21L-6260

Zain Al Abidin

IS Assignment

Q1

Since key = 3, we shift it 3 steps forward.

orginal	A	B	C	D	E	F	G	H	I	J	K	L	M	N
cipher	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

O	P	Q	R	S	T	U	V	W	X	Y	Z.		
L	M	N	O	P	Q	R	S	T	U	V	W		

HELLO WORLD ⟶ Original

EBIIL TLOIA ⟶ Cipher

We basically shift the whole alphabets 3 characters.

Q2

KHOOR ZUROG. cipher text

HELLO WORLD. original.

We basically read the key and then based on the key, we simply find the ciphers in the key and then replace that by original for each character.

2 Mono alphabetic Substitution

Q#1

S E C U R I T Y → original
L T E X K O Z N → ciphertext.

Q#2

L K K X Y L T X
S R R U F S E U

3 Vigenere Cipher

Q#1

~~B O X~~ K E Y
10 4 24..

A	T	T	A	C	K	A	T	D	A	W	N	original.
0	19	19	0	2	10	0	19	3	0	22	13	Value
10	4	24	10	4	24	10	4	24	10	4	24.	key (+)
10	23	43	10	6	34	10	23	27	10	26	37	(-26)
10	23	17	10	6	8	10	23	1	10	0	11	in case of overflows.
K	X	R	K	G	I	K	X	B	K	A	L.	cipher

So original text is
ATTACK AT DAWN
and the cipher text is
KXRKGIK X B KAL

Q#2

L	X	F	O	P	V	E	F	R	N	H	R.
11	23	5	14	15	21	4	5	17	13	7	17.
L	E	M	O	N	L	E	M	O	N	L	E

LEMON
11 4 12 14 13

for encryption we do the following

original + ~~cipher~~ key = cipher

in case of overflow

original + key - 26 = cipher.

so we simply reverse the formula.

11	23	5	14	15	21	4	5	17	13	7	17
11	4	12	14	13	11	4	12	14	13	11	4.
0	19	-7 26-7 =19	0	2	10	0	-7 26-7 =19	3	0	4 26-4 22	13
A	T	T	A	C	K	A	T	D	A	W	N.

4 Rail Fence

Q#1

D N E E

E E D H B S

F T A

DNEE EEDHBS FTA

row 1 row 2 row 3.

Q#2

4 8 8 4

TSNR|HSIETEYY|IAGMIVES|SNSA

T S N R

H S I E T E Y Y

I A G M I V E S

S N S A

This assignment is very easy.

CamScanner

5 Columnar Transposition

Q#1

3	1	4	2
S	A	V	E
␣	T	H	E
␣	D	A	T
A	␣	␣	␣

We read based on columns and then print based on the column number.

ATD EET SA VHA

Q#2

3	2	4	1
T	H	I	S
I	S	T	O
P	S	E	C
R	E	T	

This is top secret

CamScanner