Caesar Cipher

PT, Key → given

Key — 4 → single letter/no.

E → 4

PT = N F S U Y N
13 5 18 20 24 13

Encryption

↳ CT = (PT + K) mod 26

PT → 13 5 18 20 24 13
\+ + + + + + +
Key → 4 4 4 4 4 4

17 9 22 24 28 mod 26

2

CT: R J W Y C

28 mod 26 = 2

26 | 28
−26
2

Decryption

↳ PT = (CT − K) mod 26

CT: R J W Y C
17 9 22 24 2
− − − − −
K: 4 4 4 4 4

2 − 4 = −2

13 5 18 20 −2 mod 26

13 5 18 20 24

N F S U Y → PT

= (26 − 2) mod 26
= 24 mod 26
= 24

X

− 2 mod 26

(26 − 2) mod 26

Monoalphabetic Cipher

Encryption $CT \rightarrow (PT + K) \bmod 26$

PT: CYBER

K: MCFAI

PT → 2 24 1 4 17

K → 12 2 5 0 8

14 26 6 4 25

mod 26

14 0 6 4 25

CT → O A G E Z

Decryption

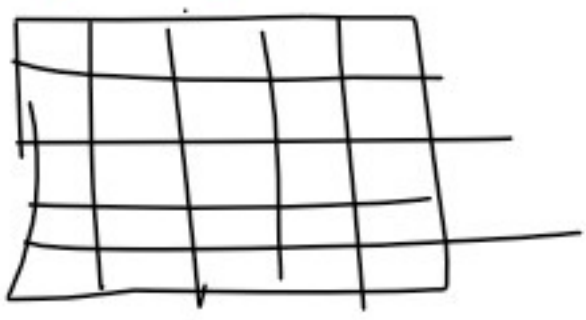
$PT = (CT - K) \bmod 26$

Vigenere Cipher

Plaintext : GEEKSFORGEEKS

Key : AYUSH

Playfair cipher



i) 5 × 5 matrix – key

ii) I/J combine

iii) no letters repeat

iv) If letter repeat, add filler letter
X or Z

v) 2-2 pairs

I) If letter are in same row
1 → 1 element right, wrap around

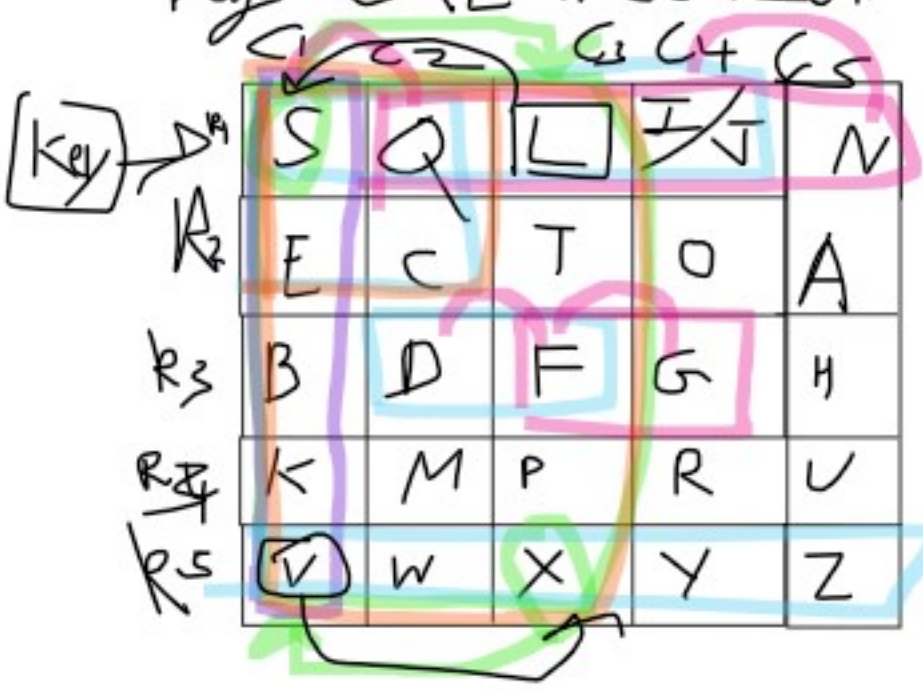
II) If letter are in same column
↓ → element below, wrap around

III) If letter form Rectangle ▭ or Square □
↔ swap

Q] T A I

PT- DFISSCSSBV

key - SQLINJECTION



PT → DF IS SC SX SB VX
CT → FG NQ QE LV EK WY

DF IS SC SX

for decryption

i) same row ← |
ii) same column ↑ |
iii) ▭ or □ ↔ |

Vigenère Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Table 2: Encoding English capital letters using integers from Z_{26}.

PT: chimu

Key: SPB SP

Encry → $CT = (PT + K) \bmod 26$

P → c h i m u

2 7 8 12 20

\+ + + + +

K → 18 15 1 18 15

20 22 9 30 35 mod 26

20 22 9 4 9

U W J E J

30 mod 26

1

26 | 30

26

4

35 mod 26

1

26 | 35

−26

9

Balloon