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

Name: **ID:** **Section D 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 and ID, 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. **[FALSE] The encryption algorithm of Affine Cipher is defined as: [5 marks]**
   C=E (K1, K2, E) = (K2 * E + K1) mod n = (K1 * E + K2) mod 26
2. **[TRUE] The encryption algorithm of Caesar Cipher? [5 marks]**
   C = E (k, p) = (p + k) mod 26
3. **[FALSE] The word cryptanalyst means hidden writing. [5 marks]**
4. **[TRUE] A cryptanalyst's is trying to break an encryption. [5 marks]**
5. **[TRUE] Ciphertext: This is the scrambled message of the plaintext produced by the encryption algorithm as an output. [5 marks]**
6. **[TRUE] Asymmetric ciphers use a Public Key and a Private Key. [5 marks]**

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

Answer

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

P: AL MUSTAQBAL

C:MS DXLRMABMS

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 D Date: 15.11.2023 Time: 60 M**

Question 3: [25 marks]
Encrypt the message "We are happy to succeed", using a keyword Mixed cipher for a given keyword (EDITION) 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
E	D	I	T	O	N	A	B	C	F	G	H	J	K	L	M	P	Q	R	S	U	V	W	X	Y	Z

P: We are happy to succeed

C: WO EQO BEMMY SL RUIIOOT

Questions 4: [25 marks]
Try to Encrypt the plaintext "*send more money*" with the key
9 0 1 7 23 15 21 14 11 11 2 8 9
Answer

s	e	n	d	m	o	r	e	m	o	n	e	y
18	4	13	3	12	14	17	4	12	14	13	4	24
9	0	1	7	23	15	21	14	11	11	2	8	9
1	4	14	10	9	3	12	18	23	25	15	12	7
B	E	C	K	J	D	M	S	X	Z	P	M	H

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