PESU Center for Information Security, Forensics and Cyber Resilience

Welcome to

PES University

Ring Road Campus, Bengaluru

PESU Center for
Information Security,
Forensics and
Cyber Resilience

APPLIED CRYPTOGRAPHY

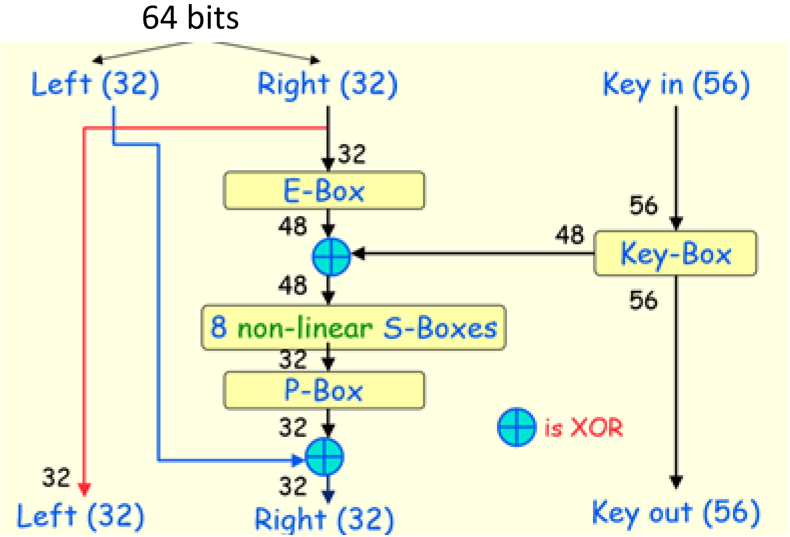
Private key Systems

Lecture 4

S-box and E-box

Substitution and extension box

One round of Fiestel cipher

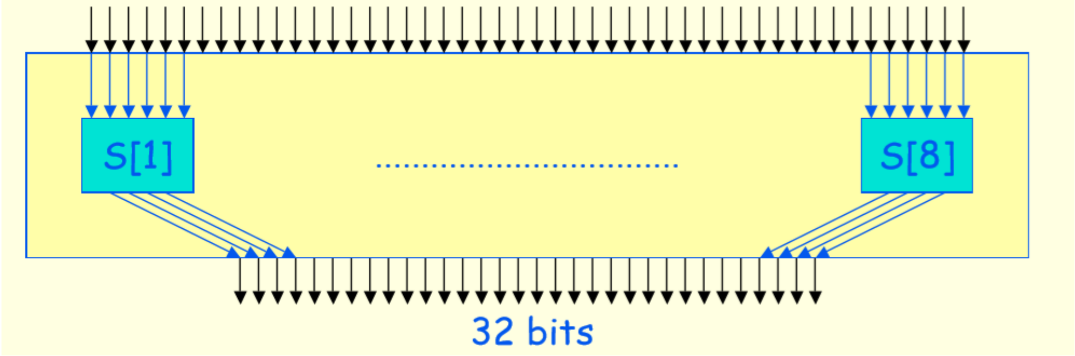


- 8 s-boxes
- 1 e-box
- *The round function in DES is a substitution-permutation network*
- *Block length of 64 bits and a key length of 56 bits are the shortcomings of DES*
- *Each S-box defines a 4 to 1 function*
- *Even though the best-known attack on DES is an exhaustive search, DES is insecure*

