Data Encryption Standard (DES)

Cryptographic Hardware for Embedded Systems

ECE 3170 A

Fall 2024

Assoc. Prof. Vincent John Mooney III

Georgia Institute of Technology

Reading Assignment

- Please read chapter 12 of the course textbook by Schneier

Data Encryption Standard (DES)

- In 1973, NIST (the National Institute of Standards and Technology – technically, in 1973 NIST was named the National Bureau of Standards) issued a public request for a standard cryptographic algorithm
  - High level of security dependent only on the key
  - Completely specified and easy to understand
  - Publically available
  - Usable in diverse application scenarios
  - Efficient & economical to implement in hardware
  - Validated & tested
- None of the large number of submissions was judged to meet the requirements, so the request was reissued in 1974
  - IBM submitted DES

DES Basics

- Block cipher
  - 64 bit plaintext input
  - 64 bit ciphertext output
- Key length is 56 bits
  - Eight bytes where the one bit out of every eight is used for parity check
  - A small number of keys are considered “weak” and should be avoided
- Simple description of DES: confusion and diffusion
  - substitution = confusion
  - permutation = diffusion
  - Each DES ***round*** consists of a substitution followed by a permutation
    - 16 rounds

Background: Linearity of XOR

- Given a two-bit XOR function, and two values reveals the third
- Examples:

DES Outline

- Plaintext input is 64 bits
- IP = Initial Permutation
- L_0 = most significant 32 bits, R_0 = least significant 32 bits
- Next 16 rounds (0…15) have same sequence of operations
  - Function ***f*** in round **i** combines R_i with K_{i+1}
- After the last round, R_{16} and L_{16} are joined with a final permutation (IP^{-1}) the inverse of the initial permutation (IP)

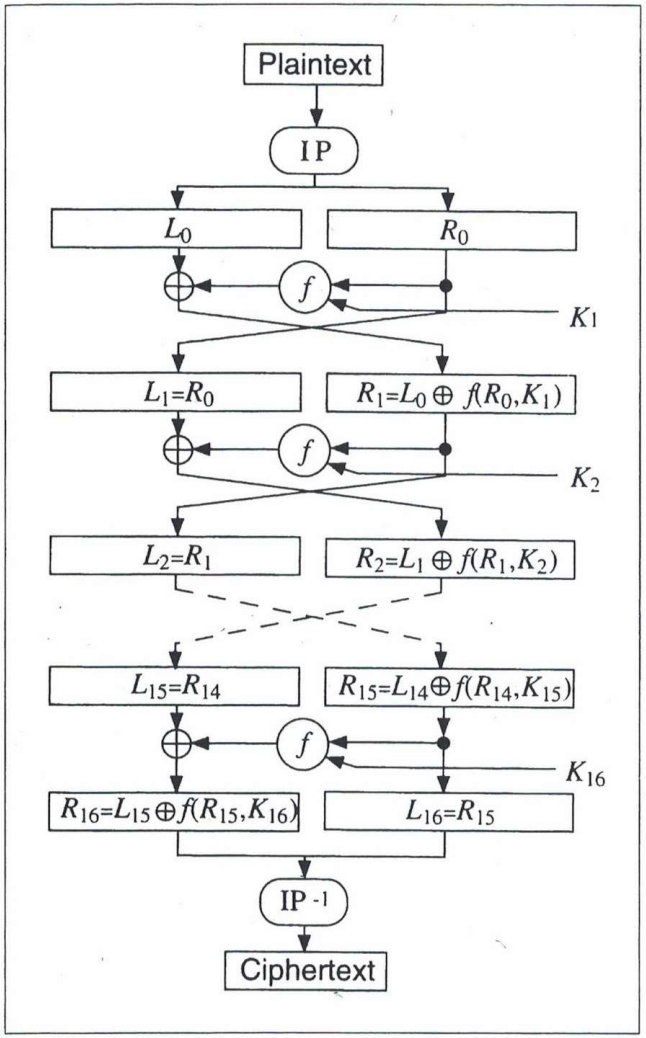

Figure 12.1 DES.

