**DES example**

Key: AABB09182736CCDD

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | A | B | B | 0 | 9 | 1 | 8 | 2 | 7 | 3 | 6 | C | C | D | D |

 PC1 PC2

-🡪divide into 28 bit and

Left Shift->

No of shift:1 bit

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Sr no | Binary | PC1 | LShift | PC2 | Round-key |
| A | 1 | 1 | 1 | 1 | 0 | 1 |
| 2 | 0 | 1 | 0 | 0 |
| 3 | 1 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 1 |
| A | 5 | 1 | 0 | 0 | 1 | 9 |
| 6 | 0 | 0 | 1 | 0 |
| 7 | 1 | 1 | 1 | 0 |
| 8 | 0 | 1 | 1 | 1 |
| B | 9 | 1 | 1 | 1 | 0 | 4 |
| 10 | 0 | 1 | 0 | 1 |
| 11 | 1 | 0 | 0 | 0 |
| 12 | 1 | 0 | 0 | 0 |
| B | 13 | 1 | 0 | 0 | 1 | C |
| 14 | 0 | 0 | 0 | 1 |
| 15 | 1 | 0 | 0 | 0 |
| 16 | 1 | 0 | 0 | 0 |
| 0 | 17 | 0 | 0 | 0 | 1 | D |
| 18 | 0 | 0 | 1 | 1 |
| 19 | 0 | 1 | 1 | 0 |
| 20 | 0 | 1 | 0 | 1 |
| 9 | 21 | 1 | 0 | 0 | 0 | 0 |
| 22 | 0 | 0 | 1 | 0 |
| 23 | 0 | 1 | 1 | 0 |
| 24 | 1 | 1 | 1 | 0 |
| 1 | 25 | 0 | 1 | 0 | 0 | 7 |
| 26 | 0 | 0 | 1 | 1 |
| 27 | 0 | 1 | 0 | 1 |
| 28 | 1 | 0 | 1 | 1 |
| 8 | 29 | 1 | 0 | 0 | 0 | 2 |
| 30 | 0 | 0 | 1 | 0 |
| 31 | 0 | 1 | 1 | 1 |
| 32 | 0 | 1 | 0 | 0 |
| 2 | 33 | 0 | 0 | 0 | 1 | D |
| 34 | 0 | 0 | 1 | 1 |
| 35 | 1 | 1 | 1 | 0 |
| 36 | 0 | 1 | 1 | 1 |
| 7 | 37 | 0 | 1 | 1 | 1 | E |
| 38 | 1 | 1 | 1 | 1 |
| 39 | 1 | 1 | 1 | 1 |
| 40 | 1 | 1 | 0 | 0 |
| 3 | 41 | 0 | 0 | 0 | 1 | 8 |
| 42 | 0 | 0 | 0 | 0 |
| 43 | 1 | 0 | 0 | 0 |
| 44 | 1 | 0 | 1 | 0 |
| 6 | 45 | 0 | 1 | 1 | 1 | C |
| 46 | 1 | 1 | 0 | 1 |
| 47 | 1 | 0 | 0 | 0 |
| 48 | 0 | 0 | 1 | 0 |
| C | 49 | 1 | 1 | 1 |  |  |
| 50 | 1 | 1 | 1 |  |  |
| 51 | 0 | 1 | 1 |  |  |
| 52 | 0 | 1 | 1 |  |  |
| C | 53 | 1 | 1 | 0 |  |  |
| 54 | 1 | 0 | 1 |  |  |
| 55 | 0 | 1 | 0 |  |  |
| 56 | 0 | 0 | 0 |  |  |
| D | 57 | 1 |  |  |  |  |
| 58 | 1 |  |  |  |  |
| 59 | 0 |  |  |  |  |
| 60 | 1 |  |  |  |  |
| D | 61 | 1 |  |  |  |  |
| 62 | 1 |  |  |  |  |
| 63 | 0 |  |  |  |  |
| 64 | 1 |  |  |  |  |

