



UTM
UNIVERSITI TEKNOLOGI MALAYSIA

School of Professional and
Continuing Education
(SPACE)

DEPARTMENT OF COMPUTER SCIENCE & SERVICES
CENTRE FOR DIPLOMA STUDIES, SPACE

DSPD 2343

Computer Security

Lab Skill 1

LECTURER NAME

Mr. Sajid Shah

SECTION 44

STUDENT NAME & MATRIC ID

LEE XUAN HUI

A24DW0423

NGOO JUN YU

A24DW0429

Magen A/L Srinivasan

A24DW0105

Thenamuthean A/L Manimaran

A24dw1382

Lab 1 - Classical Cipher Encryption & Decryption (70 Marks)

UTM-Space is tasked with improving the security of their student records system. As part of this initiative, they are testing multiple cipher algorithms for protecting sensitive data. You are part of the cybersecurity team and have been asked to implement and demonstrate encryption and decryption processes for different classical ciphers.

Question 1: Manual Encryption & Decryption (30 Marks)

Perform encryption and decryption **step-by-step** for the given plain text and key using the following cipher algorithms. Show intermediate steps clearly to demonstrate your understanding.

Given Data:

- Plain Text: "Lecturer Name"
- Key: "Student Name"

1. Affine Cipher

- Formula: $E(P) = (a * P + b) \bmod 26$.
- Use values of a and b derived from the key.
- Show the numeric conversion, encryption and back to text.

Question 1 (Affine Cipher)

answer encryption = YMFABYVMV #
 answer decryption = SAJIDSHAH #

$a = \text{length of key} = 5$

$b = \text{numeric value of the first key letter M} = 12$

Encryption formula : $C = (5P + 12) \bmod 26$

Decryption formula : $P = 21(C - 12) \bmod 26$

Plaintext = SAJIDSHAH

Key = MAGEN

Encryption

Decryption

Ciphertext	Y	M	F	A	B	Y	V	M	V
	24	12	5	0	1	24	21	12	21
	18	0	9	8	3	18	7	0	7
Plaintext	S	A	J	I	D	S	H	A	H

2. Columnar Transposition Cipher

- Arrange plaintext in columns based on key length.
- Show column order, encryption and decryption grid.

Plaintext = SAJIDSHAHX

Key = THENA

Encryption

T (5)	H (3)	E (2)	N (4)	A (1)
S	A	J	I	D
S	H	A	H	X

Column (1) = DX

Column (2) = JA

Column (3) = AH

Column (4) = IH

Column (5) = SS

Ciphertext = DXJAAHIISS #

Decryption

T (5)	H (3)	E (2)	N (4)	A (1)
S	A	J	I	D
S	H	A	H	X

DX JA AH IH SS
 (1) (2) (3) (4) (5)

Plaintext = SAJIDSHAH #

3. Playfair Cipher

- Create 5×5 matrix using the key.
- Apply Playfair rules step-by-step for encryption and decryption.

Question 3

Plaintext: SAJID SHAH

Key: MAQEN

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

replace J with I: "SAIIDS SHAH"

= SA, IX, ID, SH, AH

Encryption Process

1) SA → RM	Ciphertext → RGLVLBLUDNC
2) IX → LV	
3) ID → LB	
4) SH → UD	
5) AH → NC	

Decryption Process

1) RM → SA	Decrypted text: SAIIDS SHAH
2) LV → IX	
3) LB → ID	
4) UD → SH	
5) NC → AH	

• Replace I with J = "SAJID SHAH"

Final answer

- Encryption: Plaintext "SAJID SHAH" → Ciphertext "RGLVLBLUDNC"
- Decryption: Ciphertext "RGLVLBLUDNC" → Plaintext "SAJID SHAH"

4. Beaufort Cipher

- Use tabula recta method with inverse Vigenère approach.
- Show letter-by-letter operation.

Question 4

Plaintext = SAJJOSHAH
 Key = JUNYUY

Plaintext (P)	S	A	J	J	O	S	H	A	H
	18	0	9	8	3	18	7	0	7
Key (K)	J	U	N	Y	U	J	U	N	Y
	9	20	13	24	20	9	20	13	24
	R	U	E	Q	R	R	N	N	J

$$C = (9 - 18) \pmod{26} = 17 (R)$$

$$C = (20 - 0) \pmod{26} = 20 (U)$$

$$C = (13 - 9) \pmod{26} = 4 (E)$$

$$C = (24 - 8) \pmod{26} = 16 (Q)$$

$$C = (9 - 18) \pmod{26} = 17 (R)$$

$$C = (20 - 0) \pmod{26} = 20 (U)$$

$$C = (13 - 9) \pmod{26} = 4 (E)$$

$$C = (24 - 8) \pmod{26} = 16 (Q)$$

$$C = (9 - 18) \pmod{26} = 17 (R)$$

$$C = (20 - 0) \pmod{26} = 20 (U)$$

$$C = (13 - 9) \pmod{26} = 4 (E)$$

$$C = (24 - 8) \pmod{26} = 16 (Q)$$

$C = RUEQRNNEJ$ (Ciphertext)

