The Data Encryption Standard (DES)

NBS 1972 call:

1. It must provide a high level of security.
2. It must be completely specified and easy to understand.
3. The algorithm itself must provide the security; the security should not depend on the secrecy of the algorithm.
4. It must be available to all users.
5. It must be adaptable for use in diverse applications.
6. It must be economical to implement in electronic devices.
7. It must be efficient to use.
8. It must be able to be validated.
9. It must be exportable.

IBM's Lucifer 1976

DEA, DES

↑ algorithm

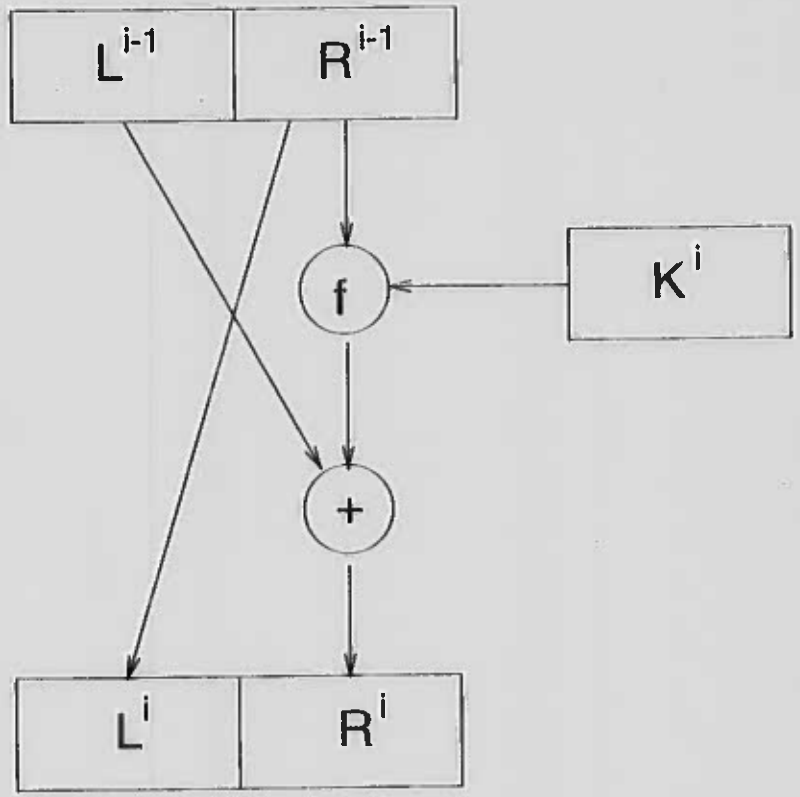


FIGURE 3.6
One round of DES encryption

$$L_j = R_{j-1}$$

$$R_j = L_{j-1} \oplus f(R_{j-1}, k_j)$$