A DES Round

- Key bits shifted, then 48 bits selected

1) R_{i-1} expanded to 48 bits
2) Key bits permuted and XORed with R_{i-1}
3) Eight S-boxes produce 32 bits
4) 32 bits are permuted

- Function ***f*** is comprised of the above four steps
- Output of ***f*** XORed w/ L_{i-1}
  - Result: R_i
- $L_i = R_{i-1}$

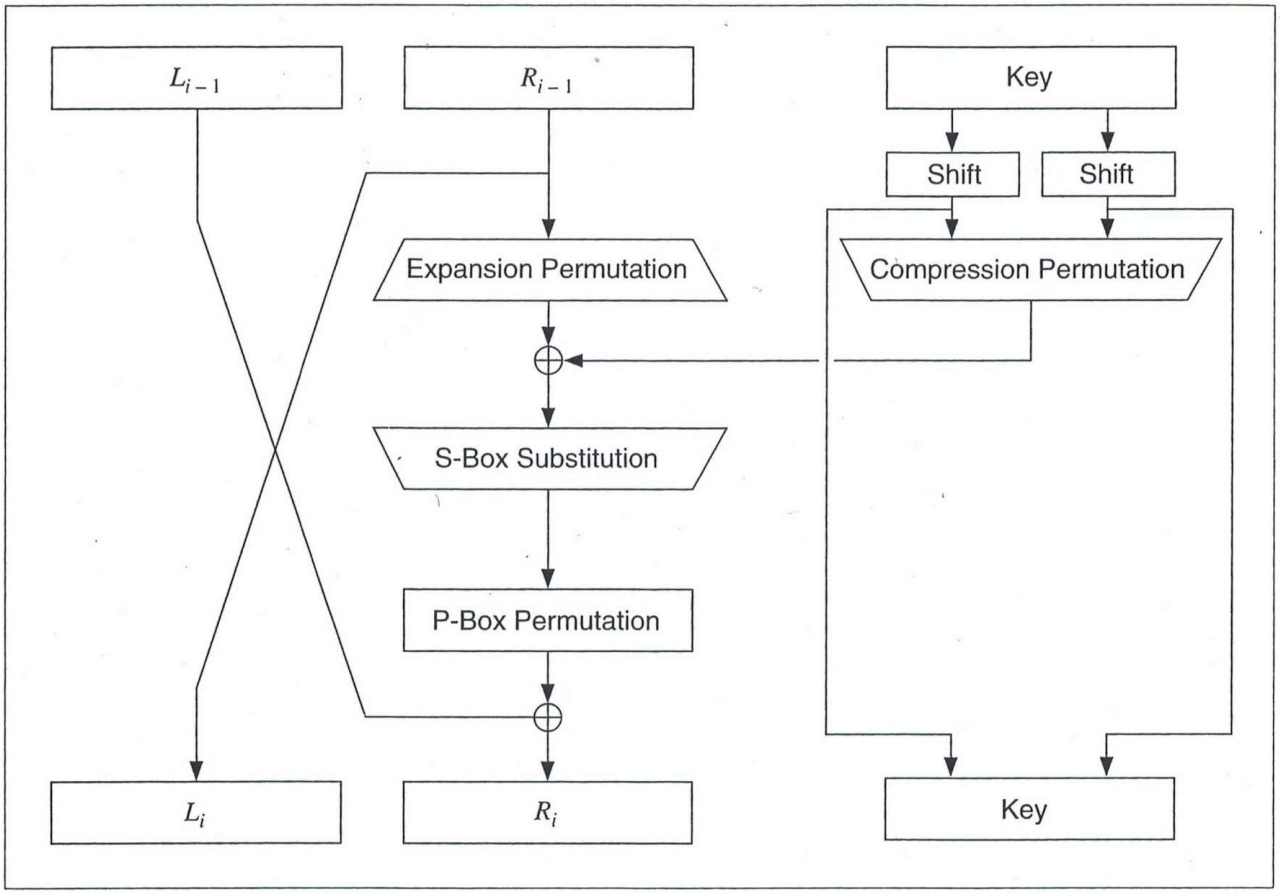

Figure 12.2 One round of DES.