Decryption

$P = (key - ciphertext) \pmod{26}$

C	R	U	E	Q	R	R	N	N	J
	17	20	4	16	17	17	13	13	9
K	J	U	N	Y	U	J	U	N	Y
	9	20	13	24	20	9	20	13	24
P	18	0	9	8	3	18	7	0	7
	S	A	J	J	O	S	H	A	H

$C = ciphertext$ $K = key$ $P = plaintext$

5. Trifid Cipher

- Show $3 \times 3 \times 3$ cube mapping, encryption in groups and decryption.

Question 5

Plaintext = SAJIOSHAH Ciphertext = RUZ.AM.FFB

Key = YUANLIN

	1	2	3
1	M	A	H
2	N	L	I
3	B	C	D

	1	2	3
1	E	F	G
2	H	J	K
3	M	O	P

	1	2	3
1	Q	R	S
2	T	V	W
3	X	Z	.

	S	A	J
Layer	3	1	2
Row	1	1	2
Column	3	3	2

	I	O	S
Layer	1	1	3
Row	2	3	1
Column	3	3	3

	H	A	H
Layer	2	1	2
Row	2	1	2
Column	1	3	1

Ciphertext = RUZ.AM.FFB #

Decryption

Ciphertext = RUZ .AM FFD Plaintext = SAJIOSHAH

Key = YUANLIN

R = 312	.	= 1 1 3	F = 2 1 2
U = 112	A = 2 3 1	E	F = 2 1 2
Z = 332	M = 3 3 3	D = 1 3 1	
SAJ	I O S	H A H	

Decryption = SAJIOSHAH #

Question 2: Programming / Pseudocode and Flowcharts (40 Marks)

For each cipher below:

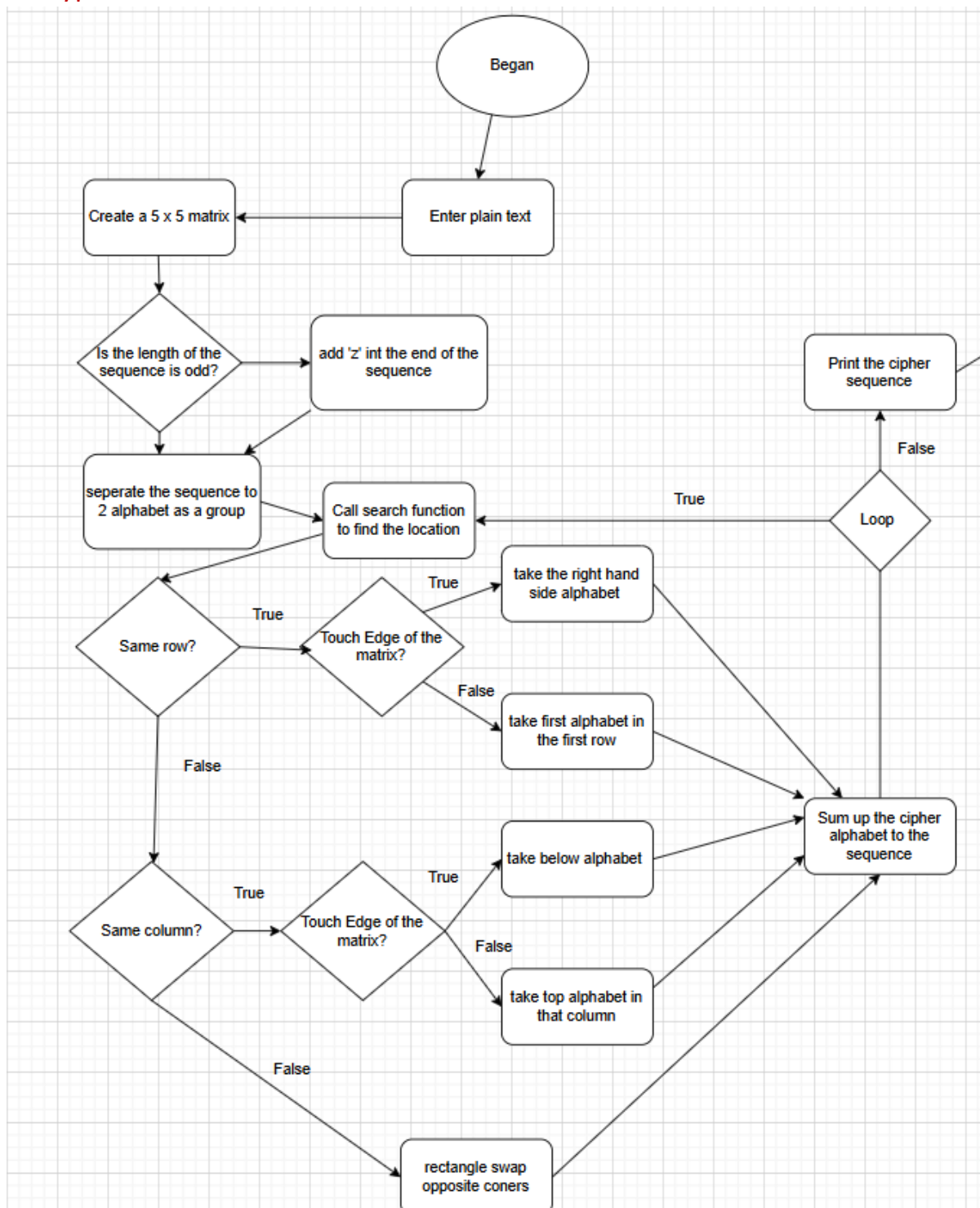
- Write a **program by using any language** (like C, C++, Python or any other) or **pseudocode** implementing both encryption and decryption.
- Draw a **flowchart** for the algorithm.

