	14
$D_K(M) = M - K \bmod 20$	12	4	18	18	0	6	4	2	0	18	18	4
M =	M	E	S	S	A	G	E	C	A	S	S	E

Le message M satisfait l'hypothèse H1. Donc la clé k = 14.

3. Qu'est-ce qu'une clé faible / semi-faible dans le chiffrement de César ?

Une clé faible ou semi faible est une clé qui a un comportement indésirable.

On dit qu'une clé est faible si : $E_{k1}(E_{k2}(M)) = M / k1 = k2$

On dit qu'une clé est semi-faible si : $E_{k1}(E_{k2}(M)) = M / k1 \neq k2$

4. Quelles sont les clés faibles / semi-faibles de ce système de chiffrement ?

Les clés faibles :

Ek1(Ek2(M)) = M => k1 + k2 + M = M / k1 = k2
=>2k1 mod 20 = 0

k1 = 0
20

Les clés semi-faibles :

Ek1(Ek2(M)) = M => k1 + k2 + M = M / k1 ≠ k2
=>k1+ k 2 mod 20 = 0

k1	k2
0	0
1	19
2	18
…	…
19	1

Considérant un chiffrement de Vigenère avec le même alphabet (de **A** à **T**).

5. Déchiffrer le Message ***C*** = **AFPQSJQCFL,** sachant que la clé = **SOL**

C =	A	F	P	Q	S	J	Q	C	F	L
Encodage	0	5	15	16	18	9	16	2	5	11
Clé	18	14	11	18	14	11	18	14	11	18
$D_{Ki}(x_i) = (xi - k_{i \bmod 3}) \bmod 20$	2	11	4	18	4	18	18	8	14	13
M =	C	L	E	S	E	S	S	I	O	N

Bon courage