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.

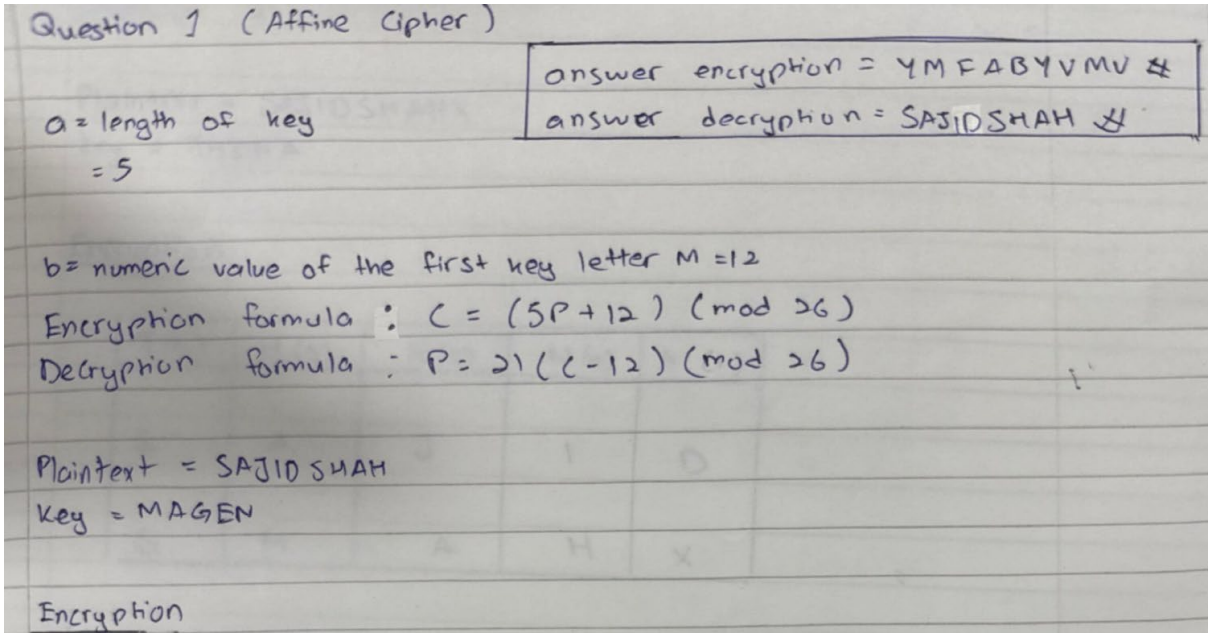
Question 1: Manual Encryption & Decryption (30 Marks)

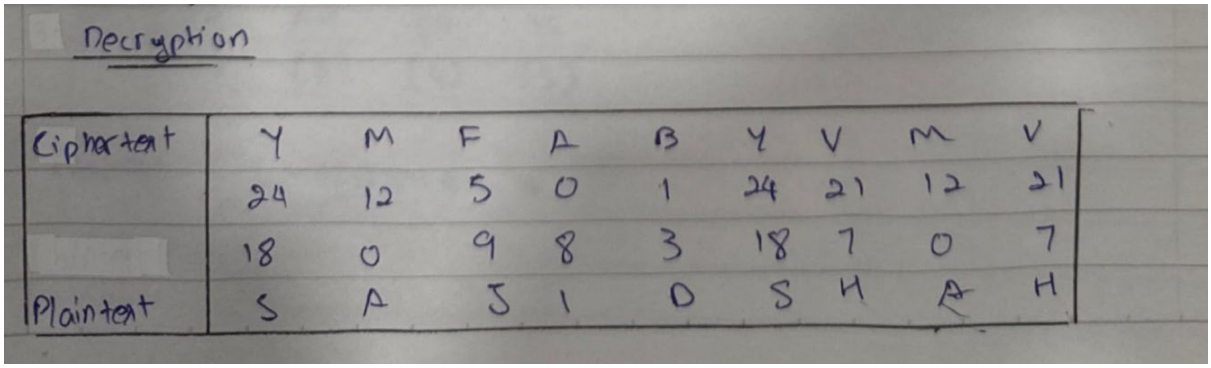
Perform encryption and decryption **step-by-step** for the given plain text and key using the following cipher algorithms. Show intermediate steps clearly to demonstrate your understanding.

