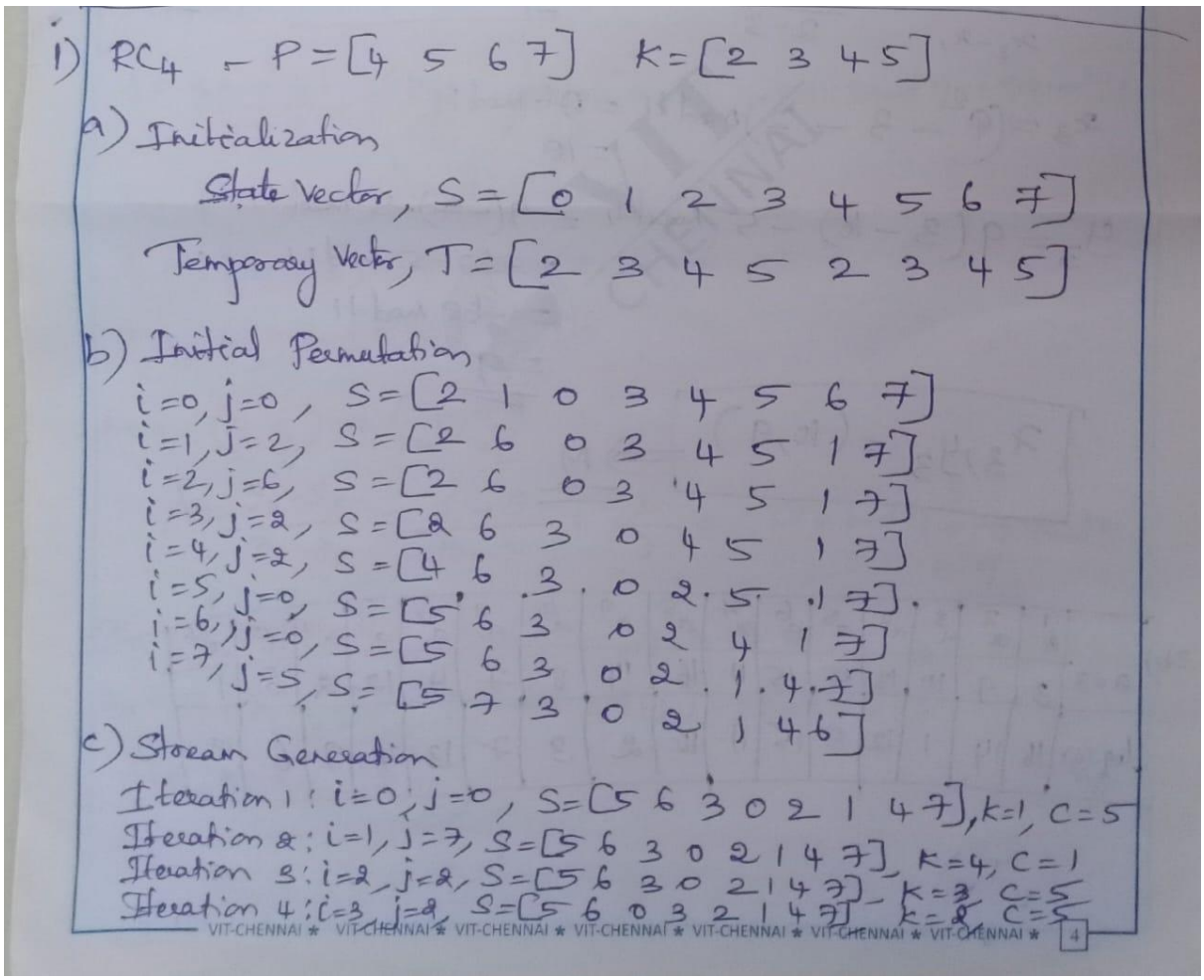
Cryptography and Network Security

FAT – F1 Key



1) RC_4 – P = [4 5 6 7] K = [2 3 4 5]

a) Initialization

State Vector, S = [0 1 2 3 4 5 6 7]

Temporary Vector, T = [2 3 4 5 2 3 4 5]

b) Initial Permutation

i=0, j=0, S = [2 1 0 3 4 5 6 7]
i=1, j=2, S = [2 6 0 3 4 5 1 7]
i=2, j=6, S = [2 6 0 3 4 5 1 7]
i=3, j=2, S = [2 6 3 0 4 5 1 7]
i=4, j=2, S = [4 6 3 0 2 5 1 7]
i=5, j=0, S = [5 6 3 0 2 4 1 7]
i=6, j=0, S = [5 6 3 0 2 4 1 7]
i=7, j=5, S = [5 7 3 0 2 1 4 6]

c) Stream Generation

Iteration 1: i=0, j=0, S = [5 6 3 0 2 1 4 7], k=1, C=5
Iteration 2: i=1, j=7, S = [5 6 3 0 2 1 4 7], K=4, C=1
Iteration 3: i=2, j=2, S = [5 6 3 0 2 1 4 7], K=3, C=5
Iteration 4: i=3, j=2, S = [5 6 0 3 2 1 4 7], K=2, C=5

2a) Extended Euclidean Algorithm

$17Y \equiv 1 \pmod{43}$

i	Dividend	Divisor	Quotient	Remainder	x_i	y_i
-1				43	1	0
0				17	0	1
1	43	17	2	9	$x_1 = x_{-1} - q_1 x_0 = 1 - 2\times0 = 1$	$y_1 = y_{-1} - q_1 y_0 = 0 - 2\times1 = -2$
2	17	9	1	8	$x_2 = x_0 - q_2 x_1 = 0 - 1\times1 = -1$	$y_2 = y_0 - q_2 y_1 = 1 - 1\times-2 = 3$
3	9	8	1	1	$x_3 = x_1 - q_3 x_2 = 1 - 1\times-1 = 2$	$y_3 = y_1 - q_3 y_2 = -2 - 1\times3 = -5$
4	8	1	8	0		

$x = 2, \; y = -5 = 38$

$17 \times 38 \equiv 1 \pmod{43}$

$\therefore \boxed{Y = 38}$

2b)

	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}
$a=3$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
$\log_{3}(a)$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

a) Digraph cipher or Playfair cipher.

Key: SECURITY

Message: HELLOWORLD

Playfair Matrix

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

Encryption:

HE LX LO WO RL DX

FU OQ MP XN SP HQ

4. p = 17, q = 11, e = 7, M = 88 (e: Public key)

1) $n = p \times q = 17 \times 11 = 187$

2) $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$

3) Compute 'd' $= 7^{-1} \bmod 160$

$\boxed{d = 23}$

4) Signature generation $S = M^d \bmod n$

$= 88^{23} \bmod 187$

$S = 11$

5) Verification $M = S^e \bmod n$

$= 11^7 \bmod 187$

$= 88$

Hence verified

b) ECC $-E_{11}(1,6)$, $G=(2,7)$, $n_B=2$, $P_m=(10,9)$, $k=2$

a) Public key $P_U = n_B G = 2(2,7) = (2,7)+(2,7)$

$\boxed{P_U = (5,2)}$

b) Encryption $C=[\overset{C_1}{(kG)}, \overset{C_2}{(M+kP_U)}]$

$C_1 = (5,2)$

$C_2 = \text{Infinity}$