



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

Question 1 (Affine Cipher)	
$a = \text{length of key}$	answer encryption = YM F A B Y V M U *
$= 5$	answer decryption = SAJID SHAH *
$b = \text{numeric value of the first key letter M} = 12$	
Encryption formula : $C = (5P + 12) \pmod{26}$	
Decryption formula : $P = 21(C - 12) \pmod{26}$	
Plaintext = SAJID SHAH	
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

Ciphertext = DXJAHHIHSS \*

Column (3) = AH

Column (4) = IH

Column (5) = SS

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  $5 \times 5$  matrix using the key.
- Apply Playfair rules step-by-step for encryption and decryption.

<u>Question 3</u>																										
Plaintext: SAJID SHAH																										
Key: MAGEN																										
<table style="margin-left: auto; margin-right: auto;"> <tr><td>M</td><td>A</td><td>G</td><td>E</td><td>N</td></tr> <tr><td>B</td><td>C</td><td>D</td><td>F</td><td>H</td></tr> <tr><td>I</td><td>K</td><td>L</td><td>O</td><td>P</td></tr> <tr><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td></tr> <tr><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td></tr> </table>		M	A	G	E	N	B	C	D	F	H	I	K	L	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	A	G	E	N																						
B	C	D	F	H																						
I	K	L	O	P																						
Q	R	S	T	U																						
V	W	X	Y	Z																						

replace J with I: "SAJIDSHAH"

= SA, IY, ID, Sh, Ah

#### Encryption Process

- 0) SA → RI
  - 1) IY → LV
  - 2) ID → LB
  - 3) SH → UD
  - 4) AH → NC
- Ciphertext → RGLVLBLUDNC

#### Description Process

- 1) RI → SA
- 2) LV → IY      Decrypted text: SAIYIDSHAH
- 3) LB → ID      Replace I with J = "SAJIDSHAH"
- 4) UD → SH
- 5) NC → AH

#### 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

$\rightarrow$  non-zeno

Plaintext: SAJID SHAH, 7901

MANZQITAZ = fIRSTNAME

Key: JUNYUVY

UJNLYV = key

Plaintext (P)	S	A	J	I	O	S	E	H	A	C	H		
key (k)	J	U	N	Y	V	J	U	N	Y				
	18	0	9	8	3	18	4	7	0	7			
	9	20	13	24	20	9	20	13	24	2	8		
	R	U	E	Q	R	R	N	N	J				

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

$$= 17 \pmod{R}$$

$$C = (20 - 3) \pmod{26}$$

$$= 17 \pmod{R} \quad \text{E} \quad \text{I}$$

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

$$= 20 \pmod{U}$$

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

$$= 17 \pmod{R} \quad \text{O} \quad \text{M} \quad \text{E}$$

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

$$= 4 \pmod{E}$$

$$C = (20 - 7) \pmod{26}$$

$$= 13 \pmod{N}$$

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

$$= 16 \pmod{Q}$$

$$( = (13 - 0) \pmod{26}$$

$$= 13 \pmod{N} \quad \text{D} \quad \text{I}$$

$$= RUEQRNNJ \pmod{\text{Ciphertext}}$$

$$( = (24 - 7) \pmod{26} \quad \text{E}$$

$$= 17 \pmod{R} \quad \text{X} \quad \text{E}$$

Decryption

R S I E

E, I, E)  $\leftarrow$  Z

U E H

(E, I, I)  $\leftarrow$  A

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

Plaintext: SAJID SHAH \*

U S I I

(E, C, I)  $\leftarrow$  I

C	R	U	E	Q	R	I	E	R	N	N	E	R	I
k	J	U	N	Y	U	S	I	C	J	U	N	I	C
	17	20	4	16	17	5	16	17	13	13	8	17	8
P	18	0	9	8	3	8	8	18	7	0	1	6	7
	S	A	J	I	D	E	I	S	H	A	H		

$$C = \underline{\text{ciphertext}}$$

$$k = \underline{\text{key}}$$

$$P = \underline{\text{plaintext}}$$

## 5. Trifid Cipher

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

Question 5

Plaintext = SAJIOSHAH

Key = YUANLIN

S I C	E I F	S E S R
E G C	I E C = A	S E E = B
1 8 1 2 0 3	E E E = M	S E S = S
1 MAHU	2 0 1	2 A S
2 N L 1		
3 B C 0		*

HANZOI2AS = not found

	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	I D S	H A H
Layer	(3 1 2)	(1 1 3)	(2 1 2)
Row	(1 1 2)	(2 3 1)	(2 1 2)
Column	(3 3 2)	(3 3 3)	(1 3 1)

