Université d'Alger 1
Faculté des Sciences
Département Mathématique et Informatique

3éme année Licence ISIL 2019-2020
Module : Sécurité des Systèmes d'Information durée : 1h00

Examen de Rattrapage

Questions de cours (05 points):

1. Définir brièvement la notion risque informatique
2. Quelle est la différence entre une vulnérabilité et une menace
3. Citer 3 objectifs de sécurité et pour chacun citer un mécanisme de sécurité permet de l'assurer

---

Exercice 01 (15 points):

Soit le chiffrement de Vigenère modifié selon le schéma suivant :

Pour un message m de taille x et une clé k de taille y (y << x), le chiffrement s'effectue selon les étapes suivantes :

1. Diviser le message m en sous messages de taille y
2. Les sous messages d'ordre impaire (1, 3, 5…etc.) sont chiffré par la clé k
3. Les sous messages d'ordre paire (2, 4, 6…etc.) sont chiffré par le mot miroir de la clé k
4. Le chiffrement utilise la table 1 ci-dessus et un chiffrement de César dans chaque caractère du sous message est chiffré par le caractère de même position dans la clé k

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

L'exemple suivant montre comment fonctionne ce chiffrement : soit le message m = « je suis étudiant » et la clé k = « ISIL ».

1. Les sous message de m sont de même taille de k qui est 4 donc on aura :

M1 = jesu, m2 = iset, m3 = udia, et m4 = nt--

2. Les sous messages m1 et m3 seront chiffrés par la clé k = « ISIL »
3. Les sous messages m2 et m4 seront chiffrés par le mot miroir de la clé k qui sera k' = « LISI »
4. Exemple de chiffrement de sous message m1 :

J	E	S	U
I	S	I	L

J + I => 9 + 8 = 17 mod 26 = 17 => R

E + S => 4 + 18 = 22 mod 26 = 22 => W

S + I => 18 + 8 = 26 mod 26 = 00 => A

U + L => 20 + 11 = 31 mod 26 = 05 => F

Le sous message chiffré de m1 sera donc « rwaf ». le reste des sous messages seront chiffrés de la même façon en utilisant la clé correspondant (k ou k')

1. Chiffrer le message m = « **classical cryptography** » avec la clé m = « **Algiers** »