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

Module : Sécurité informatique **Niveau :** L3 ISIL/SI (S6) **Nombre de pages :** 1 **Date :** 01.06.2023
Examen : ETCD de remplacement **Documents :** non autorisés **Durée :** 20 min

Matricule : Nom : Prénom : Groupe :

Questions: Cochez la ou les bonnes réponses

1. Que représente un certificat numérique ?
   - ☐ Un moyen d'assurer la non-répudiation du message transmis
   - ☐ Une garantie donnée sur l'intégrité du message transmis
   - ☐ Un moyen de garantir la relation univoque entre une clef publique et son véritable propriétaire
   - ☐ Aucune de ces réponses
2. Quelle est la principale limite de la cryptographie à clé secrète ?
   - ☐ La sécurité incertaine lors du transfert de cette clé
   - ☐ Le cryptage nécessite un nombre très important de calculs
   - ☐ La lenteur à laquelle se font les opérations de chiffrement et de déchiffrement
   - ☐ Des clés différentes sont utilisées pour crypter et décrypter

Exercice 01 :

La langue POL a la particularité d'avoir un alphabet constitué de seulement 3 lettres P, O et L encodé respectivement 0, 1 et 2. Le message ci-dessous est un message en langue POL qui a été chiffré avec une méthode de césar.

PPLPPLOLPLPPLPPPLPPLPOPLPPPLLP

1. En vous aidant des fréquences des lettres dans la langue POL ci-dessous, donner la clé de chiffrement la plus probable et déchiffrer les 7 premières lettres du message. **Détaillez votre réponse.**

- Détaillez la méthode utilisée.
- Dessinez le tableau de déchiffrement.
- Précisez la fonction de déchiffrement.

Lettre	P	O	L
Fréquence	0.30	0.65	0.05

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

Lettre	**P**	**O**	**L**
Encodage	**0**	**1**	**2**

1- Calcule des fréquences des lettres :

Lettre	**P**	**O**	**L**
Fréquence	**18**	**2**	**10**

2- H2 : On suppose que la lettre la plus fréquente P du message chiffré correspond à la lettre la plus fréquente O de la langue POL.

3- $D_k(P) = O$ => P - K = O => 0 – k = 1 => k = 0 – 1 mod 3 => k = 2 mod3 => k = 2 = "L"

4- Déchiffrer le message :

C =	P	P	L	P	P	L	O
Encodage	0	0	2	0	0	2	1
Clé	2	2	2	2	2	2	2
$D_K(C) = C - K \mod 3$	-2≡1	-2≡1	0	-2≡1	-2≡1	0	-1≡2
M =	O	O	P	O	O	P	L

Bon courage