# DATA ENCRYPTION STANDARD: DECRYPTION

Complete worked example in the exact algorithm order

DES | DECRYPTION

**CIPHERTEXT (given)**

**85E813540F0AB405**

**SECRET KEY**

**133457799BBCDFF1**

**Decryption uses the SAME DES round function...**

**...but uses the round keys in REVERSE order.**

**TARGET: RECOVER THE ORIGINAL PLAINTEXT**

**0123456789ABCDEF**

**64-bit block • 56-bit effective key • 16 Feistel rounds**

# THE CORRECT DES DECRYPTION SEQUENCE

Follow these operations in order; the keys run backward

DES | DECRYPTION

01 IP(ciphertext) → 02 Split L and R → 03 Select K16 first → 04 Expand R (E)

05 XOR with key → 06 Eight S-boxes → 07 P-permutation → 08 Update L and R

09 Complete 16 rounds → 10 Swap halves → 11 Inverse IP → 12 Original plaintext

**CRITICAL DIFFERENCE**

**Encryption: K1 → K16 | Decryption: K16 → K1**