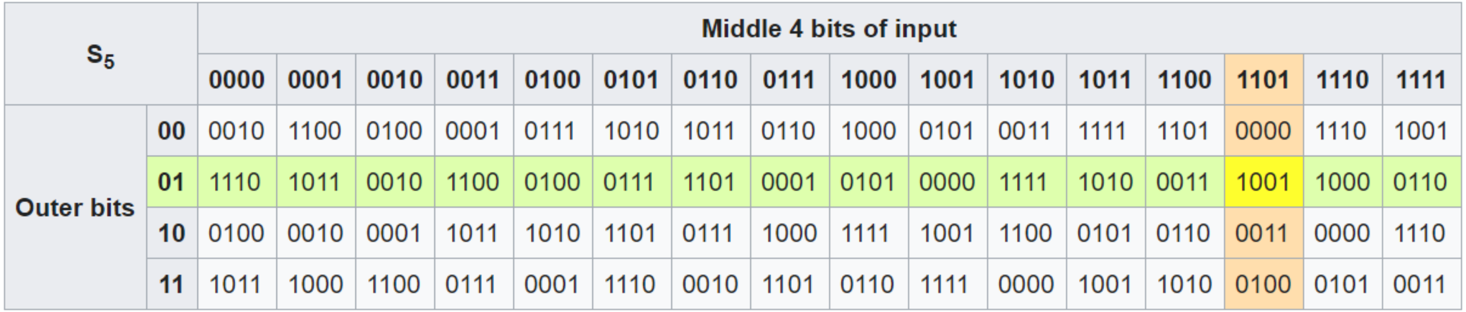
S-box

- *The S-boxes do the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.*

48 bits

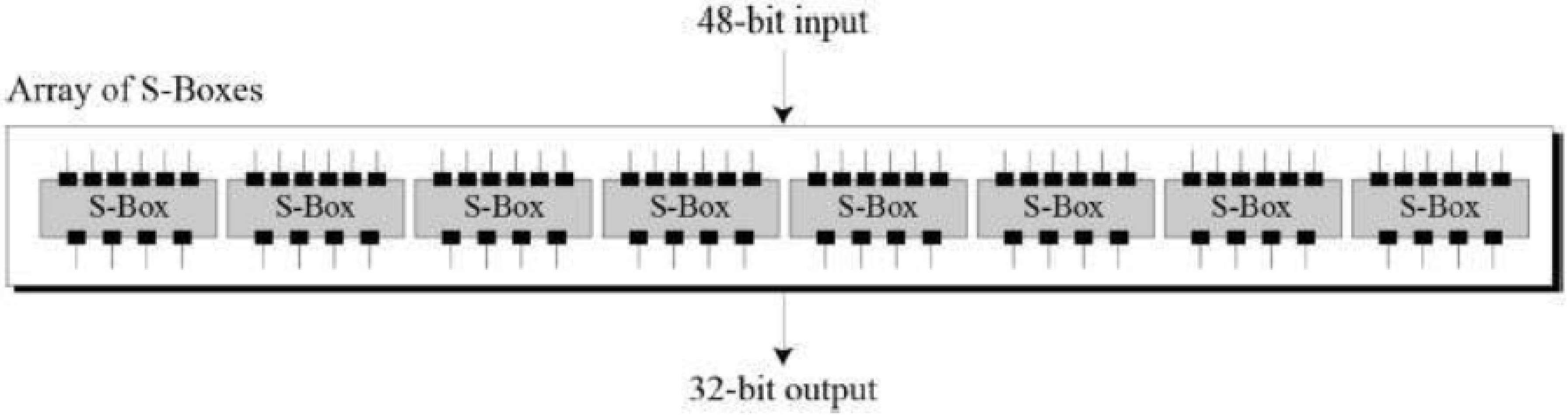


S box

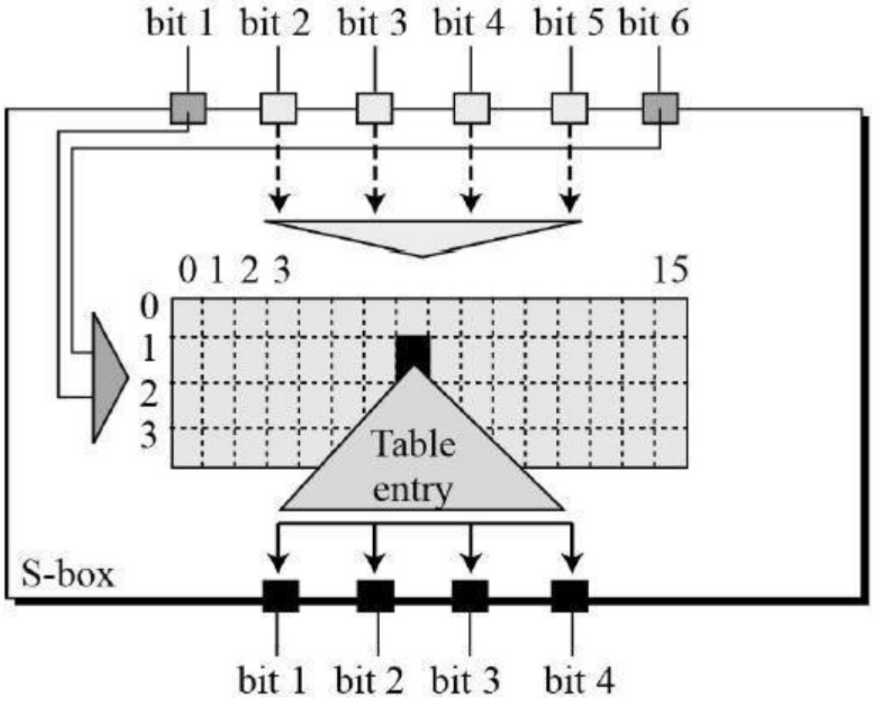


S_5		Middle 4 bits of input															
		0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**	**1000**	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**
Outer bits	**00**	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