Given Data:

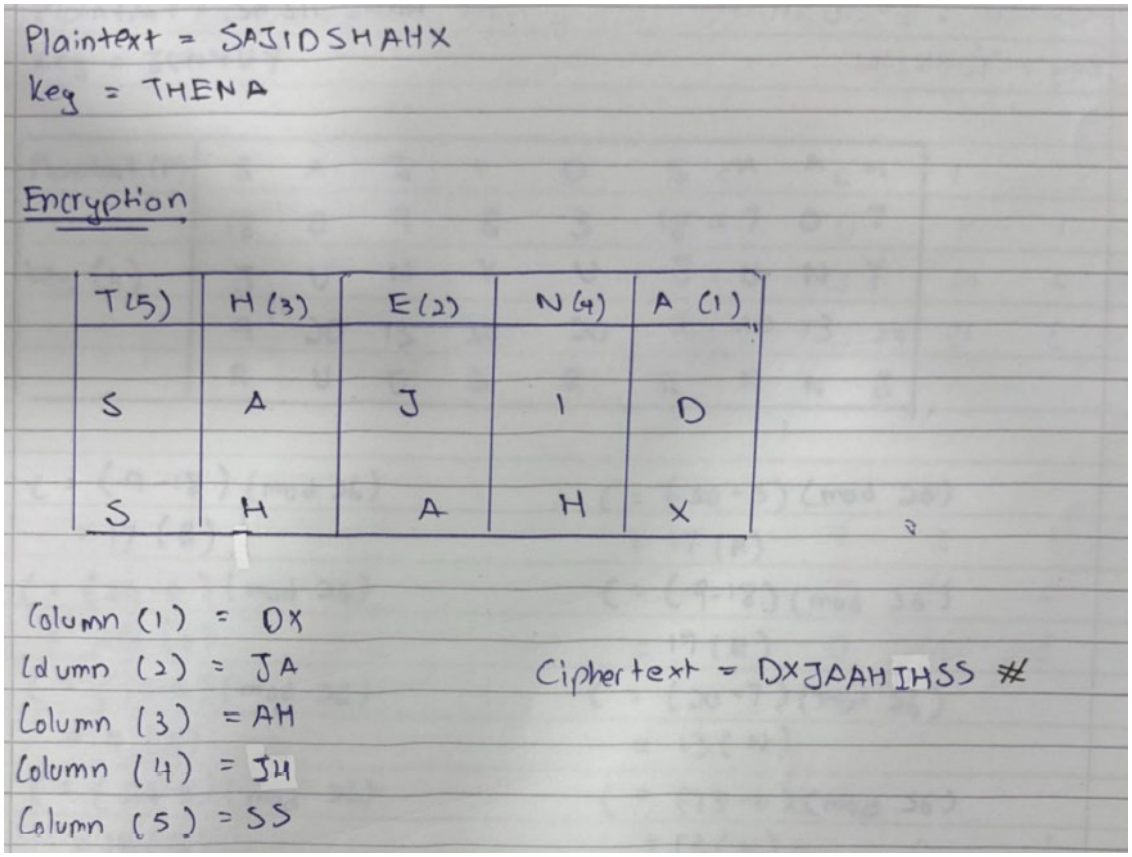
- Plain Text: "Lecturer Name"
- Key: "Student Name"

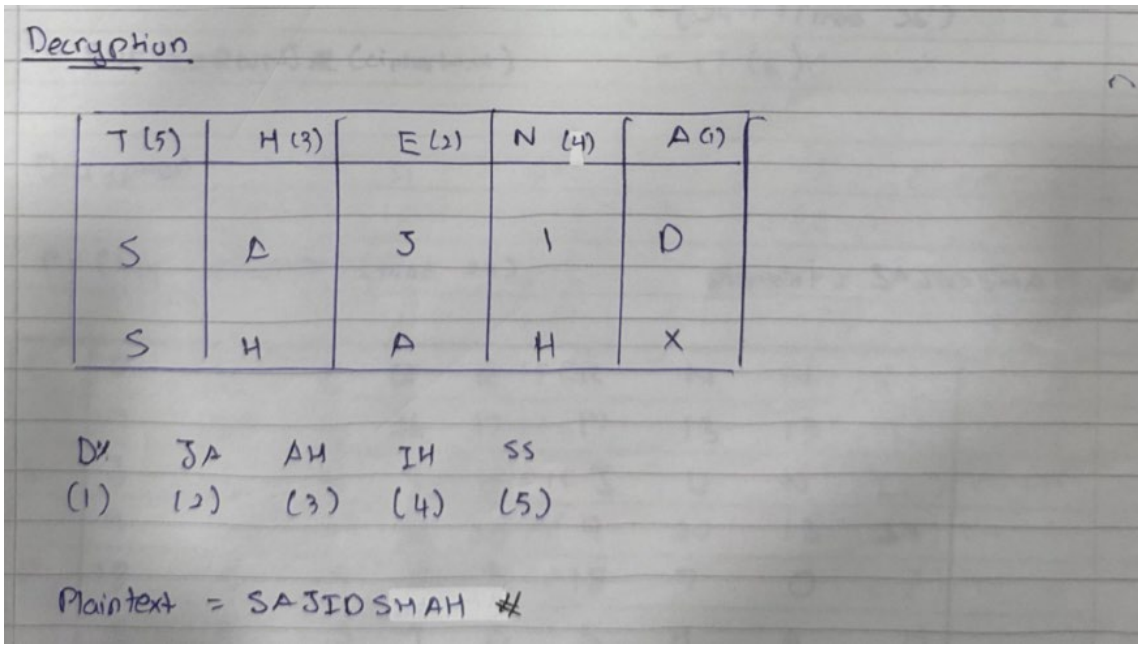
1. **Affine Cipher**
   - Formula: $E(P) = (a * P + b) \bmod 26$.
   - Use values of a and b derived from the key.
   - Show the numeric conversion, encryption and back to text.