1. Rail Fence Cipher Flowchart

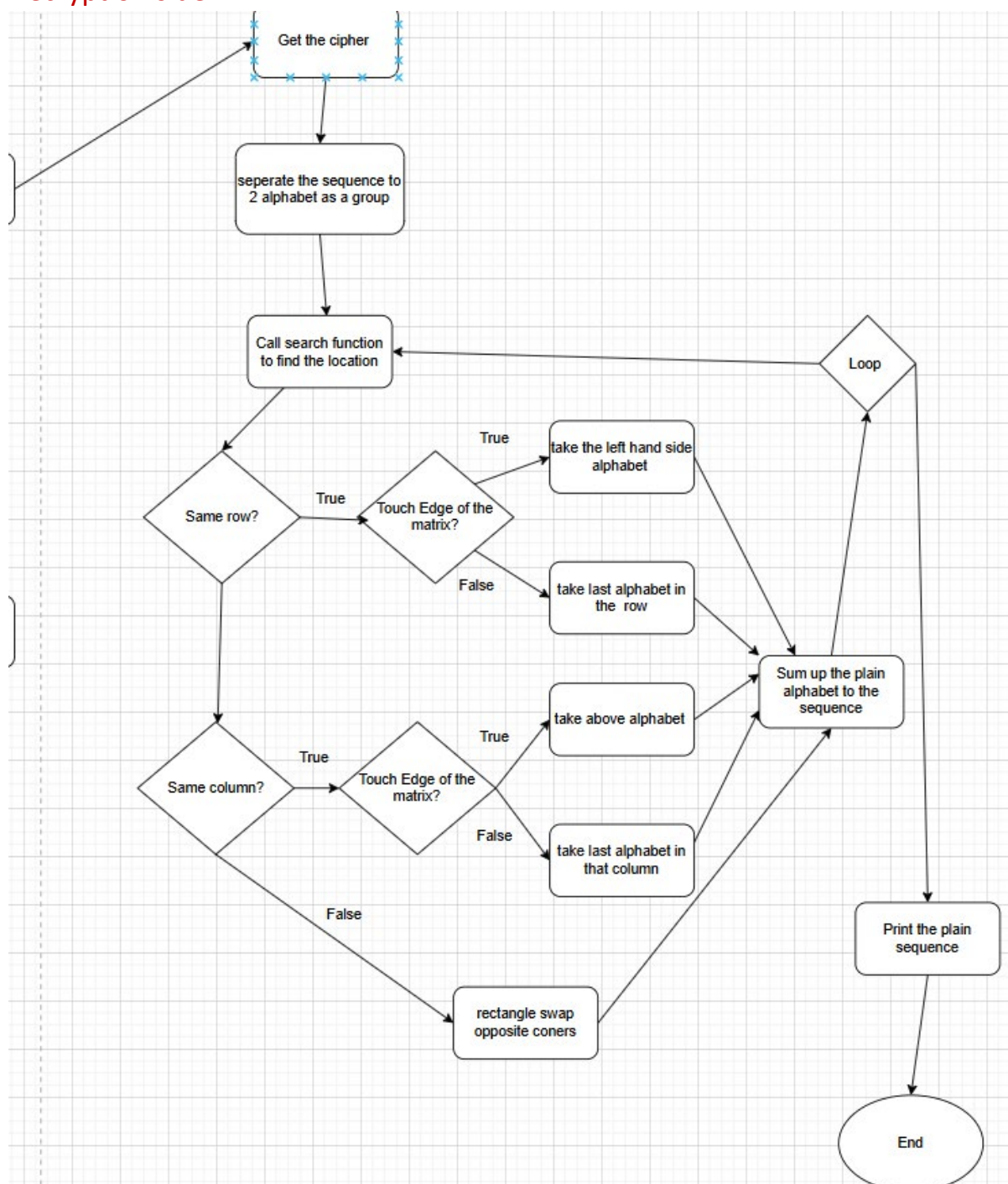


2. PlayFair Flowchart

