Sister Nivedita University

Name: Farhad Dubey Sec: B

Enrollment No: 21112000012017

Dept: B.Tech CIE S.No: 58

Subject: Cryptography and Network Security

1. Explain Blowfish in details:

Ans: Blowfish is an encryption technique designed by Bruce Schneier in 1993 as an alternative to DES Encryption Technique. It is significantly faster than DES & provide a good encryption rate with no effective cryptanalysis technique found to date.

It is one of the 1st, secure block ciphers not subjected to any patents and hence freely available for anyone to use. It is symmetric block cipher algorithm.

blocksize : 64 bits

keysize : 32 - 448 bits variable size.

No. of subkeys : 18

No. of rounds : 16

No. of substitution boxes: 4 [each having 512

entries of 32 bits each]

Step 1: Generation of subkeys:

> 18 subkeys {P[0]... P[17]} are needed for both encryption & decryption.

> 18 subkeys are stored in Parray with each of 32 bit size.

> As:

P[0] : 243f 6a 88

P[1] : 85a 308 d3

⋮

P[17] : 8979 fb 1b

↳ 32-bit hexadecimal representation of initial values of subkeys.

* Now subkeys are changed with respect to the corresponding input key by XOR operation.

P[0] = P[0] XOR 1st 32-bits of i/p key

P[1] = P[1] XOR 2nd " " " "

P[2] =

⋮

P[i] = P[i] XOR (i+1)th 32-bits of i/p key.

> Resultant p-array holds 18 subkeys that is used during the entire encryption process.

* Step2: Initializing Substitution boxes: 4 substitution box are needed with each having 256 entries where entry is of 32-bit left part of plane 64 bit.

Step3: Encryption: Encryption function consists of 2 parts:

a) Rounds: consist of 16 rounds with each round taking inputs the plain text from previous round & corresponding subkey(

b) Left part of 32 bit is divided into 4 parts of 8 bit & passed through the s-box. Then bit output of 1 & 2 ~~the~~ is extracted. Extracted o/p is again applied via XOR with 3. & both box-4.

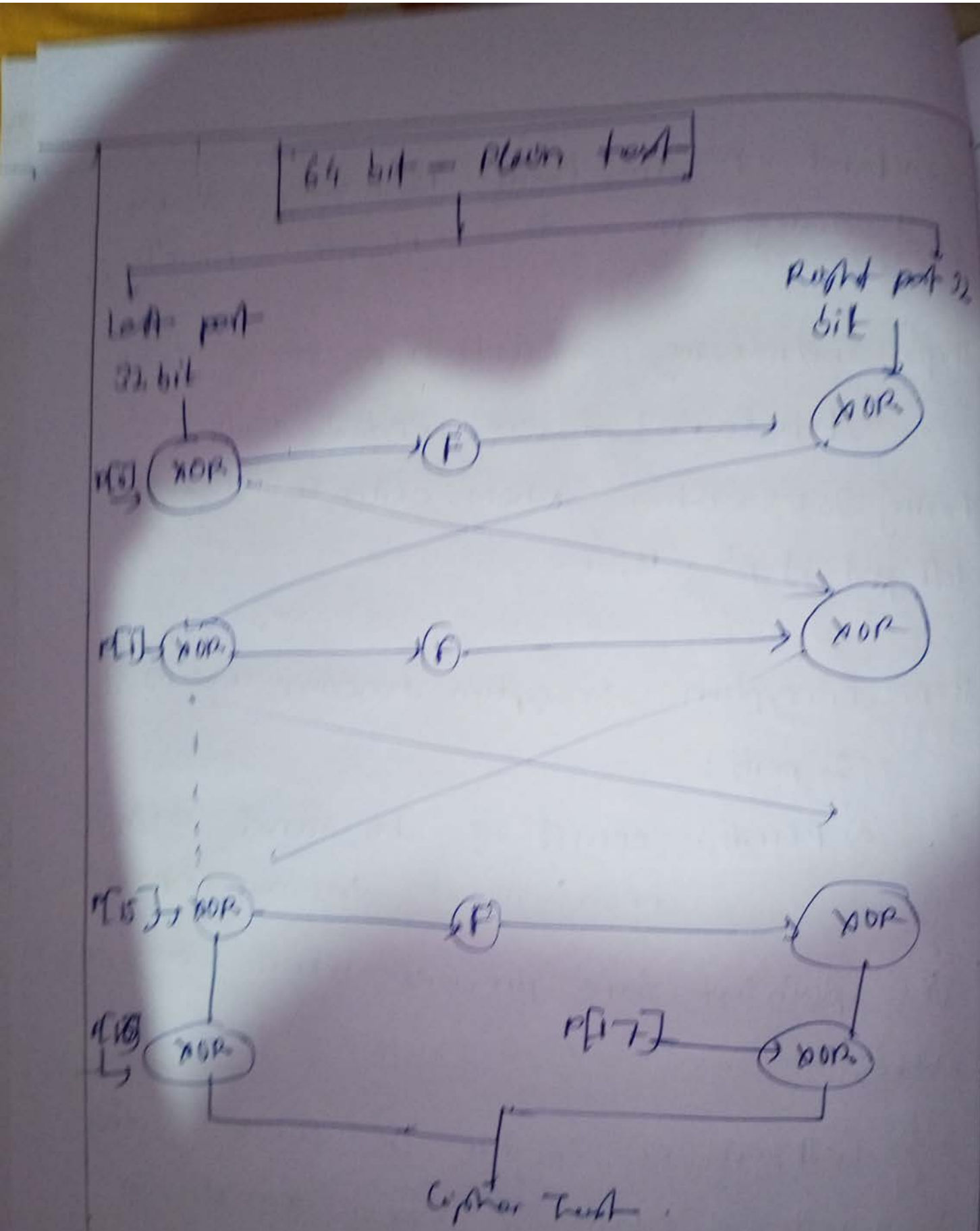
> Resultant P-array holds 18 subkeys that is used during the entire encryption process.