$$R_{j-1} = L_j$$

$$L_{j-1} = R_j \oplus f(R_{j-1}, k_j).$$

$$L_{j-1} = R_j \oplus f(L_j, k_j).$$

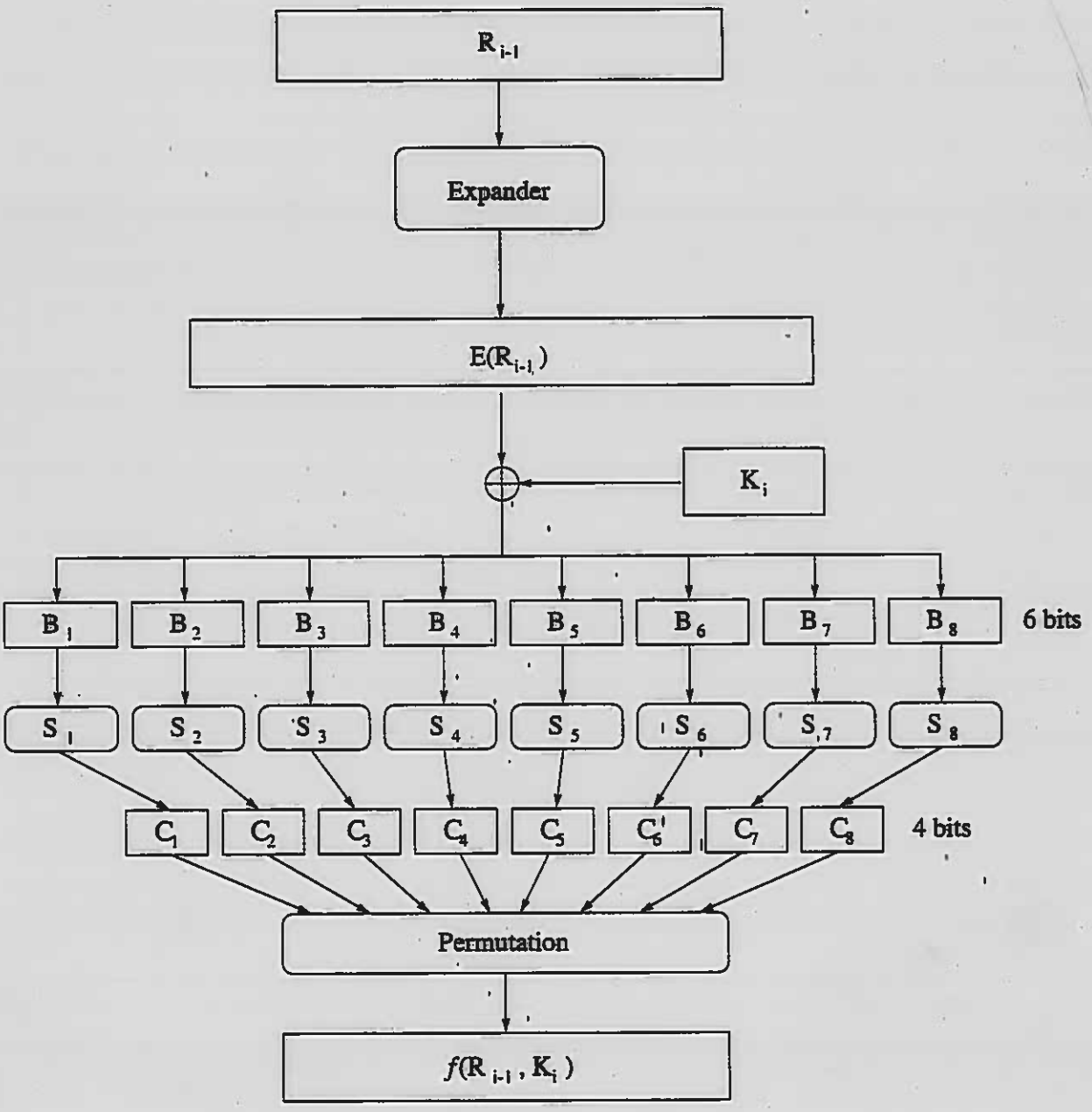


Figure 4.5: The DES Function $f(R_{i-1}, K_i)$.

DES s-boxes from FIPS-46-2

S1

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

S2

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

S3

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

S4

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

S5

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

S6

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

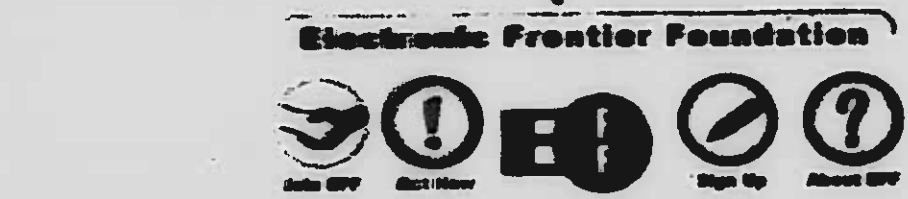
S7

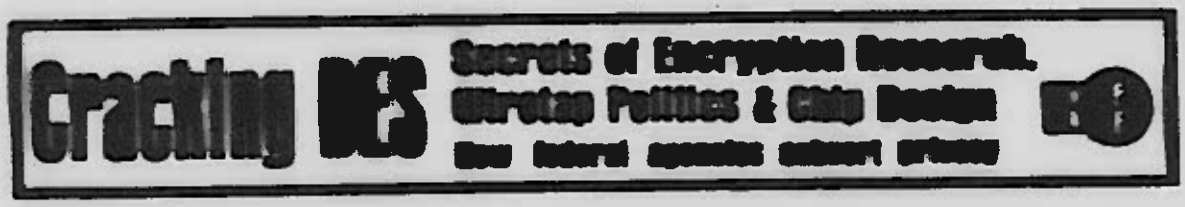
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8

