Name of the Subject: E-COMMERCE & E-SECURITY Subject Code: IT-718

Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-7

Q2 Attempt Any Two

Q2 a

Seed Value $x_0 = 11$

$P = 13$

$Q = 17$

$n = P \times Q$
$= 13 \times 17$
$= 221$

Then the initial bits are calculated

$11^2 \pmod{221} = 121 \bmod 221$
$= 121 = 1111001$

$\therefore 121^2 \pmod{221} = 14641 \bmod 221$
$\therefore 55 = 110111$

$\therefore 55^2 \pmod{221} = 3025 \bmod 221$
$= 152 = 10011000$

$\therefore 152^2 \pmod{221} = 23104 \bmod 221$
$= 120 = 1111000$

Since $\log_2(\log_2(221)) = 2.961$

Taking least significant 3 bits form each outcome =

PTO

Section – II Date: 02/08/2021 Signature of Student: Page No: 01

Name of the Subject: E-COMMERCE & E-SECURITY Subject Code: IT-710

Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-VII

Random binary bits = 001 111 000 000

Q2 b

Plain Text = dd UN IV ER SI TY

Keyword = NADIAD

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

~~Plain Text DD UN IV ER~~

Plain Text	Dx	Dx	UN	IV	ER	SI	TY
	FD	FD	OB	NY	LW	TD	YI

So, Encryption :- FD FD OB NY LW TD YI

Section – II Date: 02/08/2021 Signature of Student:

Q3 (a).

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

$a = 2$, $b = 1$, m = No. of alphabet = 26

$E(x) = (ax+b) \bmod 26$

Original Text -	L	O	C	K	D	O	W	N
x	11	14	2	10	3	14	22	13
$(ax+b)$ $(2x+1)$	23	29	5	21	7	29	45	27
$(2x+1) \bmod 26$	23	3	5	21	7	3	19	1
Cipher Text =	X	D	F	V	H	D	T	B.

Cipher Text = XDFVHDTB.

(b)

PTO →

Name of the Subject: ECES Subject Code: IT-710

Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-7

(3) Plain Text- XDF UHD TBX

$$\text{Key} = \begin{vmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{vmatrix}$$

- Now for XDF

$$\therefore \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \times \begin{bmatrix} 23 \\ 3 \\ 5 \end{bmatrix} = \begin{bmatrix} 23+6+15 \\ 0+3+20 \\ 115+18+0 \end{bmatrix}$$

$$= \begin{bmatrix} 44 \\ 23 \\ 133 \end{bmatrix} \text{mod } 26$$

$= 44 \text{ mod } 26 = 18 - S$

$= 23 \text{ mod } 26 = 23 \quad X$

$= 133 \text{mod } 26 = 3 \quad D.$

- Now for UHD

$$\therefore \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \times \begin{bmatrix} 21 \\ 7 \\ 3 \end{bmatrix} = \begin{bmatrix} 44 \\ 19 \\ 147 \end{bmatrix} \text{mod } 26$$

$= 44 \text{mod } 26 = 18 = S$

$= 19 \text{ mod } 26 = 19 = T$

$= 147 \text{mod } 26 = 17 = R.$

Name of the Subject: ECES Subject Code: IT-718

Seat No: IT076 Student ID: 18ITUBN116 Branch/Sem: IT-7

– Now for IBX.

$$\therefore \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \times \begin{bmatrix} 19 \\ 1 \\ 23 \end{bmatrix} = \begin{bmatrix} 90 \\ 93 \\ 101 \end{bmatrix}$$

= 90 mod 26 = 12 = M
= 93 mod 26 = 15 = P
= 101 mod 26 = 23 = X.

$\boxed{\text{Cipher Text = SXD STR MPX.}}$