Initial Permutation (IP)

Table 12.1
Initial Permutation

58,	50,	42,	34,	26,	18,	10,	2,	60,	52,	44,	36,	28,	20,	12,	4,
62,	54,	46,	38,	30,	22,	14,	6,	64,	56,	48,	40,	32,	24,	16,	8,
57,	49,	41,	33,	25,	17,	9,	1,	59,	51,	43,	35,	27,	19,	11,	3,
61,	53,	45,	37,	29,	21,	13,	5,	63,	55,	47,	39,	31,	23,	15,	7

- Read table left to right and top to bottom
- First entry says to move bit 58 of the plaintext input to bit 1
- Second entry says to move bit 50 of the plaintext input to bit 2
- Third entry says to move bit 42 of the plaintext input to bit 3
- And so on…
- IP and its inverse IP^{-1} do not appear to affect the security of DES
  - Some implementations omit IP and IP^{-1}

Key Permutation

Table 12.2
Key Permutation

57,	49,	41,	33,	25,	17,	9,	1,	58,	50,	42,	34,	26,	18,
10,	2,	59,	51,	43,	35,	27,	19,	11,	3,	60,	52,	44,	36,
63,	55,	47,	39,	31,	23,	15,	7,	62,	54,	46,	38,	30,	22,
14,	6,	61,	53,	45,	37,	29,	21,	13,	5,	28,	20,	12,	4

- First entry says to move bit 57 of the key input to bit 1
- Second entry says to move bit 49 to bit 2
- Third entry says to move bit 41 of the plaintext input to bit 3
- And so on…
- Note, however, that bits 64, 56, 48, 40, 32, 24, 16 and 8 are missing
  - Parity bits!
- Result of Table 12.2: 56-bit key

Key Shift (Barrel or Circular)

Table 12.3
Number of Key Bits Shifted per Round

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Number	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

- The 56-bit key is split into two 28-bit halves as shown in Figure 12.2
- Each half is barrel shifted to the left (the MSB rotates to the LSB)
  - A barrel shift is also known as a circular shift
- The shift amount is shown in Table 12.3

Key Compression Permutation (Permuted Choice)

Table 12.4
Compression Permutation

14,	17,	11,	24,	1,	5,	3,	28,	15,	6,	21,	10,
23,	19,	12,	4,	26,	8,	16,	7,	27,	20,	13,	2,
41,	52,	31,	37,	47,	55,	30,	40,	51,	45,	33,	48,
44,	49,	39,	56,	34,	53,	46,	42,	50,	36,	29,	32

- 48-bit subkeys are generated each round via compression permutation
  - The 56-bit shifted key (see Table 12.3) is the input
- First entry of Table 12.4 says to move bit 14 of the input to bit 1 of the output
- Second entry says to move bit 17 to bit 2
- …
- 35th entry says to move bit 33 to bit 35
- And so on…
- Due to the barrel shifting, different subsets of key bits are selected each round
  - Each key bit is used in approximately 14 of the 16 subkeys

