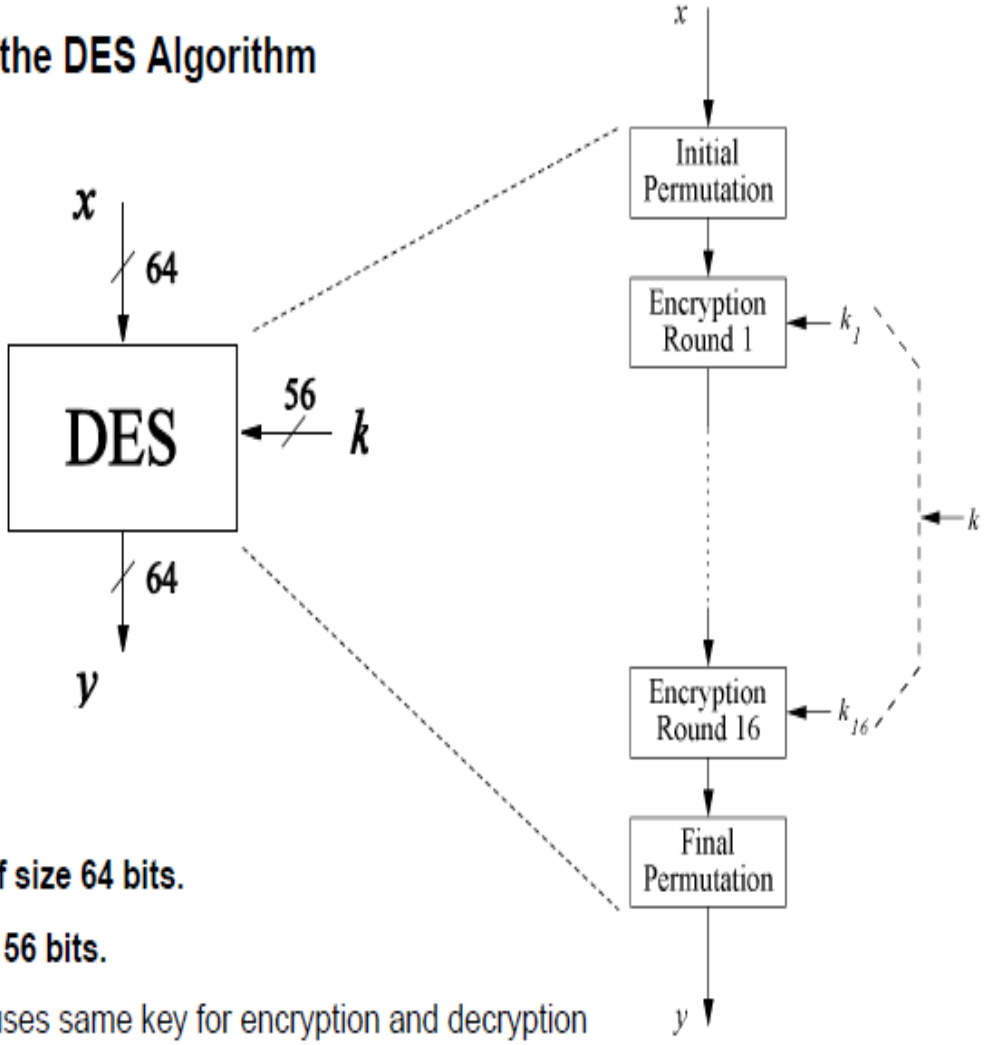
Data Encryption Standard (DES) or Data Encryption Algorithm (DEA)

