**Answer to the QN-01**

Round Robin:

Round 1:

|  |  |  |  |
| --- | --- | --- | --- |
| A0 | 5E | AC | 41 |
| 3C | 7A | CE | 36 |
| D4 | B7 | FD | 71 |
| 2B | F6 | DB | 25 |

Recon Table:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 01 | 02 | 03 | 04 | 05 |
| 00 | 00 | 00 | 00 | 00 |
| 00 | 00 | 00 | 00 | 00 |
| 00 | 00 | 00 | 00 | 00 |

Round 2 (1st column value)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Sub-byte |  | R1 (1st C) |  | RT (2nd C) | Value |
| 41 | 36 | 05 |  | A0 |  | 02 | A7 |
| 36 | 71 | A3 | XOR | 3C | XOR | 00 | 9F |
| 71 | 25 | 3F |  | D4 |  | 00 | ED |
| 25 | 41 | 83 |  | 2B |  | 00 | A8 |

Round 2 (2nd column value)

|  |  |  |  |
| --- | --- | --- | --- |
| Round 2 (1st column) |  | Round 1 (2nd Column) | Value |
| A7 |  | 5E | F9 |
| 9F | XOR | 7A | 83 |
| ED |  | B7 | 5A |
| A8 |  | F6 | 5E |

Round 2 (3rd Column value)

|  |  |  |  |
| --- | --- | --- | --- |
| Round 2 (2nd column) |  | Round 1 (3rd column) | Value |
| F9 |  | AC | 55 |
| 83 | XOR | CE | 4D |
| 5A |  | FD | A7 |
| 5E |  | DB | 85 |

Round 2 (4th column value)

|  |  |  |  |
| --- | --- | --- | --- |
| Round 2 (3rd column) |  | Round 1 (4th column) | Value |
| 55 |  | 41 | 14 |
| 4D | XOR | 36 | 7B |
| A7 |  | 71 | D6 |
| 85 |  | 25 | A0 |

Round 2

|  |  |  |  |
| --- | --- | --- | --- |
| A7 | F9 | 55 | 14 |
| 9F | 83 | 4D | 7B |
| ED | 5A | A7 | D6 |
| A8 | 5E | 85 | A0 |

Round 3 (1st column value)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Sub-byte |  | R2 (1st C) |  | RT (3rd C) | Value |
| 14 | 7B | 21 |  | A7 |  | 03 | 85 |
| 7B | D6 | F6 | XOR | 9F | XOR | 00 | 69 |
| D6 | A0 | E0 |  | ED |  | 00 | 0D |
| A0 | 14 | FA |  | A8 |  | 00 | 52 |

Round 3 (2nd column value)

|  |  |  |  |
| --- | --- | --- | --- |
| Round 2 (1st column) |  | Round 2 (2nd Column) | Value |
| 85 |  | F9 | 7C |
| 69 | XOR | 83 | EA |
| 0D |  | 5A | 57 |
| 52 |  | 5E | 0C |

Round 3 (3rd Column value)

|  |  |  |  |
| --- | --- | --- | --- |
| Round 2 (2nd column) |  | Round 2 (3rd column) | Value |
| 7C |  | 55 | 29 |
| EA | XOR | 4D | A7 |
| 57 |  | A7 | F0 |
| 0C |  | 85 | 89 |

Round 3 (4th column value)

|  |  |  |  |
| --- | --- | --- | --- |
| Round 2 (3rd column) |  | Round 2 (4th column) | Value |
| 29 |  | 14 | 3D |
| A7 | XOR | 7B | DC |
| F0 |  | D6 | 26 |
| 89 |  | A0 | 29 |

Round 3

|  |  |  |  |
| --- | --- | --- | --- |
| 85 | 7C | 29 | 3D |
| 69 | EA | A7 | DC |
| 0D | 57 | F0 | 26 |
| 52 | 0C | 89 | 29 |

**Answer to the QN-02**

Li-1

|  |  |  |  |
| --- | --- | --- | --- |
| 0 1 | 0 2 | 0 3 | 1 4 |
| 0 5 | 0 6 | 1 7 | 1 8 |
| 0 9 | 1 10 | 1 11 | 1 12 |
| 1 13 | 1 14 | 1 15 | 1 16 |
| 1 17 | 1 18 | 1 19 | 0 20 |
| 1 21 | 1 22 | 0 23 | 0 24 |
| 1 25 | 0 26 | 0 27 | 0 28 |
| 0 29 | 0 30 | 0 31 | 0 32 |

