DES EXPANSION: START WITH F0AAF0AA

A visual explanation of how 32 input bits become 48 output bits

DES | CLASS LECTURE

MAIN IDEA: Every set of 4 bits becomes 6 by borrowing ONE neighboring bit on each side.

1 Convert each hexadecimal digit into four binary bits

Given hexadecimal input: **F0AAF0AA**

Hex digit	F	0	A	A	F	0	A	A
Four bits	1111	0000	1010	1010	1111	0000	1010	1010

2 Divide the 32 bits into eight 4-bit groups

Group 1	Group 2	Group 3	Group 4	Group 5	Group 6	Group 7	Group 8
1111	0000	1010	1010	1111	0000	1010	1010

CHECK: 8 groups × 4 bits = 32 original bits.

Next: take the last bit of the previous group and the first bit of the next group.

HOW ONE 4-BIT GROUP BECOMES 6 BITS

Join (do not add): previous last bit | current four bits | next first bit

DES | CLASS LECTURE

RULE: Read the groups in a circle: before Group 1 comes Group 8; after Group 8 comes Group 1.

EXAMPLE 1 | Expand Group 1 = 1111

Wrap-around: the previous group of Group 1 is Group 8 (1010); the next is Group 2 (0000).

PREVIOUS: Group 8	CURRENT: Group 1	NEXT: Group 2
0	1111	0

0 | 1111 | 0 -> 011110

EXAMPLE 2 | Expand Group 2 = 0000

For Group 2, take Group 1's last bit (1) and Group 3's first bit (1).

PREVIOUS: Group 1	CURRENT: Group 2	NEXT: Group 3
1	0000	1

1 | 0000 | 1 -> 100001

COMPLETE EXPANSION: ALL EIGHT GROUPS

Repeat the same neighbor-bit rule for every group, then combine the answers

FORMULA: Expanded group = Previous last bit | Original 4 bits | Next first bit

GROUP	LEFT BIT	ORIGINAL 4	RIGHT BIT	EXPANDED 6 BITS
1	0	1111	0	**011110**
2	1	0000	1	**100001**
3	0	1010	1	**010101**
4	0	1010	1	**010101**
5	0	1111	0	**011110**
6	1	0000	1	**100001**
7	0	1010	1	**010101**
8	0	1010	1	**010101**

COMBINE ALL EIGHT 6-BIT GROUPS:

011110 100001 010101 010101 011110 100001 010101 010101

48 binary bits = 0111 1010 0001 0101 0101 0101 0111 1010 0001 0101 0101 0101

HEX OUTPUT: **7A15557A1555**