EXPANSION BOX (E-BOX): SIMPLE EXAMPLE

First understand the idea using just 8 input bits

DES | CLASS LECTURE

IDEA: An E-box rearranges AND repeats selected bits to produce a longer bit sequence.

1 Start with an 8-bit input and number its positions

1	2	3	4	5	6	7	8
1	0	1	1	0	0	1	0

Input bits: 1 0 1 1 | 0 0 1 0

2 Use a small expansion rule: two groups of 4 bits become two groups of 6

GROUP 1 Previous | 4 original | Next

Take positions:	8	1	2	3	4	5
Their bit values:	0	1	0	1	1	0

GROUP 2 Previous | 4 original | Next

Take positions:	4	5	6	7	8	1
Their bit values:	1	0	0	1	0	1

EXPANDED RESULT

Two groups of 6 bits = 12 output bits

010110 | 100101

010110100101 (12 bits)

REAL DES E-BOX: 32 BITS TO 48 BITS

The same concept: copy selected boundary bits and keep their prescribed order

RULE: DES uses a fixed expansion table: eight 4-bit sections each become 6 bits.

32-BIT INPUT (right half R) **F0AAF0AA**

Binary (four groups of 8):

11110000	10101010	11110000	10101010

1 Read six positions from each row, then copy the bits at those positions

GROUP	SOURCE BIT POSITIONS	BITS TAKEN FROM INPUT	6-BIT OUTPUT
E1	32 1 2 3 4 5	0 1 1 1 1 0	011110
E2	4 5 6 7 8 9	1 0 0 0 0 1	100001
E3	8 9 10 11 12 13	0 1 0 1 0 1	010101
E4	12 13 14 15 16 17	0 1 0 1 0 1	010101
E5	16 17 18 19 20 21	0 1 1 1 1 0	011110
E6	20 21 22 23 24 25	1 0 0 0 0 1	100001
E7	24 25 26 27 28 29	0 1 0 1 0 1	010101
E8	28 29 30 31 32 1	0 1 0 1 0 1	010101

48-BIT EXPANDED OUTPUT

Some input bits appear twice; no new information is created.

011110 100001 010101 010101 011110 100001 010101 010101

Hexadecimal: 7A15557A1555