812 112 332 113 231 333 212 212 131  
R V Z A M . F F B

Ciphertext = RUZ AM.FFB \*

Decryption

Ciphertext = RUZ .AM FFD

HANZOI2AS = trifid9

YUANLIN = key

R = 312

\* = 1 1 3

F = 2 1 2

V = 112

A = 2 3 1

F = 2 1 2

Z = 332

M = 3 3 3

E = 1 3 1

S A J

I D S

A U H A H I

Decryption = SAJIOSHAH \*

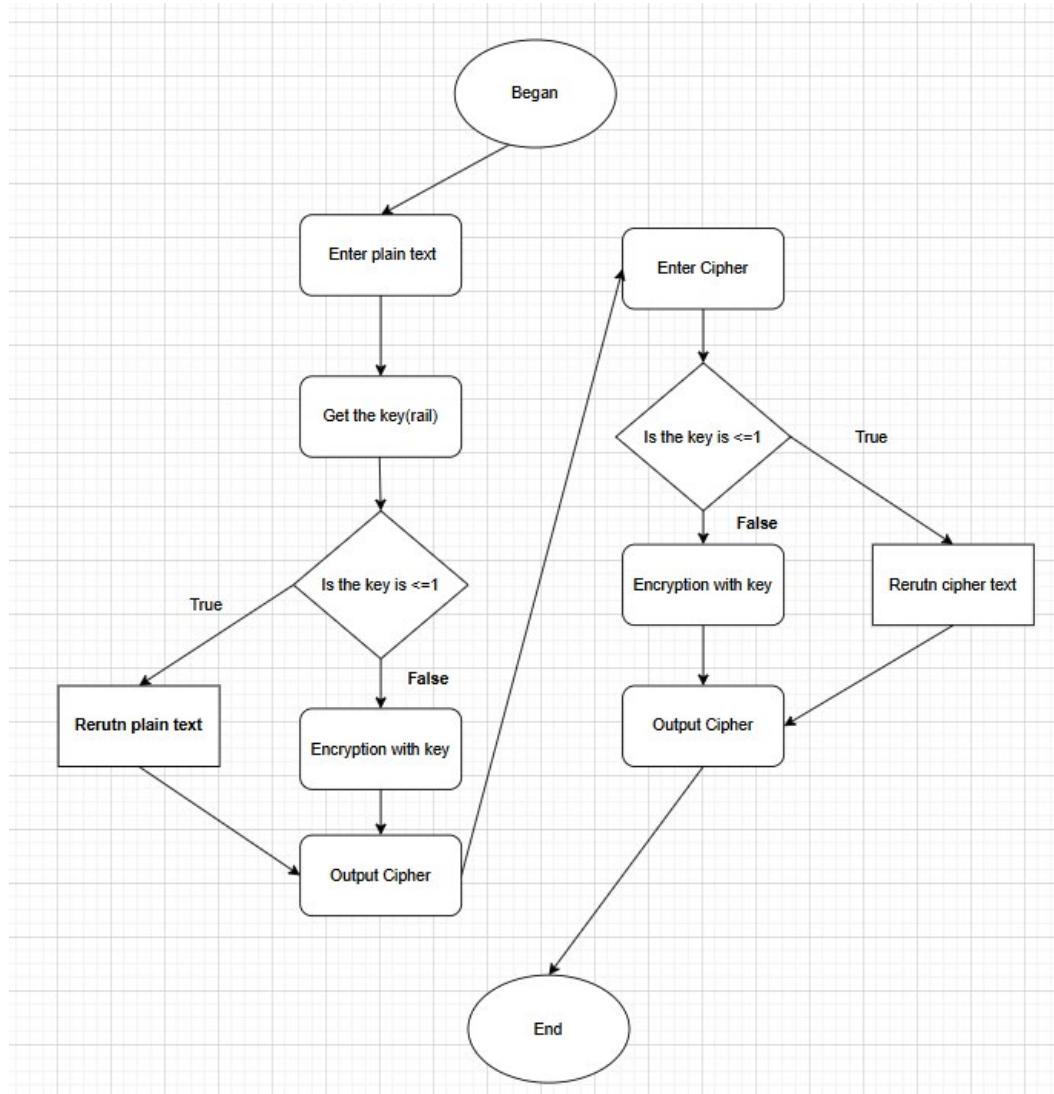
Q	S	B	E
---	---	---	---

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

For each cipher below:

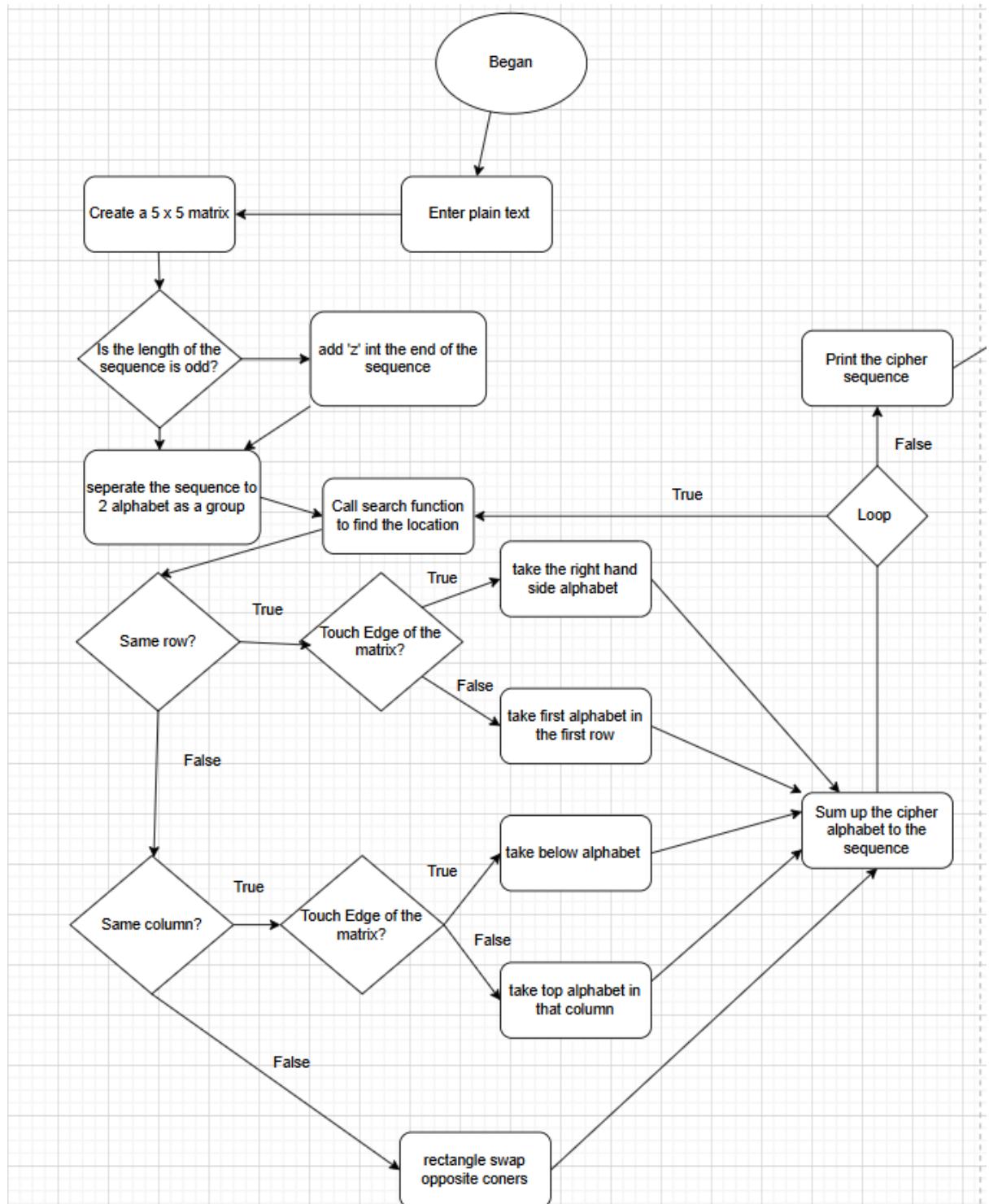
- Write a **program by using any language** ( like C, C++, Python or any other) or **pseudocode** implementing both encryption and decryption.
- Draw a **flowchart** for the algorithm.

