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

Name: **ID:** **Section A Date: 15.11.2023 Time: 60 M**

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 ID, and section clearly on this page answer sheet.
- Questions [100 marks]

Question 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 = (K2 * p + K1) mod 26
2. The encryption algorithm of Caesar Cipher? [TRUE] [5 marks]
   C = E (k, p) = (p + k) mod 26
3. The encryption algorithm is defined as: [NOT GIVEN] [5 marks]
   C=E (K1, K2, p) = (K1 * p + K2) mod n = (K1 * p + K2) mod 26
4. Suppose you want to send messages from a sender, S, to a recipient, R. [TRUE][5 marks]
   If S entrusts the message to T, who then delivers it to R, T then becomes the transmission medium.
5. The encryption and decryption rules, called algorithms. [TRUE] [5 marks]
6. Only One key is required for two people to communicate via a symmetric. [TRUE][5marks]

Question 2: Encrypt the message "AL MUSTAQBAL", using Transposed Keyword Mixed for a given keyword (SENDER). [25 marks]

Answer

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

P: **AL MUSTAQBAL → C:SN CXKQSDASN**

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

Question 3: Encrypt the message "meet at ten in the park", using a keyword Mixed cipher for a given keyword (PROTOCOL) and key latter (A). [25 marks]

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

P: meet at ten in the park → C: HCCS PS SCI DI SBC KPNF

Question 4: [25 marks]

Try to decrypt the ciphe rtext: "IHHWVC SWFRCP", using the key: K1=9, K2=2

Hint: Use the table to find $K1^{-1}$

k_1	1	3	5	7	9	11	15	17	19	21	23	25
k_1^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Answer

P=D(K1**,** K2**, C)=** $K1^{-1}$ **(C –** K2 **) mod 26**, where $K1^{-1}$ = 3, K2=2

ciphertext	I	H	H	W	V	C	S	W	F	R	C	P
Value	8	7	7	22	21	2	18	22	5	17	2	15
C-2	6	5	5	20	19	0	14	20	3	15	0	13
3(C-2)	18	15	15	60	57	0	42	60	9	45	0	39
3(C-2) mod 62	18	15	15	8	5	0	16	8	9	19	0	13
	S	P	P	I	F	A	Q	I	J	T	A	N

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