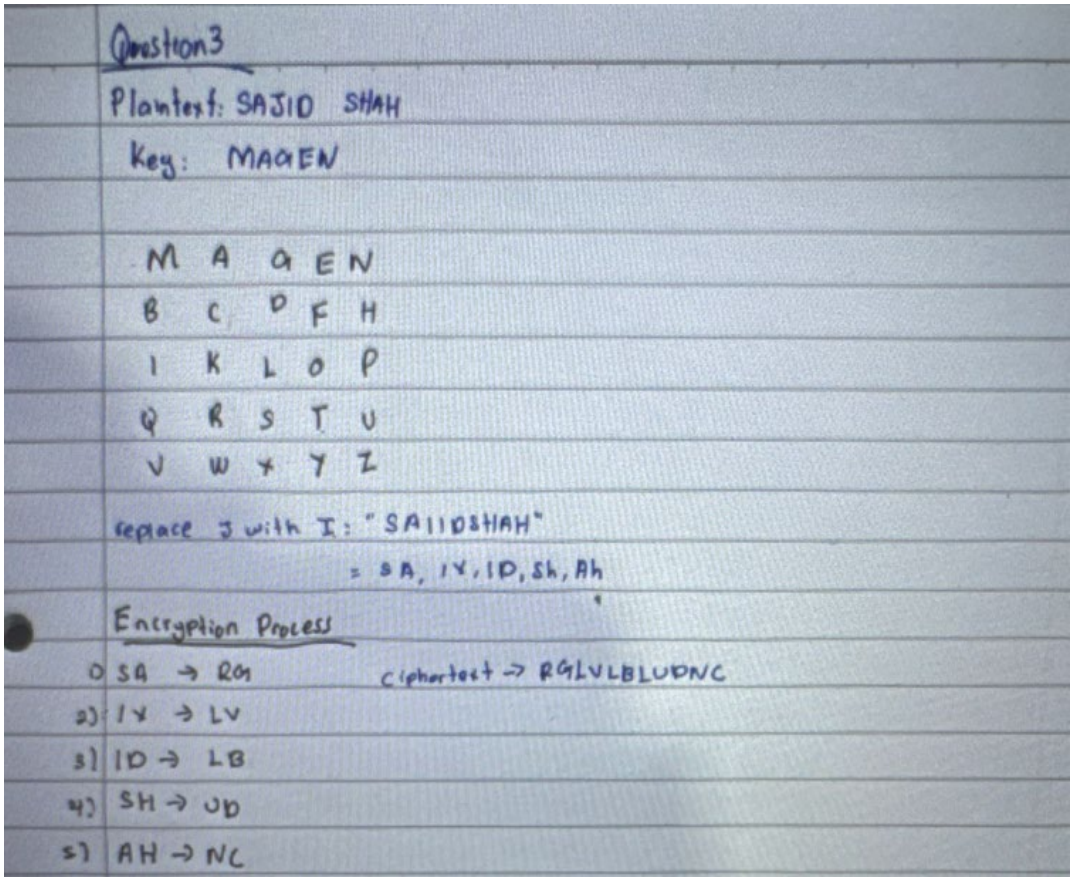


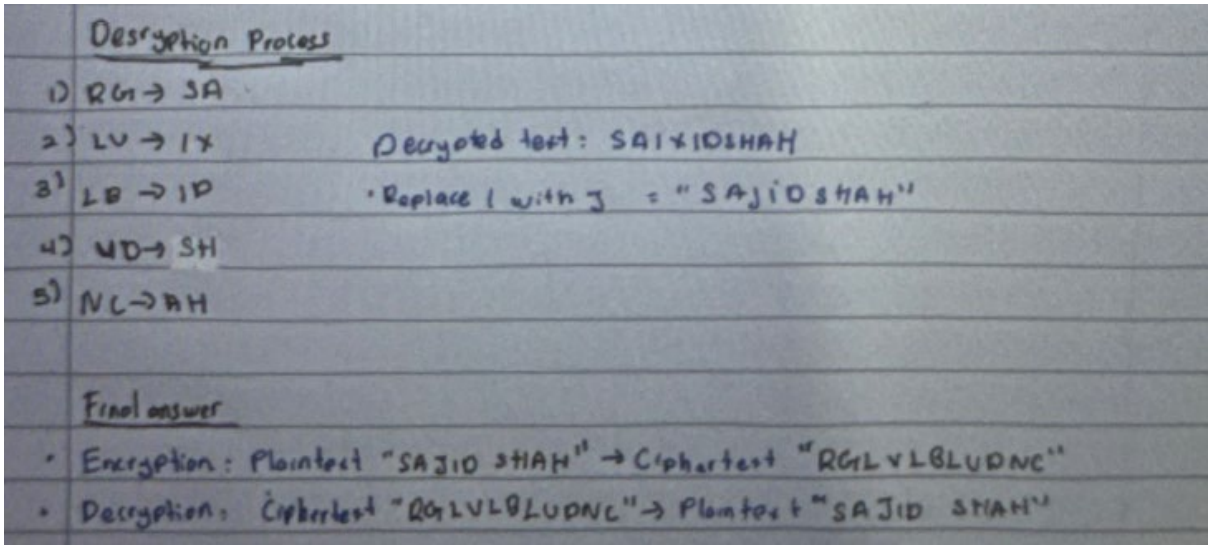
2. **Columnar Transposition Cipher**
   - Arrange plaintext in columns based on key length.
   - Show column order, encryption and decryption grid.



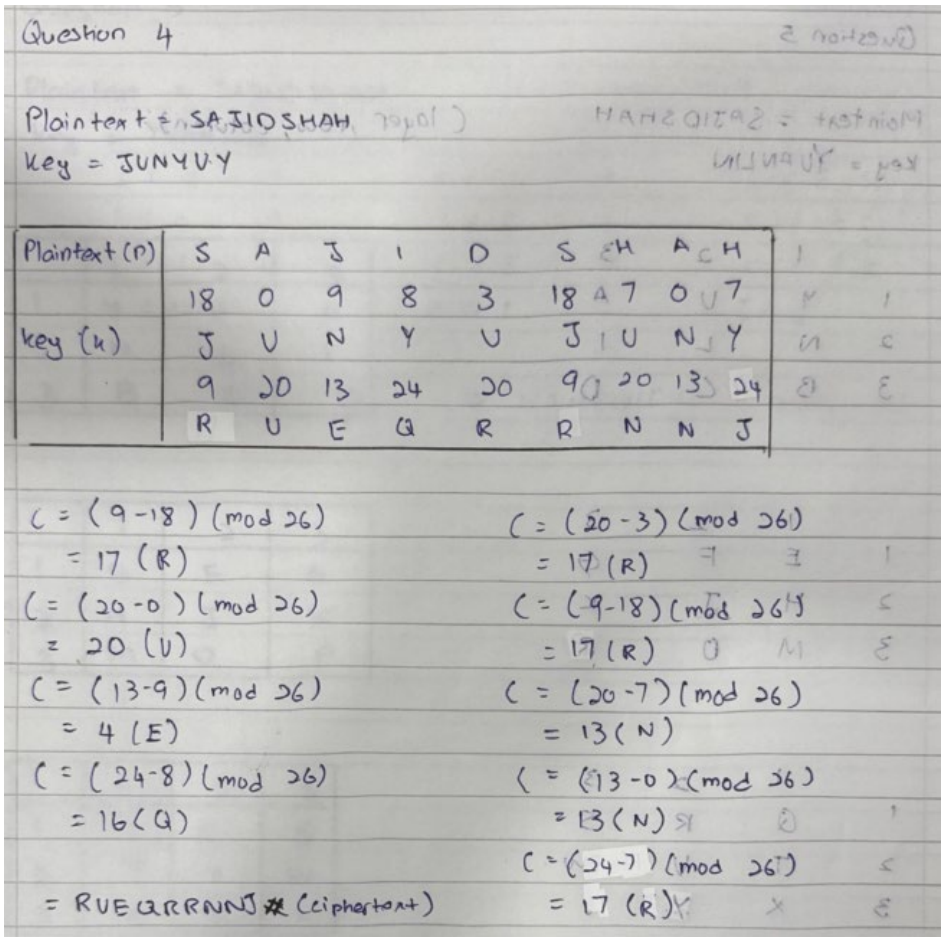


3. **Playfair Cipher**
   - Create 5×5 matrix using the key.
   - Apply Playfair rules step-by-step for encryption and decryption.





4. **Beaufort Cipher**
   - Use tabula recta method with inverse Vigenère approach.
   - Show letter-by-letter operation.