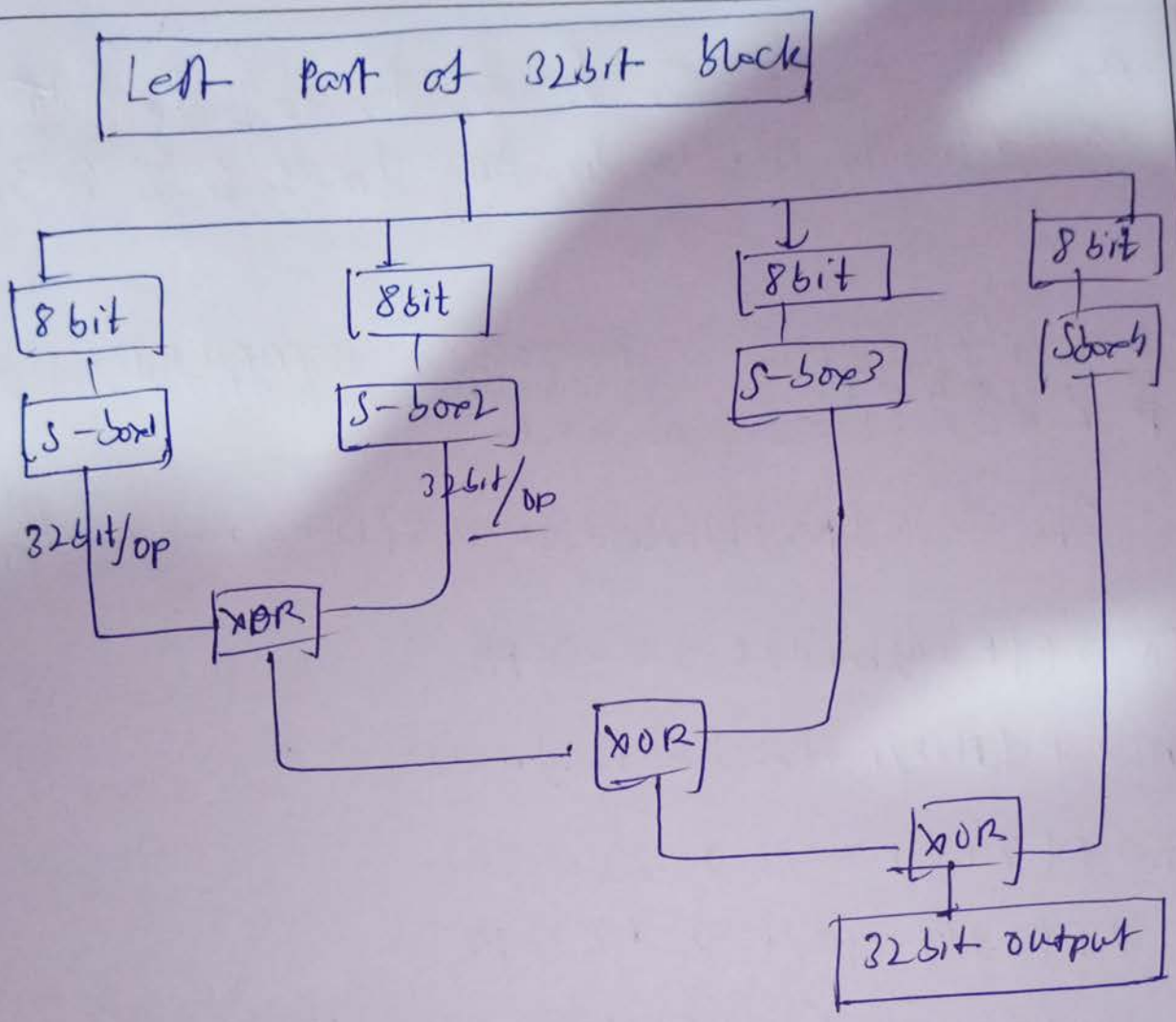
* Step2: Initializing Substitution boxes: 4 substitution box are needed with each having 256 entries where entry is of 32-bit left part of plane 64 bit.

