XOR OPERATION: SIMPLE SOLVED EXAMPLE

Understand the four XOR rules, then compare two 8-bit strings

DES | CLASS LECTURE

IDEA: XOR compares TWO bits at the same position: same = 0, different = 1.

1 THE FOUR XOR RULES

BIT A	BIT B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

REMEMBER THIS ONE RULE

DIFFERENT bits give 1

0 XOR 1 = 1 1 XOR 0 = 1

SAME bits give 0

0 XOR 0 = 0 1 XOR 1 = 0

2 Compare two 8-bit values position by position

BIT POSITION	1	2	3	4	5	6	7	8
INPUT A	1	0	1	1	0	0	1	0
INPUT B	0	1	1	0	1	0	0	1
A XOR B	1	1	0	1	1	0	1	1

FINAL 8-BIT RESULT

10110010 XOR 01101001 = 11011011

XOR IN DES: A REAL ROUND EXAMPLE

XOR the 48-bit expanded right half with the 48-bit round key

DES | CLASS LECTURE

WHY? DES combines expanded data with its round subkey using bit-by-bit XOR.

1 Take the two equal-length inputs (48 bits each)

EXPANDED RIGHT HALF

7A15557A1555

XOR

ROUND KEY K1

1B02EFFC7072

2 Perform XOR one byte (8 bits) at a time

BYTE	DATA	KEY	XOR	BINARY WORKING (DATA XOR KEY = RESULT)
1	7A	1B	61	01111010 XOR 00011011 = 01100001
2	15	02	17	00010101 XOR 00000010 = 00010111
3	55	EF	BA	01010101 XOR 11101111 = 10111010
4	7A	FC	86	01111010 XOR 11111100 = 10000110
5	15	70	65	00010101 XOR 01110000 = 01100101
6	55	72	27	01010101 XOR 01110010 = 00100111

48-BIT XOR RESULT

7A15557A1555 XOR 1B02EFFC7072 = 6117BA866527