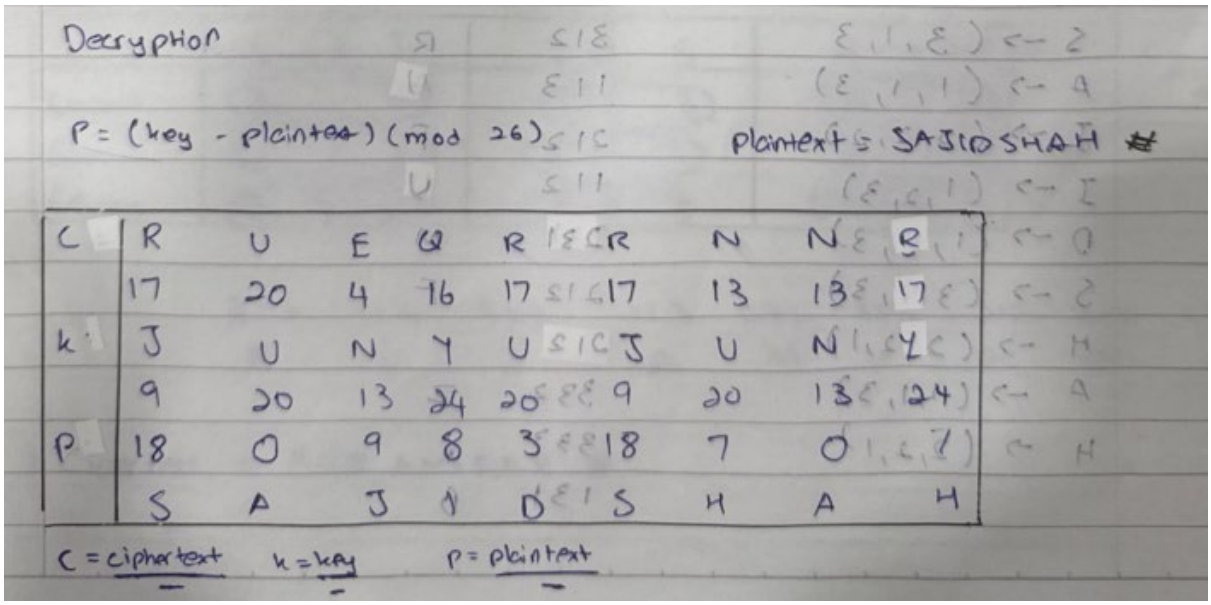
Question 4

Plaintext = SAJIOSHAH
key = JUNYUY

Plaintext (P)	S	A	J	I	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) (mod 26)
= 17 (R)
C = (20-0) (mod 26)
= 20 (U)
C = (13-9) (mod 26)
= 4 (E)
C = (24-8) (mod 26)
= 16 (Q)
C = (20-3) (mod 26)
= 17 (R)
C = (9-18) (mod 26)
= 17 (R)
C = (20-7) (mod 26)
= 13 (N)
C = (13-0) (mod 26)
= 13 (N)
C = (24-7) (mod 26)
= 17 (R)

= RUEQRRNNJ ✱ (ciphertext)



Decryption

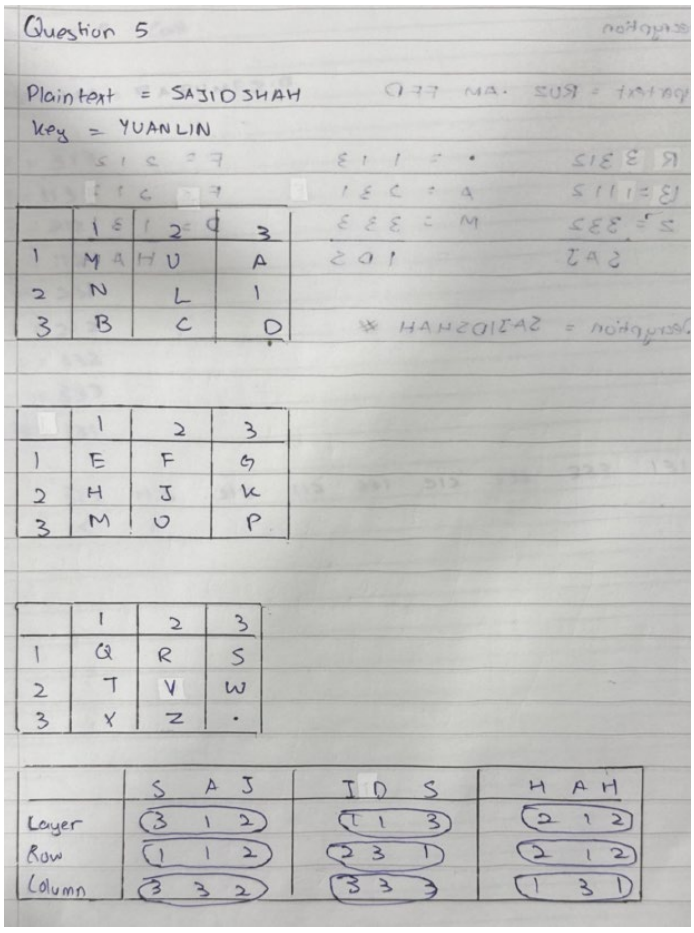
P = (key - plaintext) (mod 26)