- ➔ is a **block cipher**.
- ➔ Even though it is on the way out, no discussion of block ciphers can be complete without DES.
- ➔ is a remarkably **well-engineered algorithm** which has had a powerful influence on cryptography.
- ➔ DES is in very **widespread use** and probably will be for some years to come.
- ➔ Every time you use an **ATM machine you are using DES**.
- ➔ In **1972 the NBS (National Bureau of Standards, now NIST, the National Institute of Science and Technology) initiated a program for data protection and wanted as part of it an encryption algorithm that could be standardized.**
- ➔ They put out a request for such an algorithm.
- ➔ In **1974, IBM responded with a design based on their "Lucifer"** algorithm. This design eventually evolved into the DES.
- ➔ DES has a **key-length of k = 56 and a block-length of l = 64**.
- ➔ It consists of **16 rounds** of what is called a "**Feistel network**."
- ➔ After NBS, several other bodies **adopted DES** as a standard, including **ANSI** (the American National Standards Institute) and the American Bankers Association.
- ➔ The standard was to be reviewed every five years to see whether or not it should be re-adopted.
- ➔ Although there were claims that it would not be re-certified, the algorithm was re-certified again and again.
- ➔ Only recently did the work for finding a replacement begin in earnest, in the form of the **AES (Advanced Encryption Standard)** effort.
- ➔ **DES proved remarkably secure**. There has, since the beginning, been a concern, especially about exhaustive key-search. But for a fair length of time, the key size of 56 bits was good enough against all but very well-funded organizations.
- ➔ Attacks significantly different from key search emerged only in the nineties, and even then don't break DES in a sense significant in practice.
- ➔ But **with today's technology, 56 bits is too small a key size for many security applications**.

- Data Encryption Standard (DES) encrypts **blocks of size 64 bit**.
- Developed by **IBM** based on the cipher *Lucifer* under influence of the *National Security Agency* (NSA), the design criteria for DES have not been published
- **Standardized 1977** by the **National Bureau of Standards** (NBS) today called *National Institute of Standards and Technology* (NIST)
- Most popular **block cipher** for most of the last 30 years.
- By far best studied symmetric algorithm.
- Nowadays considered insecure due to the small **key length of 56 bit.**
- **But: 3DES yields very secure cipher**, still widely used today.
- Replaced by the *Advanced Encryption Standard* (**AES**) in 2000

Overview of the DES Algorithm



- **Encrypts blocks of size 64 bits.**
- **Uses a key of size 56 bits.**
- Symmetric cipher: uses same key for encryption and decryption
- Uses 16 rounds which all perform the identical operation
- Different subkey in each round derived from main key