#### 1. Rail Fence Cipher Flowchart

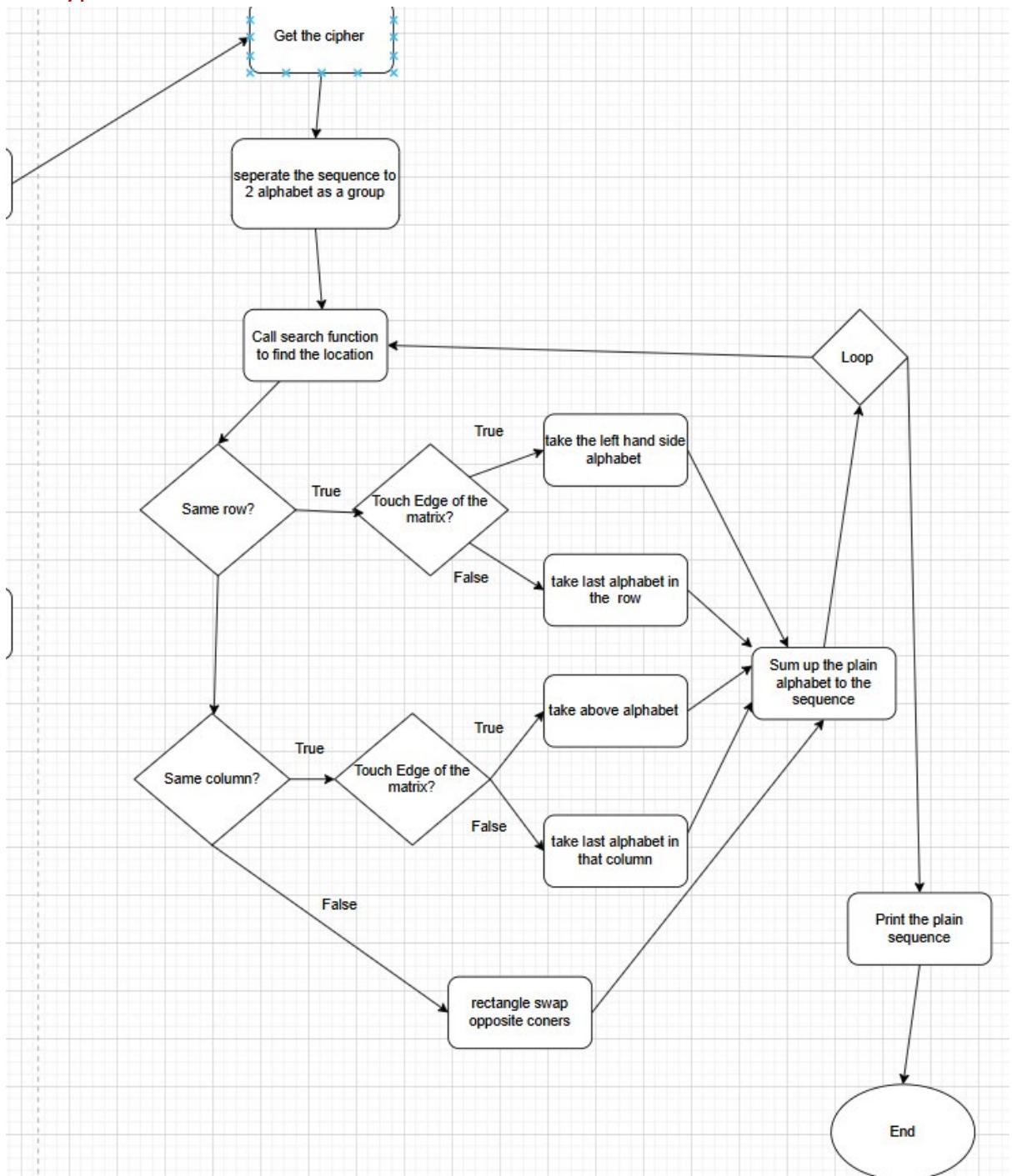


## 2. PlayFair Flowchart

