

CSE-447 Assignment - 01

Submitted By:

Mohammad Shafkat Hasan

Section: 01

ID: 19101077

Date of Submission: 13th June 2023

Ans. To The Q.No.1

tiven,

Ciphertext > VSRQJHEREVTXDUHSDQWU

We know,

Caesar)s cipher is a shift-chipher

So, the key can be between \$ -2925

Trying all possible option we get incaningful

text using key = 3

Pla;ntext Ciphertext	A	В	c	D	E	F	G_1	#	I	h.	K	L	M)	N	0	P	a	R	5	τ	V	v	wx	14/2	2
Cip hertext	D	E	F	5/	#	I	3	K	L	M	N	0	P	a	4	5	T	νl	, v)	W	x []	1/2	- /-	BC	4

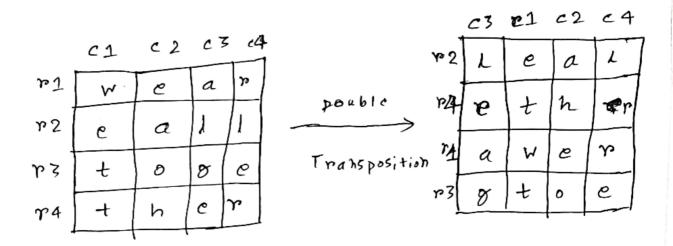
· Plaintext > SPONGEBOBSQUAREPANTR

(Ans)

Ans. To The a. No. 2

Given,

Plaintext > we are all together



i ciphertext > Lealethrawergtoe

[Ans)

Ans. To The Q.No. 3

Here,

Lc+ter > C h i k . L P 5 +
Binary > 000 001 010 011 100 101 130 111

(a)

Give, ciphertexts &ITLKF

We know,

Ciphertext + kcy = Plaintext

		×o	P		
	A	B	1	Y	L
	0	0		ð	
1	0	1	-	1	
J	2/	0	1	1	\
1	11	_2	1	0	/

ciphertext > 811 810 111 100 011 000

key → 100 011 010 110 111 100

pla;ntext > 111 001 101 040 100 100

- + ey = 100 011 010 110 111 100 C

CAns)

与

(6)

Given,

Ciphertext = *ITL KE

Plaintext > TILLER

 \dot{c} iphertext \rightarrow 011 010 111 100 011 000 \dot{c} \leftrightarrow 100 000 011 000 011 101

Plaintext -> 1 11 010 100 100 000 101

TILLER

: Fey = 1 00 000 011 000 011 101

CANS)

Ans. To The a . No. 4

 $\mathcal{X} = 1010$ 1010 1010 1010 101 $\mathcal{Y} = 1100$ 1100 1100 1100 11 $\mathcal{Z} = 1110$ 0001 1110 0001 1110 000

15+ Iteration:

 $m = major(x_8, y_{10}, z_{10})$ = maj(1, 0, 1) = 1

2 9 == m ->

 $\begin{array}{c} \chi_{3} = \chi_{23} \oplus \chi_{26} \oplus \chi_{27} \oplus \chi_{27} \oplus \chi_{29} \\ = 0 \oplus 4 \oplus 0 \oplus 1 \\ = 1 \oplus 1 = 0 \end{array}$

2 = 01 01 01 01 01 01 01 01 0

 $y_{10} \neq m$ y = 50 me as before $Z_{20} = = m \rightarrow$

27 0 2 20 0 222 O 2 22

= 1 () 0 () 0 () 0 = 1 () 0 = 1

2 = 1111 0000 1111 000 .1111 .000

2nd Iteration:

Y = 0.201 0101 0101 0100 Y = 1.200 1200 1200 1200 1200 1200 1200 Y = 1.22 0000 1212 0000 1212 0000

m = maj(xg, y10, Z10)= maj(0,0,1)

= 0

7 9 == m ->

70=1000100

= 1 1 = 0

2 = 0010 2010 1010 1010 101

420 = = m ->

y = y 20 1 421 = 1 1 1 = 0

y = 0 220 0220 0220 0220 0220 02

Z 20 7 m

z = same as before

2nd key bit
$$5 + \text{neam} = 925 \oplus 921 \oplus 222$$

$$= 919 1 \oplus 0$$

$$= 0 \oplus 0$$

$$= 0$$

3rd Iteration!

$$\mathcal{X} = 0010$$
 1010 1010 1010 1010 1010 01

 $\mathcal{Y} = 0110$ 0110 0110 0110 0110 01

 $\mathcal{Z} = 1111$ 5000 1111 0000 1111 000

3nd tey bit stream =
$$\chi_{19} \oplus \psi_{21} \oplus Z_{22}$$

= $0 \oplus 0 \oplus 0$
= 0

.. Generated tey Bit Stream = 0

(Ans)

Ans. To The Q. No. 5

- 0> 04 6: +5
- b) 6A bits
- c) 56.6;+5
 - d) 48 b; 45
 - e) 12 rounds
 - f) 8 5-boxes
 - 8) 6 bi+ 5
 - h) 4 bits