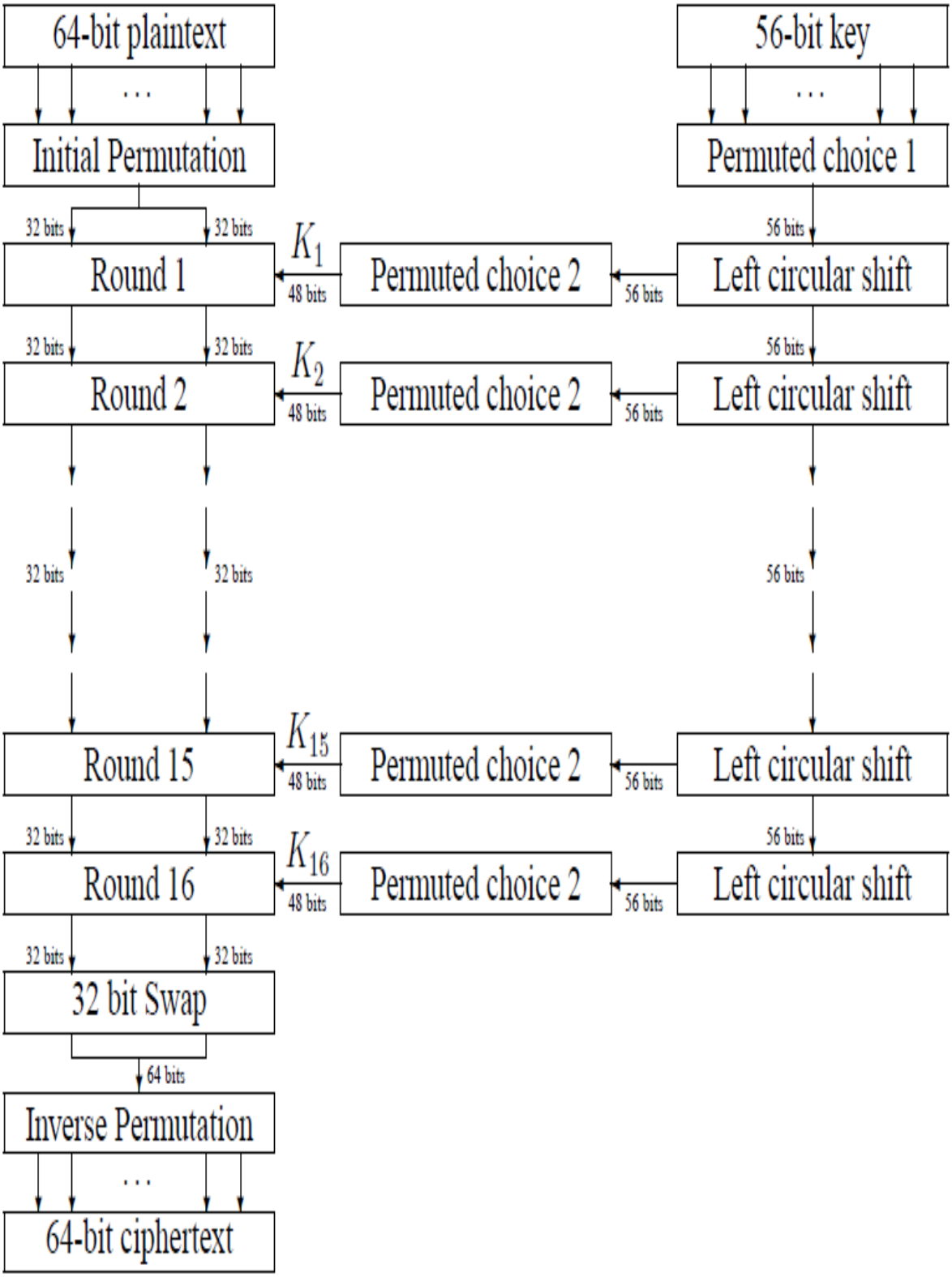
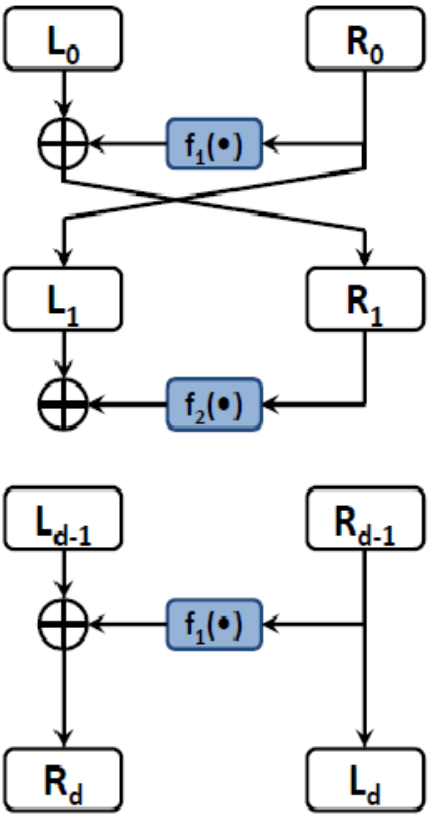


Figure 2.2: Flow Diagram of DES algorithm for encrypting data.

