I/p is 64 bit text o/p 64 bit permuted text

MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL – 576 104, S. INDIA

Initial permutation → do initial permutation

Ans

0x0002 0000 0000 0001

→ convert to binary

0000 0000 0000 0010 | 0000 0000 0000 0000

15th

0000 0000 0000 0000 | 0000 0000 0000 0001

64th

Bit 15 and Bit 64 has 1

64 − 25 } 64th bit in the table is in location
15 − 63 } 25 and 15 is in location 63

0 0 0 0 0 0 8 0
0000 0000 0000 0000 | 0000 0000 1000 0000 |

0000 0000 0000 0000 | 0000 0000 0000 0010

0 0 0 0 0 0 6 2

Hex → 0x0000 0080 0000 0002

Final permutation

0x0000 0080 0000 0002

Binary

25
0000 0000 0000 0000 | 0000 0000 1000 0000 | 0000

0000 0000 0000 0000 | 0000 0000 0000 0010 63

Only bit 25 and 63 are 1

↓ 64 ↓ 15

Ans 0x0002
0000 0000
0001

① Expansion P box — DES rounds → Before DES rounds text is divided into L & R half (32 bit) only R half goes under DES rounds

Need to expand Right 32 bit to make 48 bits so that we can XOR with 48 bit key.

② Whitener (XOR)

XOR the expanded right hand message with the 48 bit key

③ Sboxes

48 bit o/p of the above operation are divided into chunks of 8 6 bit each. each chunk is fed into a s box.

Result of each sbox is a 4 bit o/p

when combined results in 32 bit o/p.

Example

sbox 1 → i/p 100011 → 1 column

11 → 3 in decimal

(row 3)

Result in row 3 column 1 is 12 → 1100 4 bit output

④ Last round is straight permutation

32 bit i/p is mapped to 32 bit o/p as shown in table.

7th bit in the i/p becomes 2nd bit o/p of straight permutation is XORed with left bit

Key generation

① Parity drop → drops parity bit, (8, 16, 24 ... 64)
I/P → 64 bit O/P → 56 bit Arrange it according to table

② Left shift → key divided into 28 bits 2 parts each
Rounds 1 2 9 16 shifting by 1 bit
Rest shifting by 2 bits.
Combine 2 parts 2 form 56 bit key

③ Compression permutation
56 bit compressed to 48 bit
O/P used to XOR with 48 bit msg.

I/P → 64 bit key
O/P → 48 bit

Key generation Round key generator

DES → overall prossing

$L_i \Leftarrow R_{i-1}$
$R_i \Leftarrow L_{i-1} \times F(R_{i-1}, K_i)$

Key generation

left shifted key pairs of round 1, become before compression the I/P for round 2

DES – Data Encryption Standard

Diffusion and Confusion

→ Normally attackers do a statistical analysis on msg and try to find key / part of key or set of keys

ex) Most frequently occuring character in the cipher text corresponds to frequently occuring letter in plain english word like a/e

To counter this we need 2 types of methods. → changing one bit in the plaintext half the cipher text

Diffusion – Apply some operation on text must be changed like averaging ↔ vice versa

confusion – apply some complex substitution algorithm.

→ each bit in the cipher text must depend on several part of the key.

Design of DES

→ larger block size
→ Larger key size
→ complex key generation algorithm

Decryption

Use keys in reverse order

K_{16} → 1st iteration

K_1 → last "