SUBSTITUTION BOX (S-BOX): ONE LOOKUP

The easiest way to understand how a DES S-box works

DES | CLASS LECTURE

IDEA: An S-box uses 6 input bits to look up a number, then produces 4 output bits.

1 Read the six input bits

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

2 Find row and column

FIRST + LAST = 00 = row 0

MIDDLE FOUR = 1100 = column 12

3 Look up row 0, column 12 in the real DES S1 table

ROW	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

RESULT

S1[0, 12] = 5

Decimal 5 = Binary 0101

6 input bits -> 4 output bits

ALL EIGHT S-BOXES: A COMPLETE EXAMPLE

Apply the same row-column rule eight times; each box uses its own table

IDEA: 48 bits = eight groups of 6. Each S-box gives 4 bits. Total output = 32 bits.

48-BIT INPUT (hexadecimal) **6117BA866527**

Binary groups: **011000** **010001** **011110** **111010** **100001** **100110** **010100** **100111**

1 Use the outer bits for the row and the middle four bits for the column

S-BOX	6-BIT INPUT	ROW (outer)	COLUMN (middle)	S-BOX VALUE	4-BIT OUTPUT
S1	011000	00 = 0	1100 = 12	**5**	**0101**
S2	010001	01 = 1	1000 = 8	**12**	**1100**
S3	011110	00 = 0	1111 = 15	**8**	**1000**
S4	111010	10 = 2	1101 = 13	**2**	**0010**
S5	100001	11 = 3	0000 = 0	**11**	**1011**
S6	100110	10 = 2	0011 = 3	**5**	**0101**
S7	010100	00 = 0	1010 = 10	**9**	**1001**
S8	100111	11 = 3	0011 = 3	**7**	**0111**

FINAL OUTPUT

Eight 4-bit answers joined together

0101 1100 1000 0010 1011 0101 1001 0111

32 bits = 5C82B597 (hex)