Al-Mustaqbal University

Course Title: MU0224104 Security of Computer and Networks

Name: **ID:** **Section C Date: 15.11.2023 Time: 60**

Instructions:

- This examination paper has 1 page 2 faces (including this page).
- Condition of Examination Closed Book No dictionary non-programmable calculator is allowed
- Students are not allowed to be out of the exam room during the examination. Going to the restroom may result in a score deduction.
- Turn off all communication devices (mobile phone etc.) and leave them under your seat.
- Write your name, student and ID, clearly on this page answer sheet.
- Questions [100 marks]

Questions 1: Answer Only 5

Do the following statements agree with the information given in the text? Write
TRUE if the statement agrees with the information
FALSE if the statement contradicts the information
NOT GIVEN if there is no information on this

1. **The encryption algorithm of Affine Cipher is defined as: [FALSE] [5 marks]**
   C=E (K1, K2, p) = (K2 + p * K1) mod n = (K1 + p * K2) mod 26
2. **The encryption algorithm of Vigenere Cipher? [TRUE] [5 marks]**
   C = E (k, p) = (p + k) mod 26
3. **The word cryptography means hidden writing. [TRUE] [5 marks]**
4. **The encryption and decryption rules, called cryptography. [TRUE] [5 marks]**
5. **Encryption Algorithm: An algorithm which performs various substitutions and transformations on the plaintext. [TRUE] [5 marks]**
6. **Symmetric and Asymmetric ciphers both use a Public Key and a Private Key. [FALSE] [5 marks]**

Question 2: [25 marks]

Encrypt the message "AL MUSTAQBAL", using Transposed Keyword Mixed for a given keyword (EXAMINATION).

Answer

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

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

P= AL MUSTAQBAL

C=EM FTHUESBEM

Plaintext Alphabet	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
Plaintext Value	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

Al-Mustaqbal University
Course Title: MU0224104 Security of Computer and Networks

Name: **ID:** **Section C Date: 15.11.2023 Time: 60**

Question 3: [25 marks]
Encrypt the message "Create Secure Passwords", using a keyword Mixed cipher for a given keyword (letter) and key latter (A).

Answer

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

P= Create Secure Passwords

C: TPALSA QATUPA NLQQWMPRQ

Question 4: [25 marks]
Try to decrypt the ciphertext BEOKJDMSXZPMH with the key
9 0 1 7 23 15 21 14 11 11 2 8 9
Answer

Cipher	B	E	C	O	K	J	D	M	S	X	Z	P	M	H
Letter Value	1	4	2	14	10	9	3	12	18	23	25	15	12	7
Key	9	0	1	1	7	23	15	21	14	11	11	2	8	9
Sub -	26 9	26 0	26 1	26 1	26 7	26 23	26 15	26 21	26 14	26 11	26 11	26 2	26 8	26 9
Sum +	17 1	26 4	25 2	25 14	19 10	3 9	11 3	5 12	12 18	15 23	15 25	24 15	18 12	17 7
Mod 26	18	30	27	39	29	12	14	17	30	38	40	39	30	24
	18	4	1	13	3	12	14	17	4	12	14	13	4	24
Plaintext	S	E	B	N	D	M	O	R	E	M	O	N	E	Y

Plaintext Alphabet	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
Plaintext Value	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