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

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

Instructions:

- This examination paper has 2 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]
   E=C (K1, K2, C) = (K2 * C + K1) mod n = (K1 * C + K2) mod 26
2. [FALSE] What is the encryption algorithm of Caesar Cipher? [5 marks]
   P = (C - k mod m) mod 26
3. [FALSE] A cryptanalyst's is trying to break an decryption. [5 marks]
4. [TRUE] Decryption Algorithm: An algorithm which allows for the receiver to obtain the plaintext back from the ciphertext. [5 marks]
5. [TRUE Symmetric ciphers use a Secret Key. [5 marks]
6. [TRUE] Symmetric and Asymmetric ciphers both use a Public Key and a Private Key. [5 marks]

Question 2: Encrypt the message "ALMUSTAQBAL", using Transposed Keyword Mixed for a given keyword (ACTION). **[25 marks]**

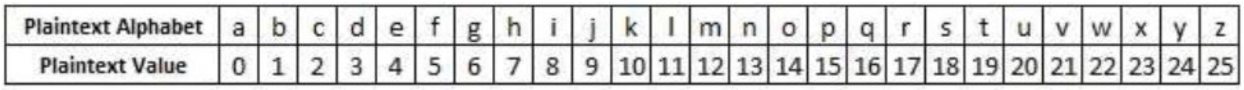
Answer

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

P= ALMUSTAQBAL

C:AELPOGAMBAE



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 E Date: 15.11.2023 Time: 60 M**

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

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

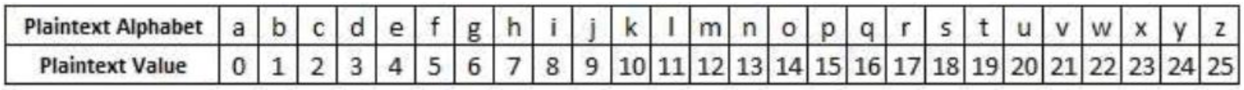
P: meet at ten in the park

C: JAAS LS SAK FK NLPH

Question 4: Try to decrypt the following Ciphertext= TAHRSPITX MAB **[25 marks]**

With Key= 76 48 16 82 44 3 58 11 60 5 48 88

Cipher	T	A	H	R	S	P	I	T	X	M	A	B
Letter Value	19	0	7	17	18	15	8	19	23	12	0	1
Key	76	48	16	82	44	3	58	11	60	5	48	88
Sub -	78 76	52 48	26 16	104 82	52 44	26 3	78 58	26 11	78 60	26 5	52 48	104 88
Sum +	2 19	4 0	10 7	22 17	8 18	23 15	20 8	15 19	18 23	21 12	4 0	16 1
Mod 26	21	4	17	39	26	38	28	34	41	33	4	17
	21	4	17	13	0	12	2	8	15	7	4	17
Plaintext	V	E	R	N	A	M	C	I	P	H	E	R



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