8 S-Boxes in DES

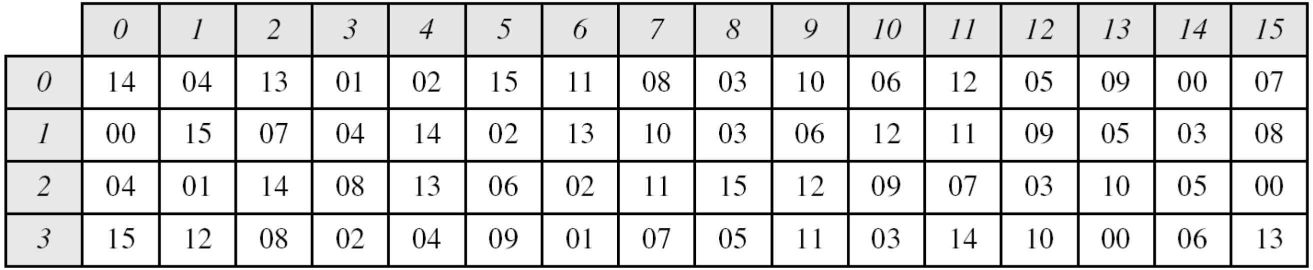


Working of s-box



- Each s-box takes 6 bit input
- First(bit1) and last(bit6) bit forms row value
- Remaining 4 bits(bit2-bit5) forms column value
- Output is 4 bit

The input to S-box 1 is 100011. What is the output?

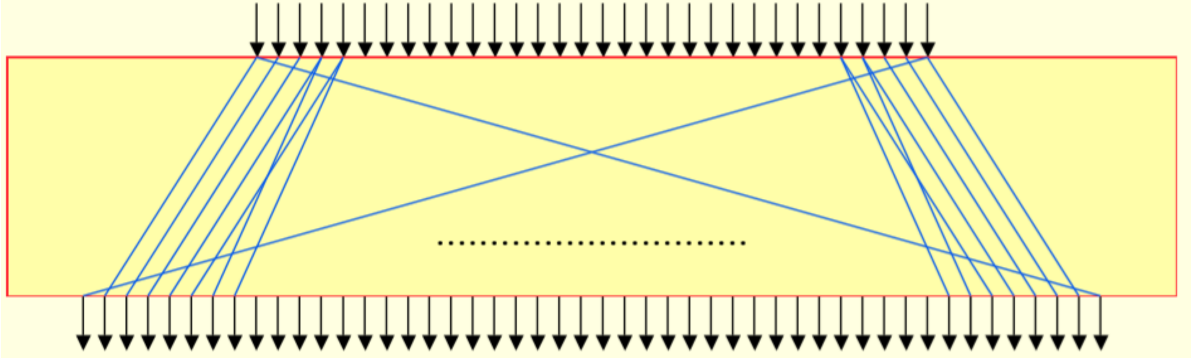


	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

E-box

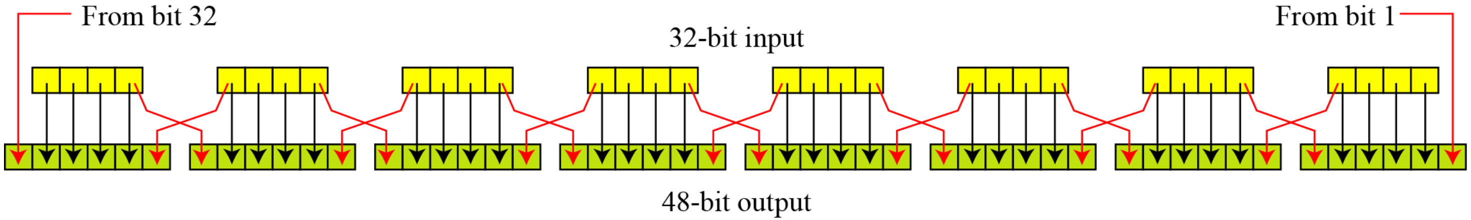
- E-box expands and permutates 32 bits to 48 bits

32 bits



48 bits

Expansion box (32 bit input 48 bit output)



1. E box take the left 32(left half) bits and expands it to 48 bits so that 48 bit key can be xor to it.

2. The o/p of step1(48 bits) is fed as i/p to 8 s-boxes (6 bits *8 = 48)

3. Each s-box produce 4 bits (4*8 = 32bits)

4. 32 bits will be concatenated to output

Avalanche effect

- Design S-boxes and mixing permutation (E-box) to ensure avalanche effect
  - Small differences should eventually propagate to entire output
- S-boxes: 1-bit change in input causes ≥2-bit change in output
  - Not so easy to ensure!
- Mixing permutation
  - Each bit output from a given S-box should feed into a *different* S-box in the next round

Thank you

Next Class

- ☞ Mandatory reading for the next class
    - ☞ https://link.springer.com/content/pdf/10.1007%2F3-540-46885-4_71.pdf

S Rajashree

Computer Science and Engineering

PES University, Bengaluru

PESU Center for Information Security, Forensics and Cyber Resilience

PESU Center for Internet of Things