Feistel Network



- **Encryption:**
  - $L_1 = R_0 \quad R_1 = L_0 \oplus f_1(R_0)$
  - $L_2 = R_1 \quad R_2 = L_1 \oplus f_2(R_1)$
  - ...
  - $L_d = R_{d-1} \quad R_d = L_{d-1} \oplus f_d(R_{d-1})$
- **Decryption:**
  - $R_{d-1} = L_d \quad L_{d-1} = R_d \oplus f_d(L_d)$
  - ...
  - $R_0 = L_1; \quad L_0 = R_1 \oplus f_1(L_1)$

(a) Initial Permutation (IP)

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

(b) Inverse Initial Permutation (IP^{-1}) (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

(To be performed on Plain Text Block (PT) of 64 bits at the beginning and end respectively)

Key Schedule (1) Or The Permuted Choice 1 (PC-1)

- Derives 16 round keys (or *subkeys*) k_i of 48 bits each from the original 56 bit key.
- The input key size of the DES is 64 bit: **56 bit key** and 8 bit parity:

(a) Input Key

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

Permuted Choice One (PC-1)

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

PC-1 (Permutation of 56 bits)

Schedule of Left Shifts

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

The Following bits are dropped

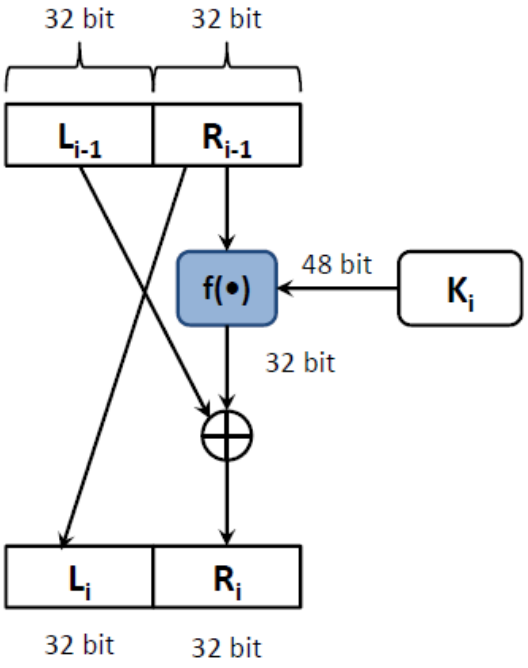
9	18	22	25	35	38	43	54

Permuted Choice Two (PC-2) (Permutation of 48 bits)

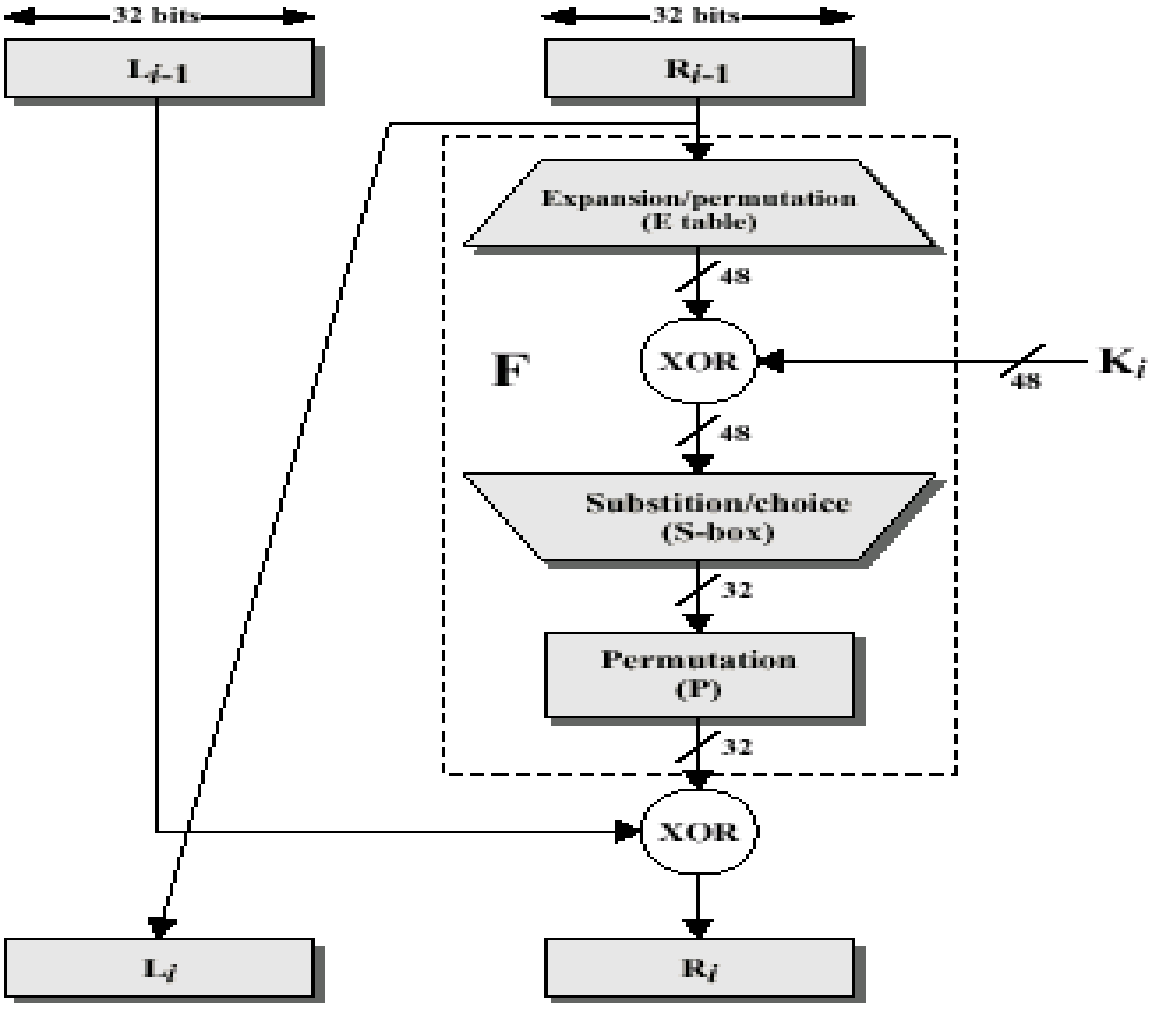
14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

