INVERSE INITIAL PERMUTATION: SIMPLE EXAMPLE

IP inverse restores the bit positions that an IP rearranged

REMEMBER: Inverse IP is a rearrangement - not XOR and not a secret-key operation.

AFTER IP

10110010 → 01001101

1 **Use the matching inverse ordering**

[5, 1, 6, 2, 7, 3, 8, 4]

2 **Select those positions from the permuted bits**

INVERSE IP RESTORES

01001101 → 10110010

FINAL INVERSE IP: RECOVER THE ORIGINAL TEXT

Apply DES IP inverse to the swapped 64-bit round result

DES | DECRYPTION

64-BIT INPUT TO INVERSE IP

CC00CCFFF0AAF0AA

Apply the standard 64-position IP inverse table



RECOVERED PLAINTEXT

0123456789ABCDEF

DES-DEC(85E813540F0AB405, 133457799BBCDFF1) = 0123456789ABCDEF

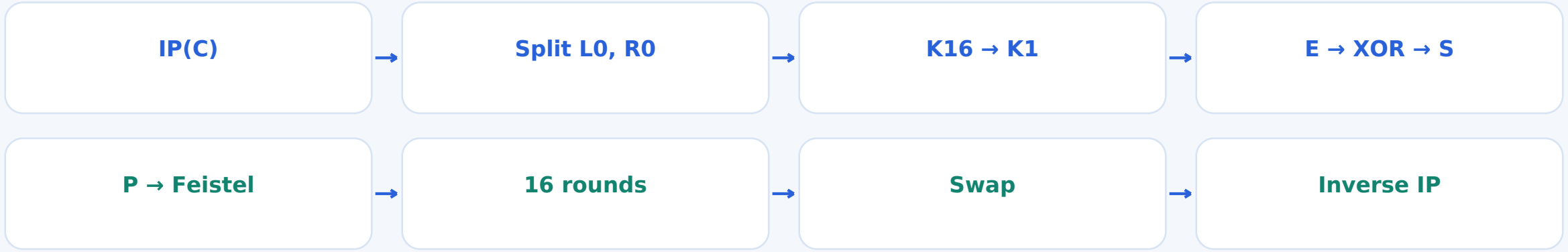
DES DECRYPTION: FINAL REVIEW

One coherent example from ciphertext back to plaintext

ENCRYPTED INPUT

85E813540F0AB405

The key sequence is reversed; the round function stays the same.



ORIGINAL PLAINTEXT

0123456789ABCDEF

DES is historically important but insecure for modern deployment (56-bit effective key).