1. "Amreen Hossain"

2. Binary Convert

A (65) - 01000001
m (109) - 01101101
r (114) - 01110010
a (97) - 01100001
n (110) - 01101110
Space (32) 00100000

H (72) - 01001000
O (111) - 01001111
S (115) - 01110011
s (115) - 01110011
a (97) - 01100001
i (105) - 01101001
n (110) - 01101110

3. 64 bit Block

block 1:

01000001
01101101
01110010
01100001
01101110
00100000
01001000
01101111
01110011
01110011

block 2

01110011
01110011
01100001
01101001
01101110
10100000
00000100

padding

4

IP

input

0 1 0 0 0 0 0 1 1 0
0 1 1 0 1 1 0 1
0 1 1 1 0 0 1 0
0 1 1 0 0 0 0 1
0 1 1 0 1 1 1 0
0 0 1 0 0 0 0 0
0 1 0 0 1 0 0 0
0 1 1 0 1 1 1 1

IP

result

1 1 0 1 1 1 1 1
0 0 0 0 0 1 0 0
1 0 0 1 0 0 1 0
1 0 0 0 1 0 1 0
0 0 0 0 0 0 0 0
1 0 1 1 1 1 1 0
1 1 0 1 0 0 1 0
1 0 0 1 0 1 0 1

PC-1

key

0 0 1 1 0 1 0 0
0 0 1 0 1 1 0 1
1 0 1 1 0 1 0 1
1 0 1 0 1 0 0 0
0 0 0 1 1 1 0 1
1 1 0 1 1 0 1 1
1 0 0 1 0 0 0 0
0 0 0 0 0 1 0 0

C:

0 1 1 0 1 1 0
0 0 0 1 0 0 0
0 0 0 0 0 0 0 1
1 1 1 0 1 1 1

D:

0 0 1 0 0 0 0
0 1 0 0 1 0 1
1 1 0 0 1 1 1
0 1 0 0 1 0 1

5. Key Scheduler

Round 1:

C_1 1101100

0010000

0000011

1101110

D_1: 0100000

1001011

1001110

1001010

Q 001

Dr.

PC-2 Key (Sub)

0000011

0000011

1001110

0011011

1000011

1000001

0010011

1111100

6. Round 1

L-in: first half

0100001

0110110

0111001

0110001

R-in: 2nd half

0110111

0010000

0100100

0110111

L_in

11011111
00000100
10010010
10001011

R_in

00000000
10111110
11010010
10010101

K:

00001100
00111001
10001101
10001110
00010010
01111100

E_bit selection table

R_in

00000000 = 100000
10111110 = 000001
11010010 = 011111
10010101 = 100101
011010
100101
010100
101010

• XOR with sub key

100000
000001
010111
111101
011010
100101
010010
101010

⊕

000011
000011
100110
001101
100011
100001
001001
111100

=

S Box

10001 1 → S1
000010 → S2
110001 → S3
110000 → S4
111001 → S5
000100 → S6
011011 → S7
010110 → S8

(Round - 1)

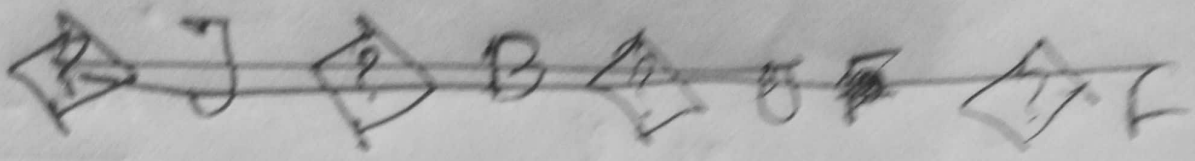
	Value	Permutation		
$S_1 \to (12) \to$	1100	1100		1001
$S_2 \to (1) \to$	0001	0001		0011
$S_3 \to (4) \to$	0100	0100	=	1111
$S_4 \to (15) \to$	1111	1111		0001
$S_5 \to (10) \to$	1010	1010		1101
$S_6 \to (10) \to$	1010	1010		0100
$S_7 \to (15) \to$	1111	1111		1100
$S_8 \to (0) \to$	0000	0000		0001

XOR Left Right

P_out		R_out		L_out
01010101		11011111		10001010
01110100	⊕	00000100	=	01110000
00000110		10010010		10010100
10011111		10001011		00010100

input		IP^{-1}	Result
10001010			10000010
01110000	=		01001010
10010100			10101111
00010100			01000010
01010101			10110111
01110100			00110000
00000110			10110000
10011111			01000110

Scanned with CamScanner



, J - B · 0 · F

Encrypted name

, J - B · 0 · F