Step3: Encryption: Encryption function consists of 2 parts:

a) Rounds: consist of 16 rounds with each round taking inputs the plain text from previous round & corresponding subkey (

b) Left part of 32 bit is divided into 4 parts of 8 bit & passed through the s-box. Then the output of 1 & 2 ~~the~~ is extracted. Extracted o/p is again applied via XOR with m. & 4th box - 4.


64 bit = Plain text
Left part 32 bit
Right part 32 bit
XOR
F
P[0]
P[1]
P[15]
P[16]
P[17]
Cipher Text



2. Ceaser Cipher:

$$C = E(P + k) \bmod 26 \quad ; \quad k = key = 3$$

C → Cipher text. P → letter of plain text.

$$P = D(C - k) \bmod 26$$

a_0 b_1 c_2 d_3 e_4 f_5 g_6 h_7 i_8 j_9 k_{10} l_{11} m_{12}
n_{13} o_{14} p_{15} q_{16} r_{17} s_{18} t_{19} u_{20} v_{21} w_{22} x_{23} y_{24}
Z_{25}

MEETTOMORROW PROCESS STARTED
12 4 13 19 14 17 8 13 6 15 17 14 2 4 18 18 18 15 0 17 15 4 3
P P Q W R U L Q J S U R F

$\therefore C_m \Rightarrow E(M+k) \bmod 26 \Rightarrow E(12+3) \bmod 26 = 15 \Rightarrow P$

$C_E \Rightarrow E(E+k) \bmod 26 \Rightarrow 7 \Rightarrow H$

$C_N \Rightarrow E(N+k) \bmod 26 \Rightarrow E(13+3) \bmod 26 \Rightarrow Q$

$C_T \Rightarrow E(T+k) \bmod 26 \Rightarrow 22 \Rightarrow W$

$C_O \Rightarrow E(O+k) \bmod 26 \Rightarrow 17 \Rightarrow R$

$C_P \Rightarrow E(P+k) \bmod 26 \Rightarrow E(17+3) \bmod 26 \Rightarrow U$

$C_Z \Rightarrow E(Z+k) \bmod 26 \Rightarrow E(8+3) \bmod 26 \Rightarrow L$

$C_P \Rightarrow E(P+k) \bmod 26 \Rightarrow E(15+3) \bmod 26 = 18 \Rightarrow S$

$C_E \Rightarrow E(E+k) \bmod 26 \Rightarrow H$

$C_S \Rightarrow E(18+3) \bmod 26 \Rightarrow 21 \Rightarrow V$

$C_A \Rightarrow E(0+3) \bmod 26 \Rightarrow D$

$C_D \Rightarrow E(3+3) \bmod 26 \Rightarrow G$

$C_G \Rightarrow E(6+3) \bmod 26 \Rightarrow J$

$\therefore$ Encrypted Cipher Text is "PHQWRULQJ SURFHVV VWDUWHG"

3. Explain RC5 in details:

Ans. RC5 is symmetric key block encryption algorithm designed by Ron Rivest in 1994. It addresses 2 blocks at a time. Depending on input plain text block size, no of rounds., key size & variable instance of RC5 can be defined and each instance is denoted as RC5 – w/r/b where w = word size in bit, r = no. of rounds & b = key size in bytes.

