Inspiring Excellence

CSE-447
Assignment - 01

Submitted By:
Mohammad Shafkat Hasan
Section: 01
ID: 19101077

Date of Submission:
13th June 2023

ID : 17101077

Ans. To The Q.No.1

Given,

Ciphertext ⇒ V S R Q J H E R E V T X D U H S D Q W U

We know,

Caesar's cipher is a shift-cipher

So, the key can be between 1 - 25

Trying all possible option we get meaningful text using key = 3

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

∴ Plaintext ⇒ S P O N G E B O B S Q U A R E P A N T R

(Ans)

Ans. To The Q.No.2

Given,

plaintext ⇒ we are all together

	c1	c2	c3	c4
r1	w	e	a	r
r2	e	a	l	l
r3	t	o	g	e
r4	t	h	e	r

double Transposition

	c3	c1	c2	c4
r2	l	e	a	l
r4	e	t	h	r
r1	a	w	e	r
r3	g	t	o	e

∴ ciphertext ⇒ lealethrawergtoe

[Ans]

Ans. To The Q.No. 3

Here,

Letter ⇒	e	h	i	k	l	p	s	t
Binary ⇒	000	001	010	011	100	101	110	111

(a)

Given, ciphertext ⇒ KITLKE

Plaintext ⇒ THRILL

We know,

Ciphertext ⊕ key

= Plaintext

XOR

A	B	Y
0	0	0
0	1	1
1	0	1
1	1	0

ID: 19101077

(a)

	*	I	T	L	K	E
ciphertext →	011	010	111	100	011	000
key →	100	011	010	110	111	100
plaintext →	111	001	101	010	100	100

∴ key = 100 011 010 110 111 100 (Ans)

(b)

Given,

Ciphertext ⇒ *ITLKE

Plaintext ⇒ TILLER

ciphertext →	011	010	111	100	011	000
key →	100	000	011	000	011	101
plaintext →	111	010	100	100	000	101
	T	I	L	L	E	R

∴ key = 100 000 011 000 011 101 (Ans)

Ans. To The Q. No. 4

$x = 1010\ 1010\ 1010\ 1010\ 101$

$y = 1100\ 1100\ 1100\ 1100\ 1100\ 11$

$z = 1110\ 0001\ 1110\ 0001\ 1110\ 000$

1st Iteration:

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

$= maj(1, 0, 1)$

$= 1$

$x_8 == m \rightarrow$

$x_8 = x_{13} \oplus x_{14} \oplus x_{17} \oplus x_{19}$

$= 0 \oplus 1 \oplus 0 \oplus 1$

$= 1 \oplus 1 = 0$

$x = 0101\ 0101\ 0101\ 0101\ 010$

$y_{10} \neq m$ y = same as before

$z_{10} == m \rightarrow$

$z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22}$

$= 1 \oplus 0 \oplus 0 \oplus 0 = 1 \oplus 0 = 1$

$z = 1111\ 0000\ 1111\ 000\ 1111\ 000$

ID: 19101077

∴ 1st key bit stream

$= x_{18} \oplus y_{21} \oplus z_{27} = 0 \oplus 1 \oplus 0$

$= 1 \oplus 0$

$= 1$

2nd Iteration :

$x = 0101 \quad 0101 \quad 0101 \quad 0101 \quad 010$

$y = 1100 \quad 1100 \quad 1100 \quad 1100 \quad 1100 \quad 11$

$z = 1111 \quad 0000 \quad 1111 \quad 0000 \quad 1111 \quad 000$

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

$= 0$

$x_9 == m \rightarrow$

$x_0 = 1 \oplus 0 \oplus 1 \oplus 0$

$= 1 \oplus 1 = 0$

$x = 0010 \quad 1010 \quad 1010 \quad 1010 \quad 101$

$y_{10} == m \rightarrow$

$y_0 = y_{20} \oplus y_{21} = 1 \oplus 1 = 0$

$y = 0110 \quad 0110 \quad 0110 \quad 0110 \quad 0110 \quad 01$

$z_{10} \neq m$

$z =$ same as before

2nd key bit stream $= x_{19} \oplus y_{21} \oplus z_{22}$

$= 0 \oplus 1 \oplus 0$

$= 0 \oplus 0$

$= 0$

3rd Iteration:

$x = 0010\ 1010\ 1010\ 1010\ 101$

$y = 0110\ 0110\ 0110\ 0110\ 011$

$z = 1111\ 0000\ 1111\ 0000\ 1111\ 000$

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

$= maj(1, 1, 1)$

$= 1$

$x_8 == m \rightarrow$

$x_0 = 0 \oplus 1 \oplus 0 \oplus 1$

$= 1 \oplus 1 = 0$

$\therefore x = 0001\ 0101\ 0101\ 0101\ 010$

ID: 19101077

$y_{10} == z \rightarrow$

$y_8 = y_{20} \oplus y_{21}$

$= 0 \oplus 1 = 1$

$\therefore y = 1011 \quad 0011 \quad 0011 \quad 0011 \quad 0011 \quad 00$

$z_{10} == m \rightarrow$

$z_8 = 0 \oplus 0 \oplus 0 \oplus 0$

$= 0$

$\therefore z = 0111 \quad 1000 \quad 0111 \quad 1000 \quad 0111 \quad 100$

3rd key bit stream $= x_{18} \oplus y_{21} \oplus z_{22}$

$= 0 \oplus 0 \oplus 0$

$= 0$

$\therefore$ Generated key Bit Stream $= 0$

(Ans)

Ans. To The Q. No. 5

a) 64 bits

b) 64 bits

c) 56 bits

d) 48 bits

e) 16 rounds

f) 8 S-boxes

g) 6 bit s

h) 4 bits