DES EXAMPLE

M = 0123456789ABCDEF

Where **M** is in hexadecimal (base 16) format.

Convert the binary: Rewriting **M** in binary format, we get the 64-bit block of text:

M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111
L = 0000 0001 0010 0011 0100 0101 0110 0111
R = 1000 1001 1010 1011 1100 1101 1110 1111

K = 133457799BBCDFF1

Convert the binary: This gives us as the binary key (setting 1 = 0001, 3 = 0011, etc., and grouping together every eight bits, of which the last one in each group will be unused):

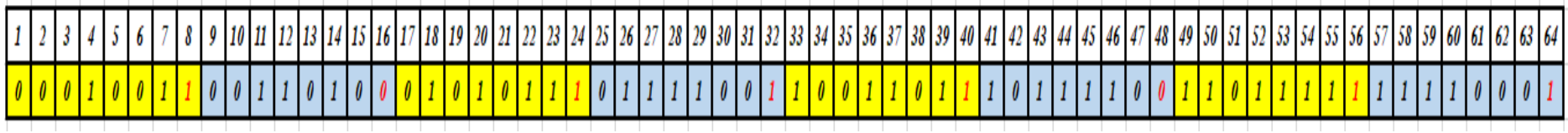
K = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001

Step 1: Use permutation Choice-1 (PC-1) to create the permute key (PC-1)

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

From the original 64-bit key

K = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001

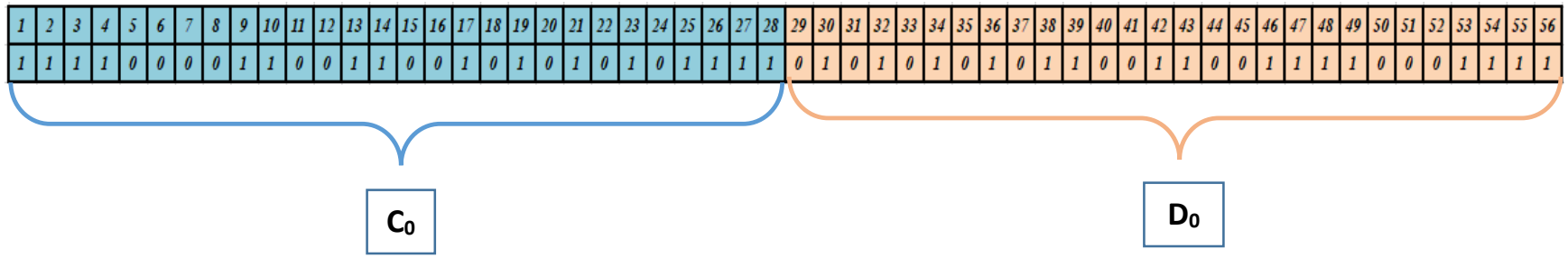


we get the 56-bit permutation:

K_P = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

Step 2:

Split this key into left and right halves, ***C_0*** and ***D_0***, where each half has 28 bits.



C_0 = 1111000 0110011 0010101 0101111
D_0 = 0101010 1011001 1001111 0001111

Step 3: Rotate shift

- In **rounds *i* = 1, 2, 9 ,16,** the two halves are each rotated left by **one bit**.
- In **all other rounds** where the two halves are each rotated left by **two bits**.

From original pair pair C_0 and D_0 we obtain:

C_0 = 11110000110011001010101111
D_0 = 01010101011001100111100011111

R_i and K_i	Left Part (C)	Right Part (D)
K_0:	11110000110011001010101111	01010101011001100111100011111
K_1:LS-1:	11100001100110010101010111111	10101010110011001111100011110
K_2: LS-1:	11000011001100101010101111111	01010101100110011111000111101
K_3: LS-2:	00001100110010101010111111111	01010110011001111000111101010
K_4: LS-2:	00110011001010101011111111100	01011001100111100011110101010
K_5: LS-2:	11001100101010101111111110000	01100110011110001111010101011
K_6: LS-2:	00110010101010111111111000011	10011001111000111101010101011
K_7: LS-2:	11001010101011111111100001100	01100111100011110101010101100
K_8: LS-2:	00101010101111111110000110011	10011110001111010101011001100
K_9: LS-1:	01010101011111111100001100110	00111100011110101010110011001
K_{10}: LS-2:	01010101111111100001100110011	11110001111010101011001100100
K_{11}: LS-2:	01010111111110000110011001011	11000111101010101100110011001
K_{12}: LS-2:	01011111111000011001100101011	00011110101010101100110011111
K_{13}: LS-2:	01111111100001100110010101011	01111010101010110011001111100

K_{14}: LS-2:	11111110000110011001010101	11101010101011001100111110001
K_{15}: LS-2:	11111000011001100101010111	10101010101100110011111000111
K_{16}: LS-1:	11110000110011001010101111	01010101011001100111100011111

Step 4: **PC-2**

*In each round (R_i) permuted choice **PC-2***

We now form the keys K_n, for 1<=n<=16, by applying the following permutation table to each of the concatenated pairs C_nD_n. Each pair has 56 bits, but **PC-2** only uses 48 of these.

PC-2

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

K_1:LS-1:	11100001100110010101011111	10101010110011001111100011110

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
1	1	1	0	0	0	0	1	1	0	0	1	1	0	0	1	0	1	0	1	0	1	0	1	1	1	1	1	1	0	1	0	1	0	1	0	1	1	0	0	1	1	0	0	1	1	1	1	0	0	0	1	1	1	1	0

The following bits are discarded

9 18 22 25 35 38 43 54

K_1 = 00011011 00000010 11101111 111111000 1110000 01110010

For the other keys we have

K_2 = 011110 011010 111011 011001 110110 111100 100111 100101
K_3 = 010101 011111 110010 001010 010000 101100 111110 011001
K_4 = 011100 101010 110111 010110 110110 110011 010100 011101
K_5 = 011111 001110 110000 000111 111010 110101 001110 101000
K_6 = 011000 111010 010100 111110 010100 000111 101100 101111
K_7 = 111011 001000 010010 110111 111101 100001 100010 111100
K_8 = 111101 111000 101000 111010 110000 010011 101111 111011
K_9 = 111000 001101 101111 101011 111011 011110 011110 000001
K_{10} = 101100 011111 001101 000111 101110 100100 011001 001111
K_{11} = 001000 010101 111111 010011 110111 101101 001110 000110
K_{12} = 011101 010111 000111 110101 100101 000110 011111 101001
K_{13} = 100101 111100 010111 010001 111110 101011 101001 000001
K_{14} = 010111 110100 001110 110111 111100 101110 011100 111010
K_{15} = 101111 111001 000110 001101 001111 010011 111100 001010
K_{16} = 110010 110011 110110 001011 000011 100001 011111 110101