

225W040  $\Rightarrow$  section # 01  $\Rightarrow$  IS  $\Rightarrow$  Assignment

$\Rightarrow$  Plain text : message

(a) OTP  $\Rightarrow$  (one Time Pad)

sol

Key = KeyKeyK

109	101	115	115	97	103	101
m	e	s	s	a	g	e
1101101	1100101	1110011	1110011	1100001	1100111	1100101
107	101	121	107	101	121	107
K	e	y	K	e	y	K
1101011	1100101	1110111	1101011	1100101	1110111	1101011

$$2^0 = 1$$

$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 8$$

$$2^4 = 16$$

$$2^5 = 32$$

$$2^6 = 64$$

Encryption  $\Rightarrow$  Applying XOR

1101101	1100101	1110011	1110011	1100001	1100111	1100101
1101011	1100101	1110111	1101011	1100101	1110111	1101011
<hr/>						
0000110	0000000	0000100	0011000	0000100	0010000	0001110

$\Downarrow$  This is the cipher text.

Decryption  $\Rightarrow$  Again Applying XOR to cipher.

0000110	0000000	0000100	0011000	0000100	0010000	0001110
1101011	1100101	1110111	1101011	1100101	1110111	1101011
<hr/>						
1101101	1100101	1110011	1101011	1100001	1100111	1100101

conclusion satisfied

(b) ceaser cipher

sol

plain text = message

shift  $\Rightarrow 3$

m	e	s	s	a	g	e
$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$	$\Downarrow$
p	h	v	v	d	j	h

cipher text = phvvdjth

(c) vigenere cipher

sol

plain text = message

key = keykeykey

$\frac{10}{m}$	$\frac{4}{e}$	$\frac{24}{s}$	$\frac{10}{s}$	$\frac{4}{a}$	$\frac{24}{g}$	$\frac{10}{e}$
----------------	---------------	----------------	----------------	---------------	----------------	----------------

k	e	y	k	e	y	k
---	---	---	---	---	---	---

Now, shifting the text:-

w i q c e e o

message  $\Rightarrow$  wiace<sup>e</sup>oo

A = 0

L = 17

B = 1

S = 18

C = 2

T = 19

D = 3

U = 20

E = 4

V = 21

F = 5

W = 22

G = 6

X = 23

H = 7

Y = 24

I = 8

Z = 25

J = 9

K = 10

L = 11

M = 12

N = 13

O = 14

P = 15

Q = 16

Date 6/8/25

22SW40 => IS -> Assignment

## IS #w

Plain Text = she went to the store

Key - problem, Bogus letter = v

### ① Encryption

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

Go & same R => →

Go & same C => ↓

Neither ⇔

=> making pair of 2 letters of P.T

sh	ew	en	ta	to	th	es	to	se
↓	↓	↓	↓	↓	↓	↓	↓	↓
xs	mv	Fv	us	sb	st	an	sb	pm

=> cipher Text => xs mv Fv us sb st an sb pm

### ② Decryption

xs	mv	Fv	us	sb	st	an	sb	pm
↓	↓	↓	↓	↓	↓	↓	↓	↓
sh	ew	en	ta	to	th	es	to	se

rules -> reverse  
of encryption

=> message (she went to the store.)

⌋ Bogus letter

=> (she went to the store) ✓

Both condition satisfied



22sw040 => section #01 => IS: Assignment

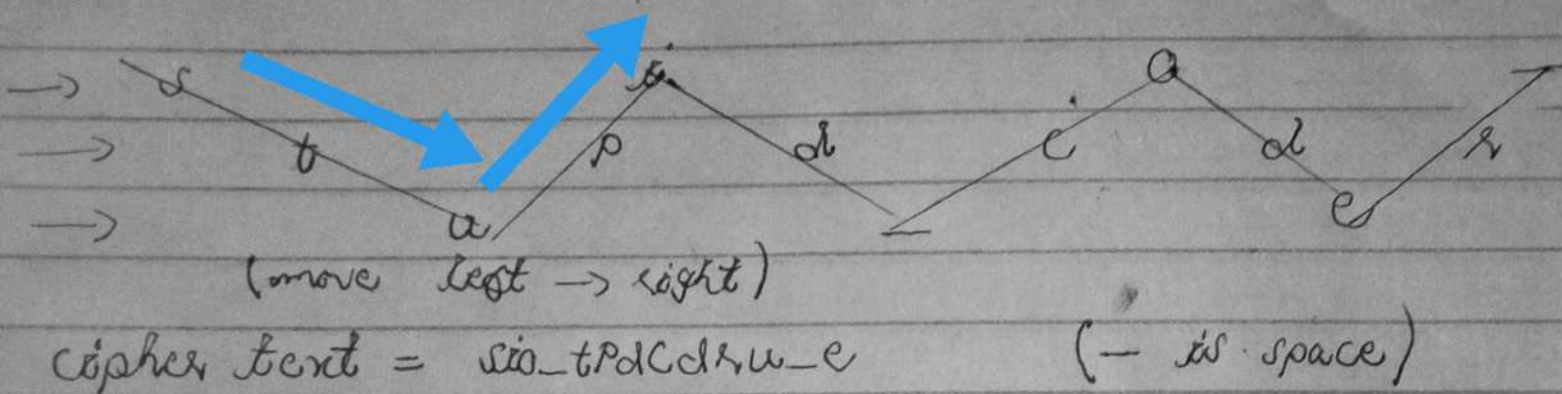
## Rail fence cipher

### Problem

=> message => stupid coder  
G04 3 spaces/rows/keys/rails

### Sol

#### ① Encryption



#### ③ Decryption

