FEISTEL ROUND: SIMPLE LEFT/RIGHT UPDATE

Each DES round applies the SAME two half-update equations

RULE: New left = old right. New right = old left XOR F(old right, key).

OLD LEFT L0

1011

OLD RIGHT R0

0010

Given this miniature example: F(R0, key) = 0110

NEW LEFT L1 = R0

0010

NEW RIGHT R1 = 1011 XOR 0110

1101

ACTUAL DECRYPTION ROUND 1: UPDATE THE HALVES

The first decryption round uses K16, not K1

OLD LEFT L0

0A4CD995

OLD RIGHT R0

43423234

F(R0, K16) = C8C04F98

1 **Now apply the two update equations**

L1 = R0

43423234

R1 = L0 XOR F

C28C960D

0A4CD995 XOR C8C04F98 = C28C960D

DECRYPTION ROUND 2: ONE MORE EXAMPLE

Use the output from Round 1 as the input to Round 2

ROUND 2 OPERATION	ACTUAL HEXADECIMAL VALUE
Key K15	BF918D3D3F0A
Expand R1	E054594AC05B
XOR with K15	5FC5D477FF51
Apply S1 ... S8	B2E88D3C
P permutation	5B81276E

L2 = R1

C28C960D

R2 = L1 XOR F

18C3155A