Université d'Oum El Bouaghi

Département des Mathématiques et de l'Informatique

Niveau : 03ème Licence informatique SI +ISIL 17Mai 2023

Remarque :*Les réponses doivent être brèves, claires et concises* **Durée**: 1h30'

Module: Sécurité Informatique

Examen Final

Questions (06 Pts)

1. Définir la sécurité informatique.

La sécurité informatique est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité des systèmes informatiques contre les menaces intentionnelles et accidentelles. (01)

2. Expliquer trois types de logiciels malveillants (malware).

Il suffit d'expliquer trois malwares comme : virus, bombe logique, keylogger, cheval de Troie…etc. (0.5*3+0.5*3 = 03)

3. Citer quarte sources pour connaitre la cible dans une méthodologie d'attaque.

Les sources peuvent être des être humains (employés), des sites web, des moteurs de recherche ou des commandes réseaux. (0.5*4 = 02)

Exercice 01

Le message suivant "SDBRSDGPJPJVCUKBKFQULO" est crypté par la technique Playfair avec la clé présentée dans le tableau suivant.

1. Comment peut-on crypter le caractère "W", s'il est appartient au message clair?

   On remplace « W » par « V » (01)

2. Décrypter le message au-dessus.

   Après l'application de la méthode on trouve le message « VERYVELXLITISCORXRECTX » (02)

   On déduit le message « Very well it is correct » (01)

3. Quel est le type de la technique Playfair, parmi les types de techniques par substitution ? justifier.

   Le type de la technique Playfair est polygramme car on remplace chaque deux lettres par deux autres (c'est-à-dire par bloc).

M	D	G	E	N
K	O	X	Q	H
A	V	P	S	I
R	B	F	C	Y
Z	T	L	U	J

Exercice 02

Soit les nombres suivants: p = 17, q = 11, E= 19.

1. Calculer l'inverse de E mod 160. (03pts)

N	b	R	Q	T0	T	temp
160	19	8	8	0	1	152
19	8	3	2	1	152	17
8	3	2	2	152	14	118
3	2	1	1	17	118	59
2	1	0	2	118	59	

L'inverse de 19 mod 160 est 59.

2. Sachant qu'on va utiliser la technique de cryptage RSA, déduire la clé publique et la clé privé.

On remarquant que 160 = (p-1)*(q-1). Donc, d (l'inverse de 19 mod 160) est 59. Donc, on déduit la clé publique est (187, 19) et la clé privé (187, 59)

3. En utilisant les clés générés précédemment, crypter le message M = 5.

Après le calcul, on trouve 5^{19} mod 187 = 108. (01)

4. Est-il possible de déduire la clé privé à partir de la clé publique? Justifier.

Il est impossible de déduire la clé privé à partir de la clé publique parce que pour déduire la clé privé, on doit connaitre les valeurs p et q. Comme la valeur N est très grande, il est pratiquement impossible de déduire ces deux valeurs. (02)

Bon courage !

Dr. Toufik MARIR