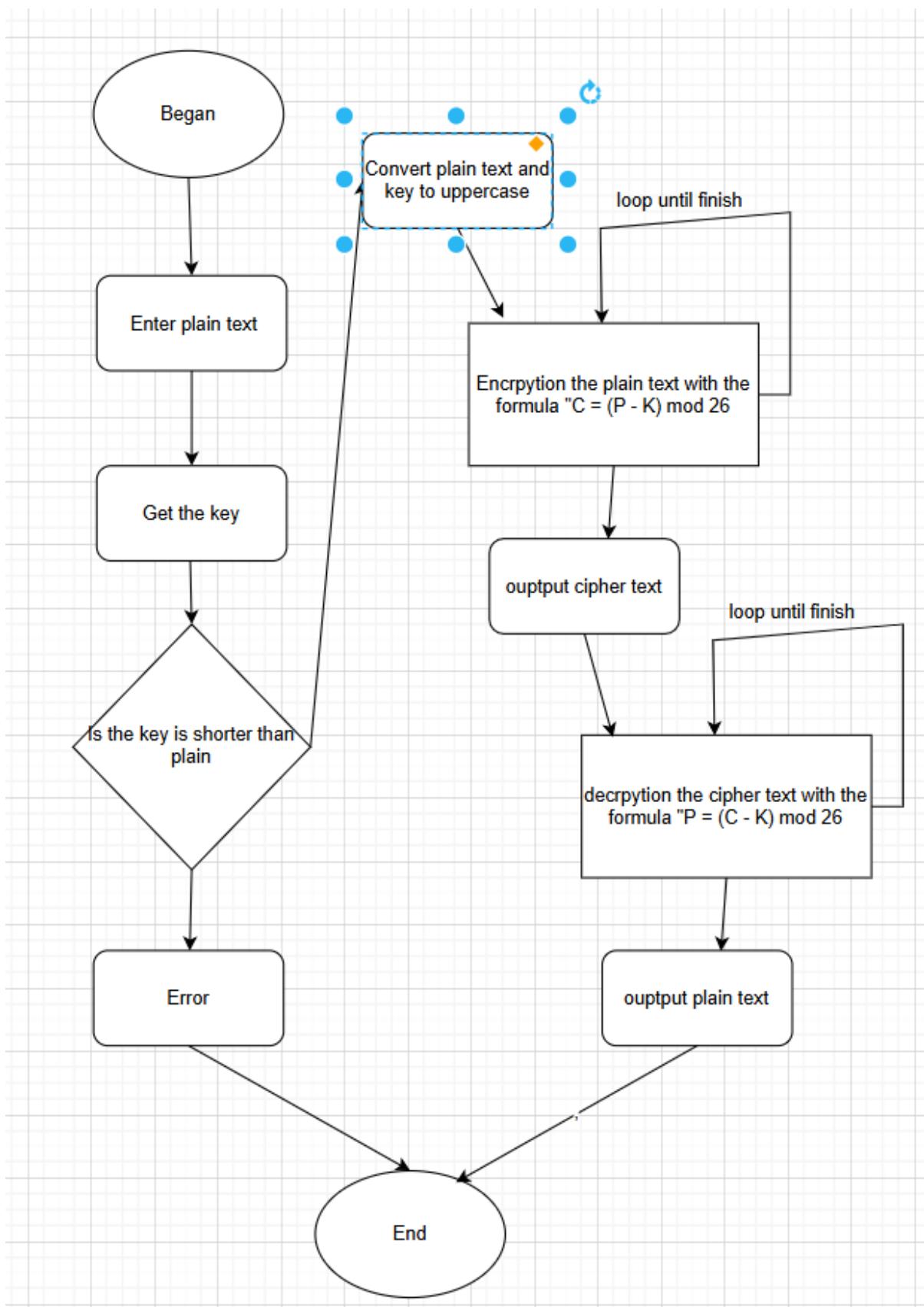
Encryption side:



## Decryption side:



### 3. Running Key Flowchart



#### 4. Bifid Flowchart