1st Round key of Round 1: 194CD072DE8C

Plaintext: 123456ABCD132536 Step1: Initial permutation (PC1)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Sr no | Binary | PC1 | O/p |
| 1 | 1 | 0 | 0 | 1 |
| 2 | 0 | 0 |
| 3 | 0 | 0 |
| 4 | 1 | 1 |
| 2 | 5 | 0 | 0 | 4 |
| 6 | 0 | 1 |
| 7 | 1 | 0 |
| 8 | 0 | 0 |
| 3 | 9 | 0 | 1 | A |
| 10 | 0 | 0 |
| 11 | 1 | 1 |
| 12 | 1 | 0 |
| 4 | 13 | 0 | 0 | 7 |
| 14 | 1 | 1 |
| 15 | 0 | 1 |
| 16 | 0 | 1 |
| 5 | 17 | 0 | 1 | D |
| 18 | 1 | 1 |
| 19 | 0 | 0 |
| 20 | 1 | 1 |
| 6 | 21 | 0 | 0 | 6 |
| 22 | 1 | 1 |
| 23 | 1 | 1 |
| 24 | 0 | 0 |
| A | 25 | 1 | 0 | 7 |
| 26 | 0 | 1 |
| 27 | 1 | 1 |
| 28 | 0 | 1 |
| B | 29 | 1 | 1 | 8 |
| 30 | 0 | 0 |
| 31 | 1 | 0 |
| 32 | 1 | 0 |
| C | 33 | 1 | 0 | 1 |
| 34 | 1 | 0 |
| 35 | 0 | 0 |
| 36 | 0 | 1 |
| D | 37 | 1 | 1 | 8 |
| 38 | 1 | 0 |
| 39 | 0 | 0 |
| 40 | 1 | 0 |
| 1 | 41 | 0 | 1 | C |
| 42 | 0 | 1 |
| 43 | 0 | 0 |
| 44 | 1 | 0 |
| 3 | 45 | 0 | 1 | A |
| 46 | 0 | 0 |
| 47 | 1 | 1 |
| 48 | 1 | 0 |
| 2 | 49 | 0 | 0 | 1 |
| 50 | 0 | 0 |
| 51 | 1 | 0 |
| 52 | 0 | 1 |
| 5 | 53 | 0 | 1 | 8 |
| 54 | 1 | 0 |
| 55 | 0 | 0 |
| 56 | 1 | 0 |
| 3 | 57 | 0 | 1 | A |
| 58 | 0 | 0 |
| 59 | 1 | 1 |
| 60 | 1 | 0 |
| 6 | 61 | 0 | 1 | D |
| 62 | 1 | 1 |
| 63 | 1 | 0 |
| 64 | 0 | 1 |

After Intial Permutation: 14 A7D67818CA18AD

L0=14A7D678 R0=18CA18AD 1st Round key of Round 1: 194CD072DE8C

Round 1:

After Initial Permutation: 14 A7D67818CA18AD

L0=14A7D678 R0=18CA18AD

Expansion P-BOX🡪EX-or with key🡪S-box🡪Straight P-box-🡪Ex-or with L0->swapping

Expansion P-box straight P-Box



|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sr no | Key | L0 | R0 | EP-box entry | E-OR  With key | S-box | Straight P-box | Ex-OR with L0 | Hex  value |
| 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0  1  0  1 | 5 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| 5 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | A |
| 6 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 |
| 7 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| 8 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 9 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 7 |
| 10 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 11 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 12 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| 13 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 8 |
| 14 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| 15 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |
| 16 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 17 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | E |
| 18 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 19 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 20 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 21 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 3 |
| 22 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| 23 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| 24 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| 25 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 9 |
| 26 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| 27 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 |
| 28 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |
| 29 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 4 |
| 30 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 31 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 32 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| 33 | 1 |  |  | 0 | 1 |  |  |  |  |
| 34 | 1 |  |  | 0 | 1 |  |  |  |  |
| 35 | 0 |  |  | 0 | 0 |  |  |  |  |
| 36 | 1 |  |  | 1 | 0 |  |  |  |  |
| 37 | 1 |  |  | 0 | 1 |  |  |  |  |
| 38 | 1 |  |  | 1 | 0 |  |  |  |  |
| 39 | 1 |  |  | 0 | 1 |  |  |  |  |
| 40 | 0 |  |  | 1 | 1 |  |  |  |  |
| 41 | 1 |  |  | 0 | 1 |  |  |  |  |
| 42 | 0 |  |  | 1 | 1 |  |  |  |  |
| 43 | 0 |  |  | 0 | 0 |  |  |  |  |
| 44 | 0 |  |  | 1 | 1 |  |  |  |  |
| 45 | 1 |  |  | 1 | 0 |  |  |  |  |
| 46 | 1 |  |  | 0 | 1 |  |  |  |  |
| 47 | 0 |  |  | 1 | 1 |  |  |  |  |
| 48 | 0 |  |  | 0 | 0 |  |  |  |  |
| 49 |  |  |  |  |  |  |  |  |  |
| 50 |  |  |  |  |  |  |  |  |  |
| 51 |  |  |  |  |  |  |  |  |  |
| 52 |  |  |  |  |  |  |  |  |  |
| 53 |  |  |  |  |  |  |  |  |  |
| 54 |  |  |  |  |  |  |  |  |  |
| 55 |  |  |  |  |  |  |  |  |  |
| 56 |  |  |  |  |  |  |  |  |  |
| 57 |  |  |  |  |  |  |  |  |  |
| 58 |  |  |  |  |  |  |  |  |  |
| 59 |  |  |  |  |  |  |  |  |  |
| 60 |  |  |  |  |  |  |  |  |  |
| 61 |  |  |  |  |  |  |  |  |  |
| 62 |  |  |  |  |  |  |  |  |  |
| 63 |  |  |  |  |  |  |  |  |  |
| 64 |  |  |  |  |  |  |  |  |  |