DES Round i

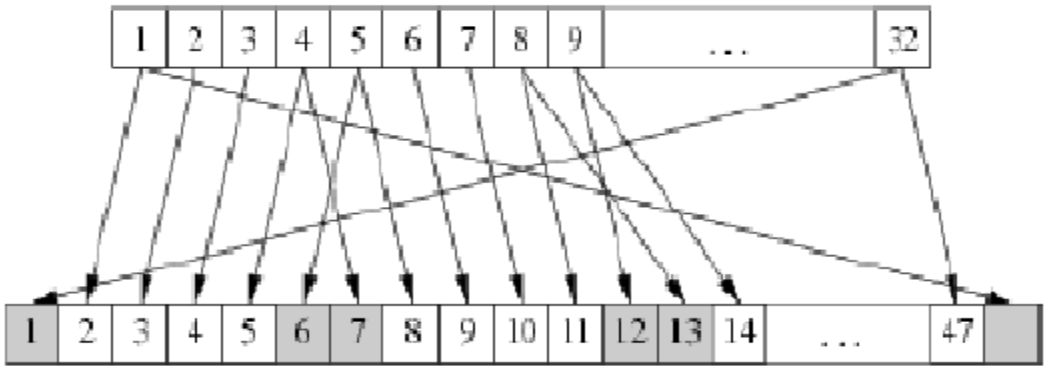
- $L_i = R_{i-1}$
- $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$