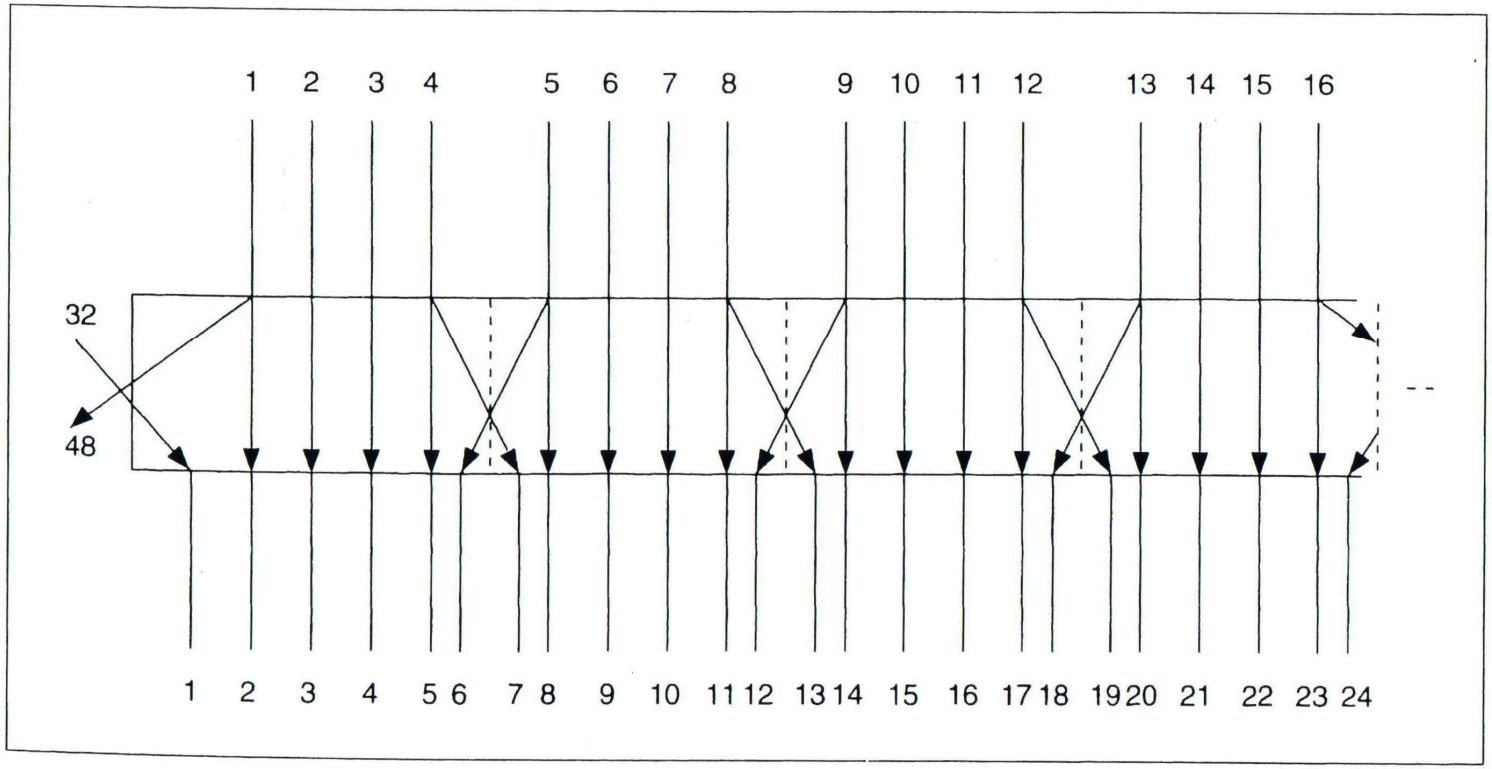

Figure 12.3 Expansion permutation.

