Al-Mustaqbal University

Course Title: MU0224104 Security of Computer and Networks

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

Instructions:

- This examination paper has 2 pages (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: Do the following statements agree with the information given in the text? Write **Answer Only 5**

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, p) = (K1 * p + K2) mod n = (K1 * p + K2) mod 26
2. **[TRUE] The encryption algorithm of Vernam Cipher? [5 marks]**
   C = E (k, p) = (p + k) mod 26
3. **[NOT GIVEN] The decryption algorithm is defined as: [5 marks]**
   p=D(K1, K2, C)= K1^{-1} (C - k2) mod n = K1^{-1} (C - k2) mod 26)
4. **[TRUE] The encryption and decryption rules, called cryptography. [5 marks]**
5. **[TRUE] Plaintext: The original intelligible message or data. [5 marks]**
6. **[TRUE] Only Two keys are required for two people to communicate via an asymmetric cipher? [5 marks]**

Question 2: [25 marks]

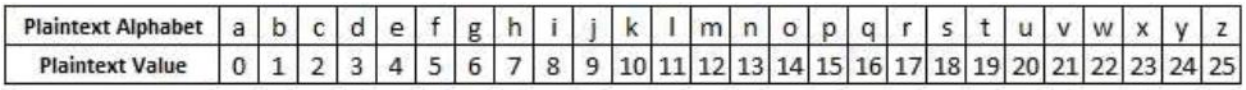
Encrypt the message "AL MUSTAQBAL", using Transposed Keyword Mixed for a given keyword (ALLOW).

Answer

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

P= AL MUSTAQBAL → AQ UWRVAHBAQ



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 B Date: 15.11.2023 Time: 60**

Question 3: [25 marks]

Encrypt the message “Security of Computer”, using a keyword Mixed cipher for a given keyword (GLOBAL) 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**
G	**L**	**O**	**B**	**A**	**C**	**D**	**E**	**F**	**H**	**I**	**J**	**K**	**M**	**N**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**

P: Security of Computer

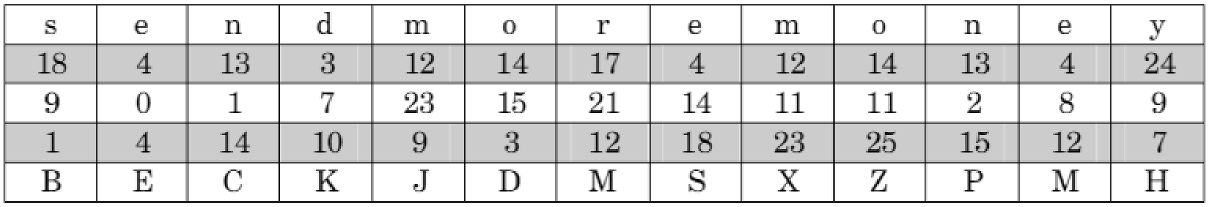
C: SAOURFTY NC ONKPUTAR

Question 4: [25 marks]

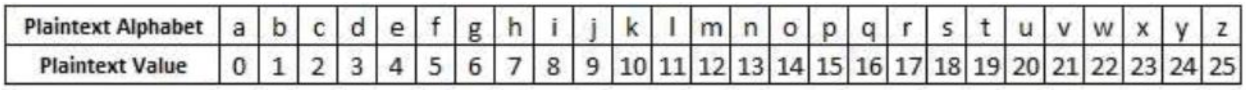
Try to Encrypt the plaintext “send more money” with the key

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