Details of Single Round



DES Expansion function (expansion of 32-bit RPT to 48 bits

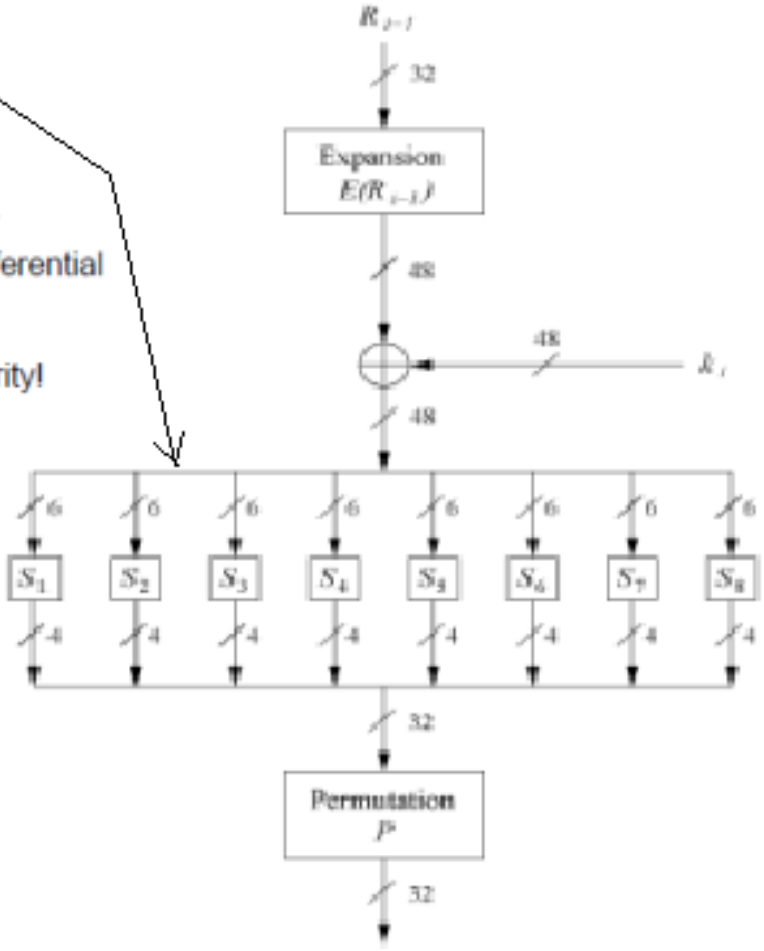


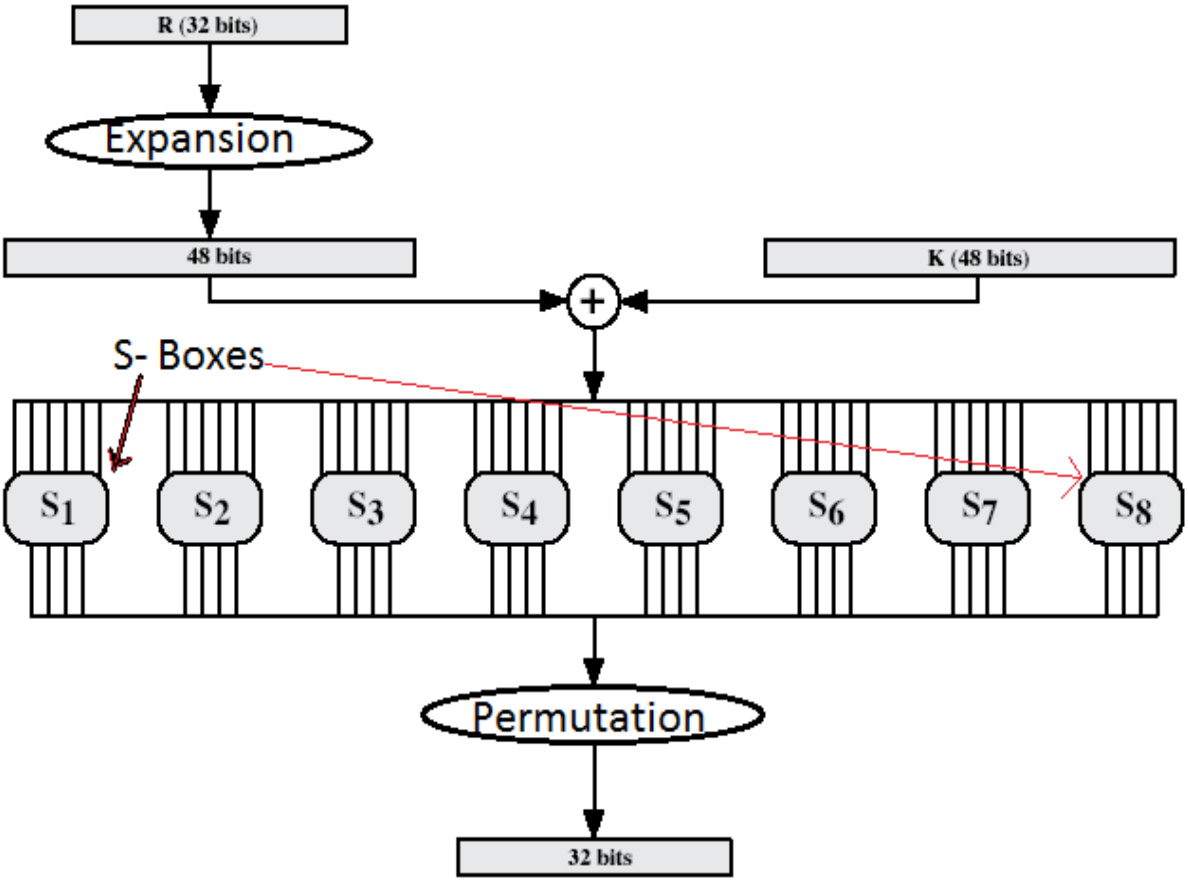
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

