COMPLETE DECRYPTION: ROUNDS 1 THROUGH 8

Use the same Feistel equations for every successive round

ROUND	48-BIT SUBKEY	NEW LEFT (32 BITS)	NEW RIGHT (32 BITS)
01	CB3D8B0E17F5	43423234	**C28C960D**
02	BF918D3D3F0A	C28C960D	**18C3155A**
03	5F43B7F2E73A	18C3155A	**75BD1858**
04	97C5D1FABA41	75BD1858	**C5783C78**
05	7571F59467E9	C5783C78	**B7D5D7B2**
06	215FD3DED386	B7D5D7B2	**247CC67A**
07	B1F347BA464F	247CC67A	**D5694B90**
08	E0DBEBEDE781	D5694B90	**064ABA10**

The output halves of one round become the inputs of the next.

COMPLETE DECRYPTION: ROUNDS 9 THROUGH 16

The final decryption round uses the original encryption subkey K1

ROUND	48-BIT SUBKEY	NEW LEFT (32 BITS)	NEW RIGHT (32 BITS)
09	F78A3AC13BFB	064ABA10	**E967CD69**
10	EC84B7F618BC	E967CD69	**8A4FA637**
11	63A53E507B2F	8A4FA637	**77220045**
12	7CEC07EB53A8	77220045	**A25C0BF4**
13	72ADD6DB351D	A25C0BF4	**CC017709**
14	55FC8A42CF99	CC017709	**EF4A6544**
15	79AED9DBC9E5	EF4A6544	**F0AAF0AA**
16	1B02EFFC7072	F0AAF0AA	**CC00CCFF**

Final decryption subkey: K1 = 1B02EFFC7072.

AFTER ROUND 16: SWAP THE TWO HALVES

DES performs the final half-swap before applying inverse IP

DES | DECRYPTION

FINAL LEFT HALF L16

F0AAF0AA

FINAL RIGHT HALF R16

CC00CCFF

Swap the order of the two halves

↓

R16 || L16

CC00CCFFF0AAF0AA

This 64-bit block is the INPUT to the final IP inverse.