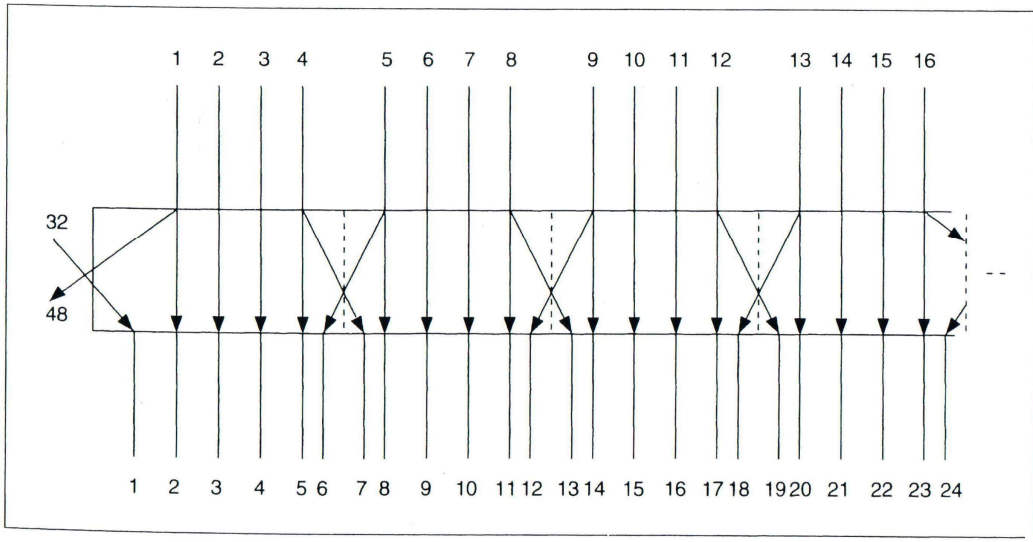

Figure 12.3 Expansion permutation.

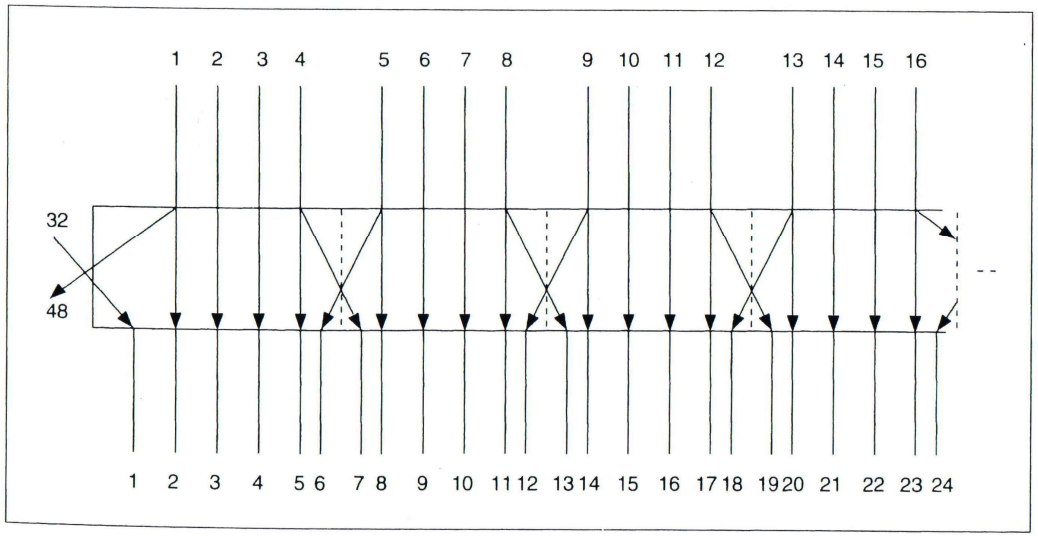

Figure 12.3 Expansion permutation.