Ri-1

|  |  |  |  |
| --- | --- | --- | --- |
| 1 1 | 1 2 | 1 3 | 1 4 |
| 1 5 | 0 6 | 1 7 | 0 8 |
| 0 9 | 1 10 | 0 11 | 1 12 |
| 0 13 | 0 14 | 1 15 | 1 16 |
| 1 17 | 1 18 | 0 19 | 0 20 |
| 0 21 | 0 22 | 1 23 | 0 24 |
| 1 25 | 1 26 | 0 27 | 1 28 |
| 1 29 | 1 30 | 1 31 | 0 32 |

Ci-1

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 |

Di- 1

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 |
| 0 | 0 | 1 | 0 |

Left Circular shift of Ci-1

|  |  |  |  |
| --- | --- | --- | --- |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 0 |

Left Circular shift of Di-1

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 1 |
| 1 | 1 | 0 | 0 |
| 0 | 1 | 0 | 0 |

**Marge of Ci-1 & Di-1**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 |

**Permutation Choice 2**

**Expansion Permutation of Ri-1 Permutation Choice 2**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0 32 | 1 1 | 1 2 | 1 3 | 1 4 | 1 5 |
| 1 4 | 1 5 | 0 6 | 1 7 | 0 8 | 0 9 |
| 0 8 | 0 9 | 1 10 | 0 11 | 1 12 | 0 13 |
| 1 12 | 0 13 | 0 14 | 1 15 | 1 16 | 1 17 |
| 1 16 | 1 17 | 1 18 | 0 19 | 0 20 | 0 21 |
| 0 20 | 0 21 | 0 22 | 1 23 | 0 24 | 1 25 |
| 0 24 | 1 25 | 1 26 | 0 27 | 1 28 | 1 29 |
| 1 28 | 1 29 | 1 30 | 1 31 | 0 32 | 1 1 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 |

**XOR of Expansion Permutation and Permutation choice 2**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 0 | 0 | 1 | 0 | S1 | R= 00 = 0  C= 1001 = 9 | 10 | 1010 |
| 1 | 0 | 0 | 0 | 0 | 1 | S2 | R= 11 =3  C=0000 = 0 | 13 | 1101 |
| 1 | 0 | 1 | 1 | 1 | 0 | S3 | R = 10 =2  C= 0111 =7 | 0 | 0000 |
| 0 | 0 | 1 | 0 | 1 | 0 | S4 | R=00 =0  C=0101 =5 | 3 | 0011 |
| 0 | 0 | 1 | 1 | 0 | 1 | S5 | R=01 =1  C=0110 =6 | 13 | 1101 |
| 0 | 0 | 1 | 1 | 0 | 0 | S6 | R=00 =0  C=0110 =6 | 6 | 0110 |
| 0 | 0 | 0 | 1 | 1 | 1 | S7 | R= 01 =1  C=0011 =3 | 7 | 0111 |
| 0 | 0 | 1 | 1 | 1 | 1 | S8 | R= 01 =1  C=0111 =7 | 4 | 0100 |

|  |  |  |  |
| --- | --- | --- | --- |
| 0 31 | 0 29 | 1 20 | 1 23 |
| 1 1 | 1 8 | 1 16 | 1 10 |
| 0 19 | 1 6 | 1 22 | 0 14 |
| 0 11 | 0 25 | 0 2 | 1 18 |
| 1 30 | 1 27 | 0 7 | 0 4 |
| 1 15 | 0 32 | 1 28 | 1 17 |
| 1 26 | 1 5 | 0 9 | 1 3 |
| 0 12 | 0 24 | 0 21 | 0 13 |

|  |  |  |  |
| --- | --- | --- | --- |
| 1 1 | 0 2 | 1 3 | 0 4 |
| 1 5 | 1 6 | 0 7 | 1 8 |
| 0 9 | 0 10 | 0 11 | 0 12 |
| 0 13 | 0 14 | 1 15 | 1 16 |
| 1 17 | 1 18 | 0 19 | 1 20 |
| 0 21 | 1 22 | 1 23 | 0 24 |
| 0 25 | 1 26 | 1 27 | 1 28 |
| 0 29 | 1 30 | 0 31 | 0 32 |

**Permutation choice**