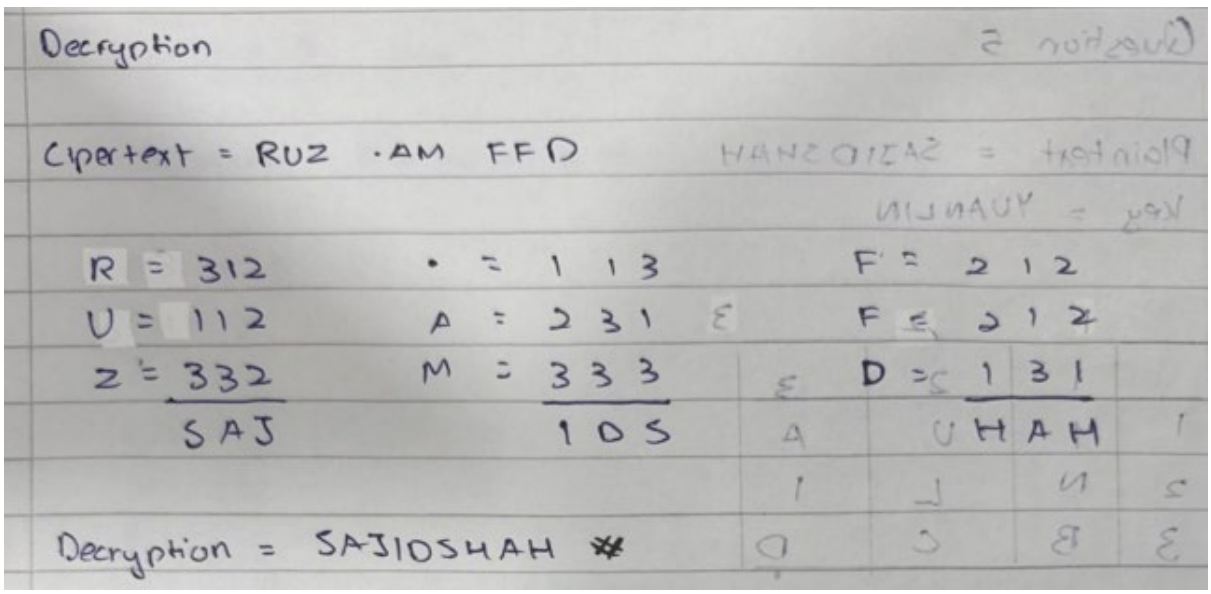
plaintext = SAJIOSHAH #

C	R	U	E	Q	R	R	N	N	J
	17	20	4	16	17	17	13	13	17
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	I	D	S	H	A	H

C = ciphertext k = key P = plaintext

5. **Trifid Cipher**
   - Show 3×3×3 cube mapping, encryption in groups and decryption.





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

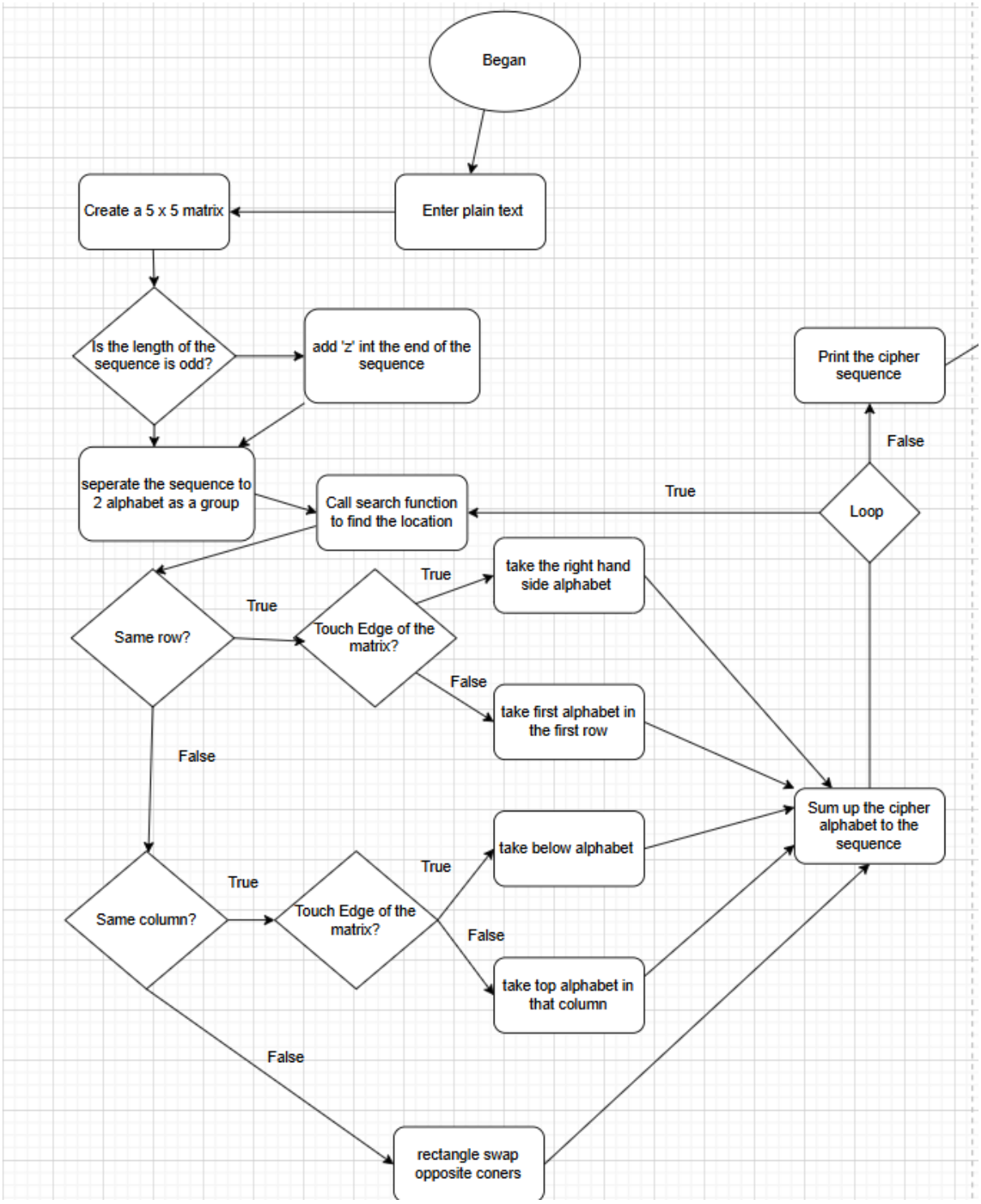
For each cipher below:

- 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.

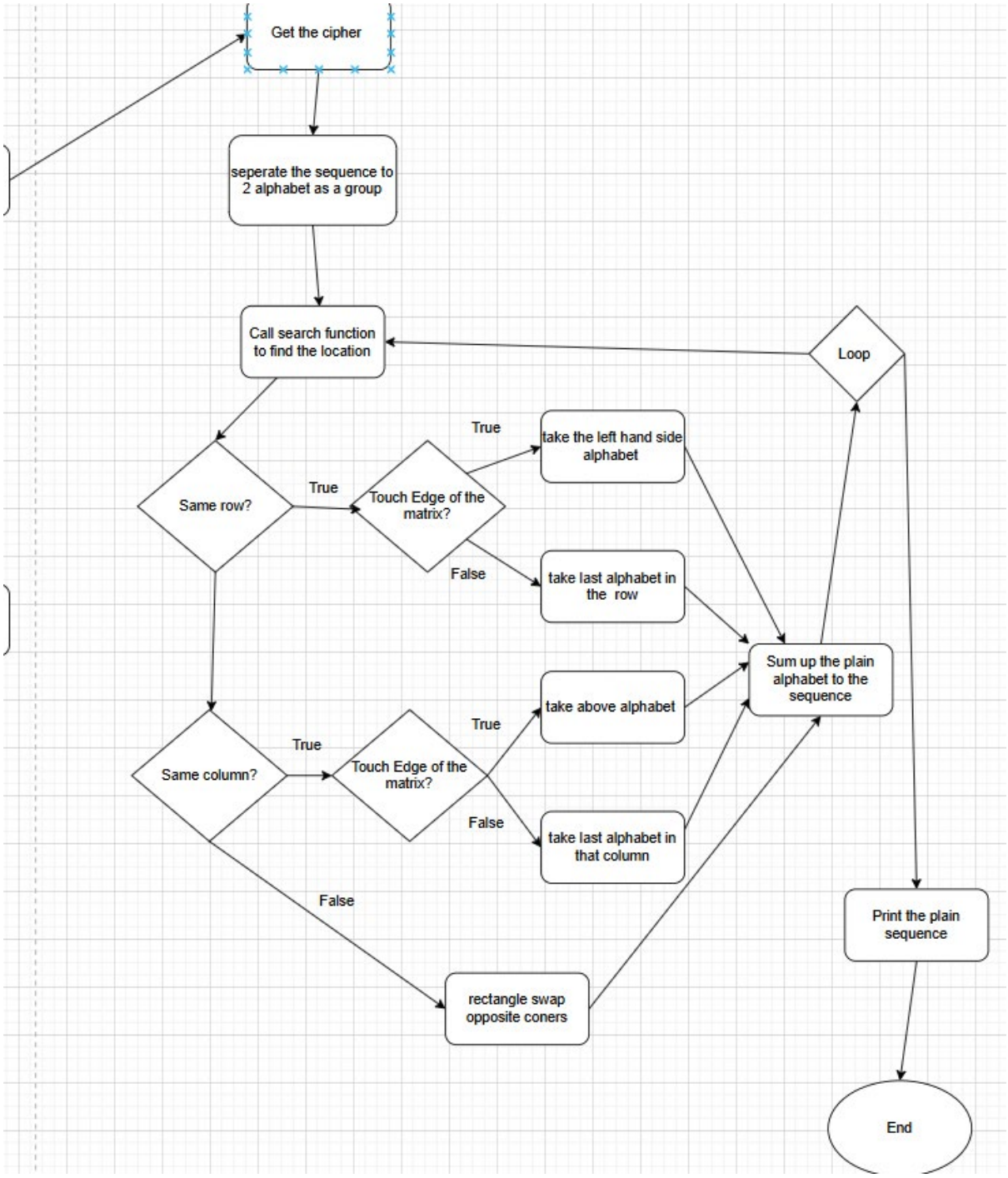
1. Rail Fence Cipher Flowchart

