WHY DES DECRYPTION USES REVERSED KEYS

Same Feistel round structure; only the subkey order changes

DES | DECRYPTION

Original 64-bit key: 133457799BBCDFF1

ENCRYPTION

K1	K2	K3	...	K15	K16

DECRYPTION

K16	K15	K14	...	K2	K1

! **The subkeys are used in reverse order**

Important: Do not reverse the bits of a key; reverse the ORDER of the 16 subkeys.

K16 is used in decryption Round 1. K1 is used in decryption Round 16.

ROUND KEY: FIRST DECRYPTION SUBKEY K16

The same PC-1, rotations and PC-2 produce all sixteen round subkeys

DES | DECRYPTION

1 64-bit key → 2 PC-1: 56 bits → 3 C and D halves → 4 Circular shifts → 5 PC-2: 48 bits

FIRST SUBKEY USED IN DECRYPTION

K16 = CB3D8B0E17F5

Next keys:

Round 2: K15 = BF918D3D3F0A

Round 16: K1 = 1B02EFFC7072

Each subkey contains 48 bits. The complete sequence is shown later.