S-BOX: ONE LOOKUP IN DES DECRYPTION

Six bits select one row and one column; the output has four bits

FIRST SIX BITS: 111010

bit 1	bit 2	bit 3	bit 4	bit 5	bit 6
1	1	1	0	1	0

OUTER BITS: ROW

10 = 2

INNER FOUR: COLUMN

1101 = 13

Standard DES S1[2, 13] = 10 (decimal).

S1 OUTPUT

10 decimal = 1010 binary

ALL EIGHT S-BOXES: COMPLETE ROUND 1

48 bits become 32 bits after eight independent S-box lookups

48-BIT INPUT **EB578F14565D**

S-BOX	6-BIT INPUT	ROW	COLUMN	DECIMAL	4-BIT RESULT
S1	111010	2	13	10	**1010**
S2	110101	3	10	7	**0111**
S3	011110	0	15	8	**1000**
S4	001111	1	7	3	**0011**
S5	000101	1	2	2	**0010**
S6	000101	1	2	4	**0100**
S7	011001	1	12	2	**0010**
S8	011101	1	14	9	**1001**

JOIN ALL 4-BIT RESULTS **A7832429 (32 bits)**