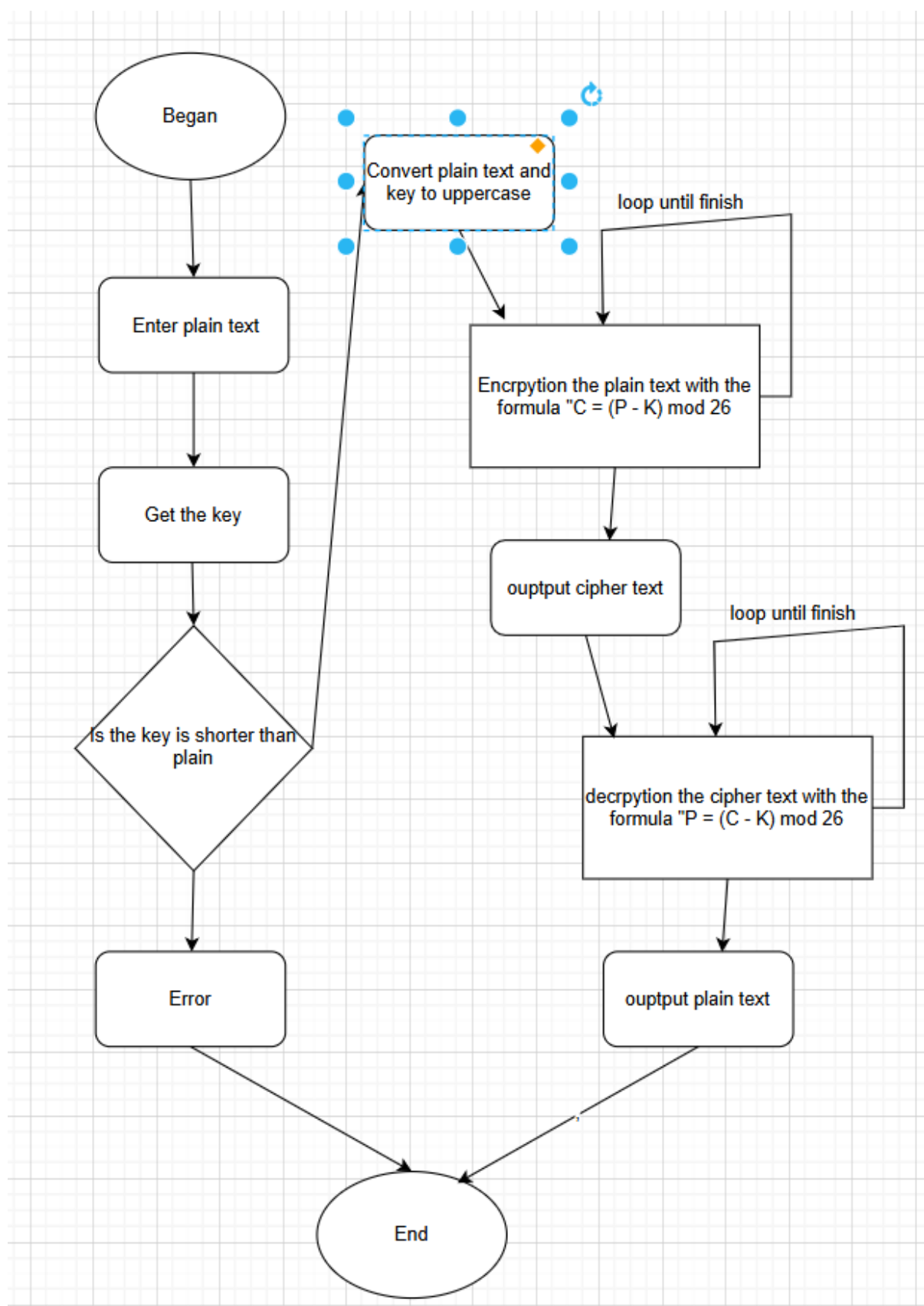
Encryption side:



Decryption side:



3. Running Key Flowchart



4. Bifid Flowchart