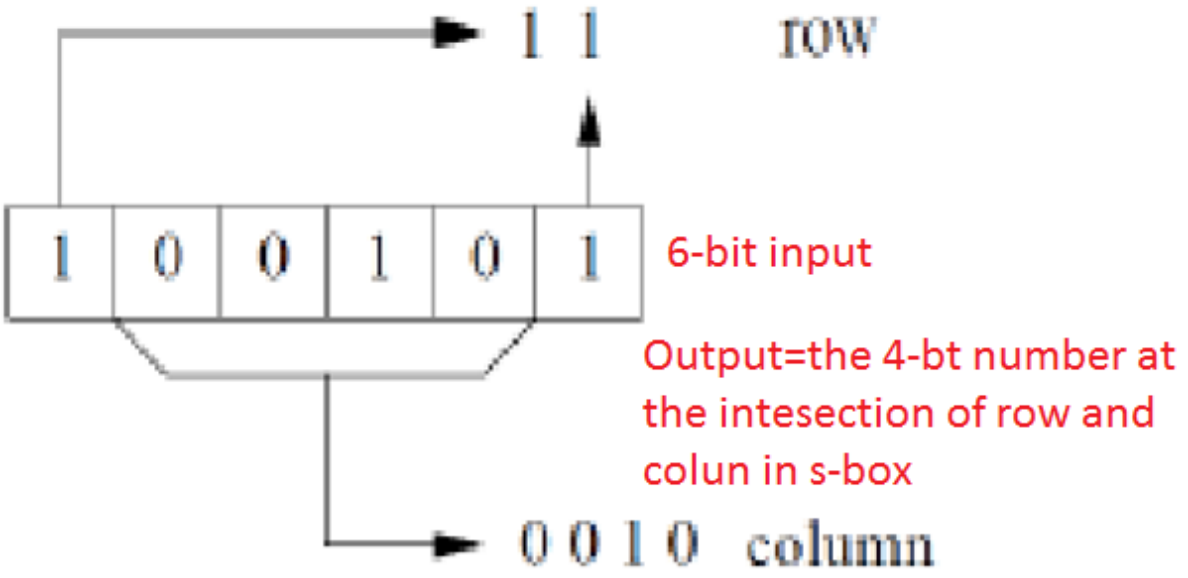
The DES S-Boxes

S-Box substitution

- Eight substitution tables.
- 6 bits of input, 4 bits of output.
- Non-linear and resistant to differential cryptanalysis.
- Crucial element for DES security!







6-bits to 4-bits conversion

Col->	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Row
S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	0
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	1
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	2
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	3

S_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_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_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_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_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_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_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

After substitution, the function output is now 32 bits and it goes through a fixed 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