Table 12.5
Expansion Permutation

1,	2,	3,	4,	5,	4,	5,	6,	7,	8,	9,
9,	10,	11,	12,	13,	12,	13,	14,	15,	16,	17,
17,	18,	19,	20,	21,	20,	21,	22,	23,	24,	25,
25,	26,	27,	28,	29,	28,	29,	30,	31,	32,	1

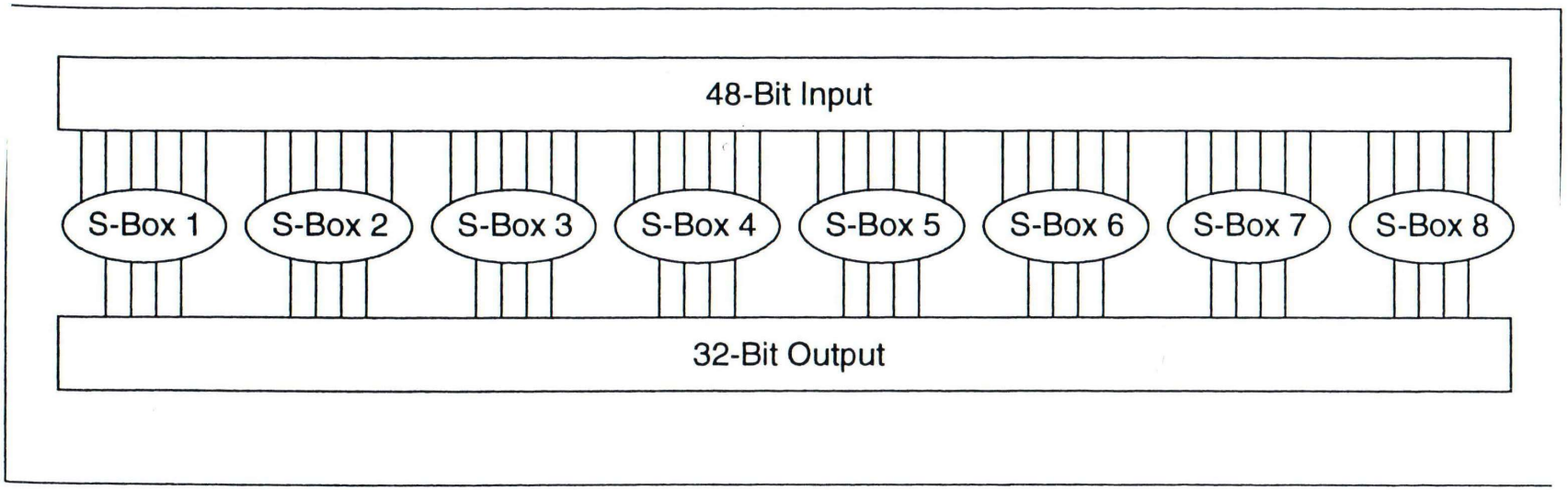

Figure 12.4 S-box substitution.

Table 12.6
S-Boxes

S-box 1:

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

S-box 2:

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

S-box 3:

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

S-box 4:

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

S-box 5:

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

S-box 6:

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

S-box 7:

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

S-box 8:

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

Table 12.6
S-Boxes

S-box 1:

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

S-box 2:

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

S-box 3:

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

S-box 4:

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

P-box Permutation

Table 12.7
P-Box Permutation

16,	7,	20,	21,	29,	12,	28,	17,	1,	15,	23,	26,	5,	18,	31,	10,
2,	8,	24,	14,	32,	27,	3,	9,	19,	13,	30,	6,	22,	11,	4,	25

- Straightforward 32-bit permutation
- E.g., bit 21 moves to bit 4
- E.g., bit 4 moves to bit 31

Final Permutation (IP^{-1})

Table 12.8
Final Permutation

40,	8,	48,	16,	56,	24,	64,	32,	39,	7,	47,	15,	55,	23,	63,	31,
38,	6,	46,	14,	54,	22,	62,	30,	37,	5,	45,	13,	53,	21,	61,	29,
36,	4,	44,	12,	52,	20,	60,	28,	35,	3,	43,	11,	51,	19,	59,	27,
34,	2,	42,	10,	50,	18,	58,	26,	33,	1,	41,	9,	49,	17,	57,	25