Answer 1:

Here,

1st round inputted key is:

|  |  |  |  |
| --- | --- | --- | --- |
| 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 Calculation:

Round-2 (1st column value)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R-1(Last column value) | Re-Arrange | Sub-bite |  | R-1(1st column Value) |  | RT(1st column value) | Value |
| 41 | 36 | 05 |  | A0 |  | 01 | A4 |
| 36 | 71 | A3 | XOR | 3C | XOR | 00 | 9F |
| 71 | 25 | 3f |  | D4 |  | 00 | EB |
| 25 | 41 | 83 |  | 2B |  | 00 | A8 |

Round-2 (2nd column value)

|  |  |  |  |
| --- | --- | --- | --- |
| 1st column value |  | R-1(2nd column value) | Value |
| A4 |  | 5E | FA |
| 9F | XOR | 7A | E5 |
| EB |  | B7 | 5C |
| A8 |  | F6 | 5E |

Round-2 (3rd column value)

|  |  |  |  |
| --- | --- | --- | --- |
| 2nd column value |  | R-1(3rd column value) | Value |
| FA |  | AC | 56 |
| E5 | XOR | CE | 2B |
| 5C |  | FD | A1 |
| 5E |  | DB | 85 |

Round-2 (4th column value)

|  |  |  |  |
| --- | --- | --- | --- |
| 3rd column value |  | R-1(4th column value) | Value |
| 56 |  | 41 | 17 |
| 2B | XOR | 36 | 1D |
| A1 |  | 71 | D0 |
| 85 |  | 25 | A0 |

Round-2

|  |  |  |  |
| --- | --- | --- | --- |
| A4 | FA | 56 | 17 |
| 9F | E5 | 2B | 1D |
| EB | 5C | A1 | D0 |
| A8 | 5E | 85 | A0 |

Round 3 Calculation:

Round-3 (1st column value):

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| R-2(Last column value) | Re-Arrange | Sub-bite |  | R-2(1st column Value) |  | RT(2ND column value) | Value |
| 17 | 1D | A4 |  | A4 |  | 02 | 02 |
| 1D | D0 | 70 | XOR | 9F | XOR | 00 | EF |
| D0 | A0 | E0 |  | EB |  | 00 | 0B |
| A0 | 17 | F0 |  | A8 |  | 00 | 58 |

Round-3 (2nd column value)

|  |  |  |  |
| --- | --- | --- | --- |
| 1st column value |  | R-2(2nd column value) | Value |
| 02 |  | FA | F8 |
| EF | XOR | E5 | 0A |
| 0B |  | 5C | 57 |
| 58 |  | 5E | 06 |

Round-3 (3rd column value)

|  |  |  |  |
| --- | --- | --- | --- |
| 2nd column value |  | R-2(3rd column value) | Value |
| F8 |  | 56 | AE |
| 0A | XOR | 2B | 21 |
| 57 |  | A1 | F6 |
| 06 |  | 85 | 83 |

Round-3 (4th column value)

|  |  |  |  |
| --- | --- | --- | --- |
| 3rd column value |  | R-2(4th column value) | Value |
| AE |  | 17 | B9 |
| 21 | XOR | 1D | 3C |
| F6 |  | D0 | 26 |
| 83 |  | A0 | 23 |

Round-3

|  |  |  |  |
| --- | --- | --- | --- |
| 02 | F8 | AE | B9 |
| EF | 0A | 21 | 3C |
| 0B | 57 | F6 | 26 |
| 58 | 06 | 83 | 23 |