> Block/word size (bits) → 16, 32, 64

> No of rounds → 0 – 255

> key size (bytes) → 0 – 255

* $x \lll y$ → Circular left shift of x by y bits.

* $\wedge$ → bit wise exclusive or.

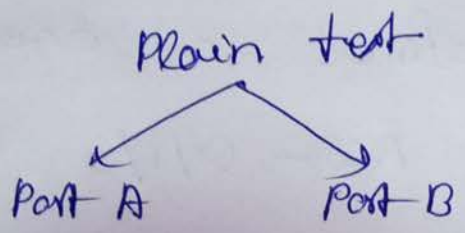
> Procedure of RC5:

① Adding

(a) It we divide the plain text into 2 parts. eg: Part-A ; Part-B

① Adding S[0] with part A to produce C

② Adding S[1] with part B to produce D



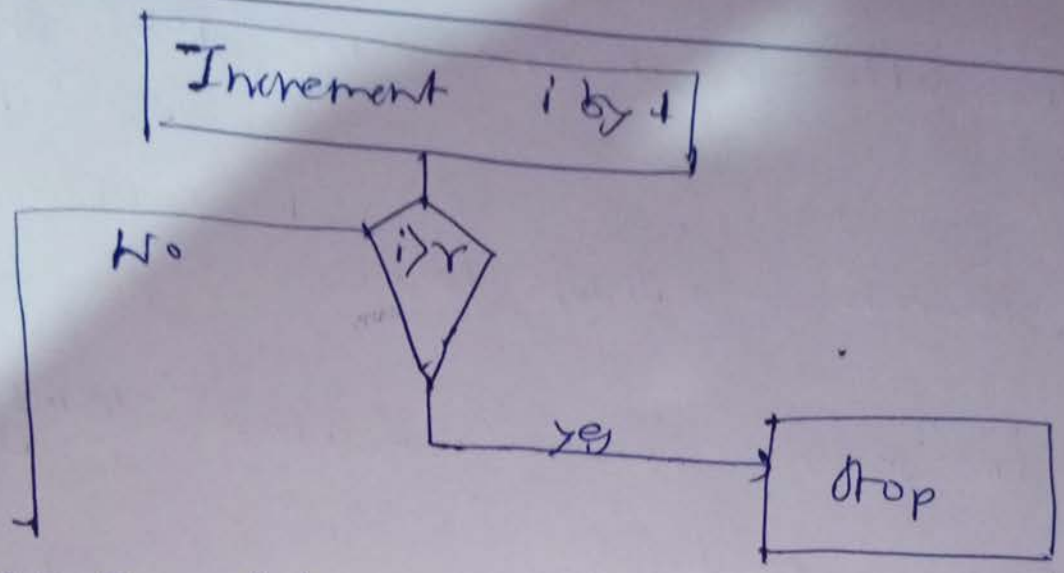
S[0] + Part A ⟶ C

S[1] + Part B ⟶ D

(iii) Starting counter i

1. XOR C & D to produce E (C⊕D) → E
2. Circular left shift E by D bits.
3. Add D & 2i to produce F
   ↳ no of iterations.
4. XOR. D & F to produce G.
5. Circular Left shift G by F bits.
6. Add F & (2i+1) to produce R.

(iv) Incrementing i by 1;



c = F
b = A

(final o/p is maintained as new i/p)

> Nr of keys & rounds depends on user.

4. Encrypt the plain text "MEET ME TOMORROW" with key "THURSDAY" by using playfair cipher.

> I/J treated as same.

key → THURSDAY

↳ Dividing plain text in pairs.

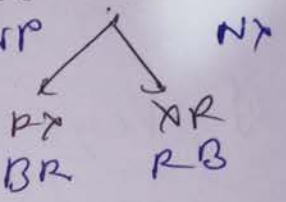
T	H	U	R	S
B	A	Y	B	C
E	F	G	I	K
L	M	N	O	P
Q	V	W	X	Z

1. If the letter is in the same row, shift right.

2. Same column → shift below.

3. Not in same row or column then Triangular prediction.

Plain Text: ME ET ME TO MO RP OW
> LF QD LF LR NP NX



∴ The cipher text is

LF QD LF LR NP BR RB NX