2. PlayFair Flowchart

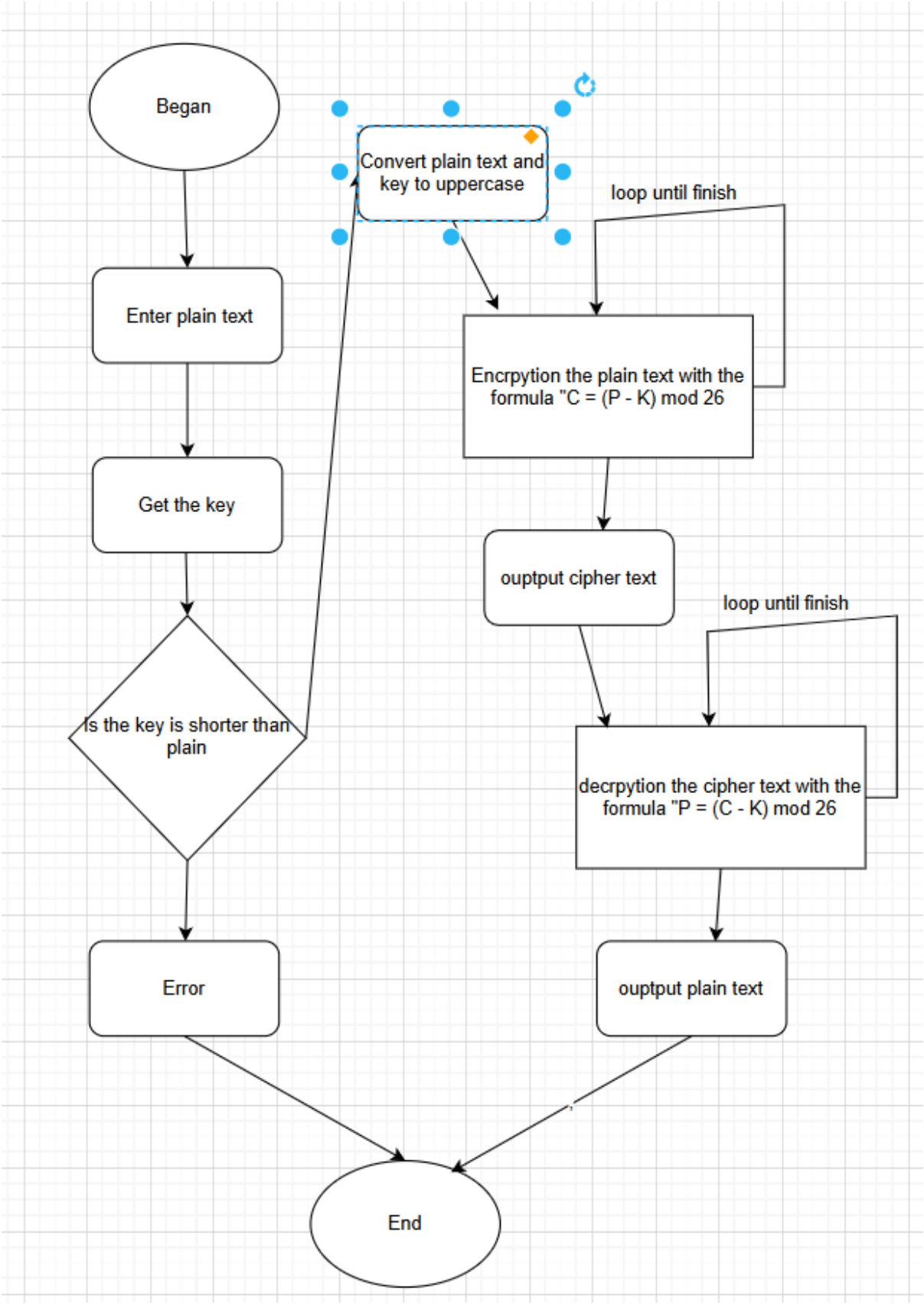
Encryption side:



Decryption side:



3. Running Key Flowchart



4. Bifid Flowchart