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

www.eff.org/descracker.html





EFF press release (July 17, 1998): EFF Builds DES Cracker that proves that Data Encryption Standard is insecure

Table of Contents

Triple DES

168 bit $E_{K_1} E_{K_2} E_{K_3}(m)$

112 bit $E_{K_1} D_{K_2} E_{K_1}(m)$

56 bit $K_1 = K_2$

DESX, 168 bits

$$K_3 \oplus E_{K_2}(K_1 \oplus m)$$

Modes of Operation

- *electronic codebook mode* (ECB mode),
- *cipher feedback mode* (CFB mode),
- *cipher block chaining mode* (CBC mode), and
- *output feedback mode* (OFB mode).

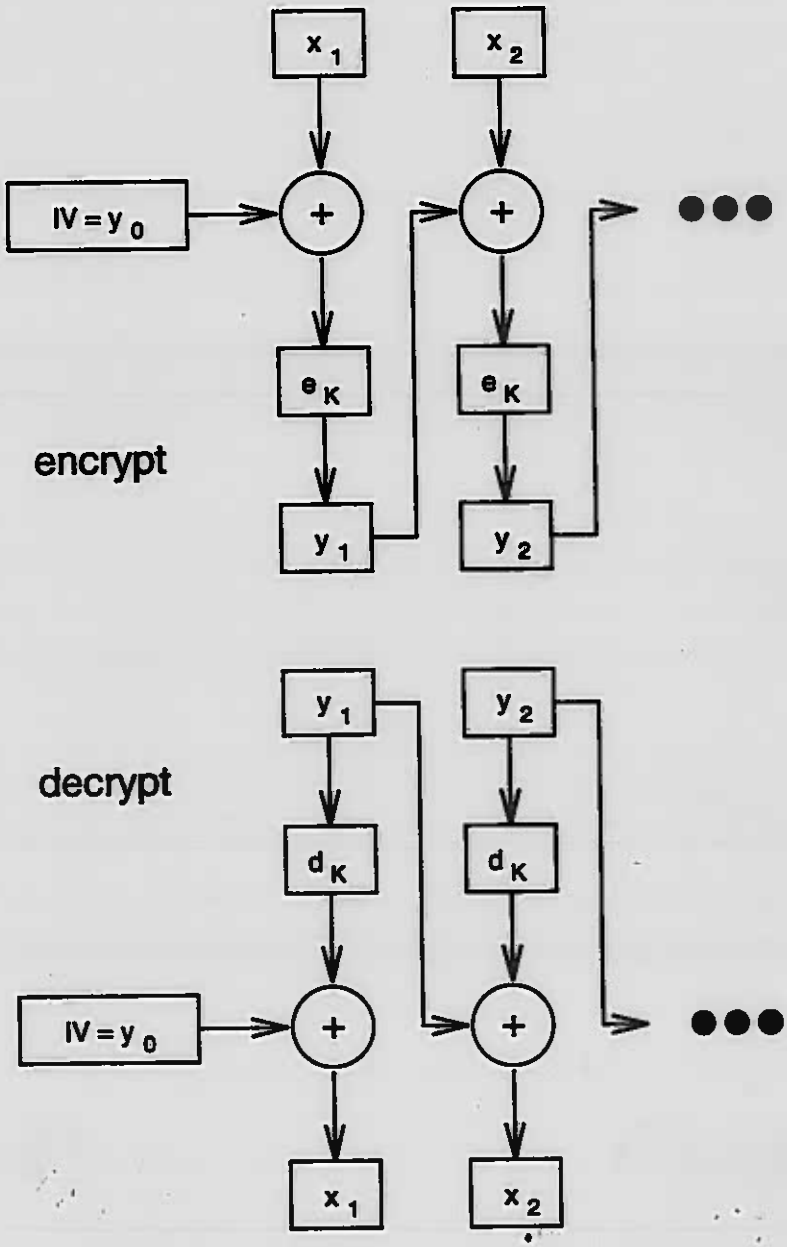
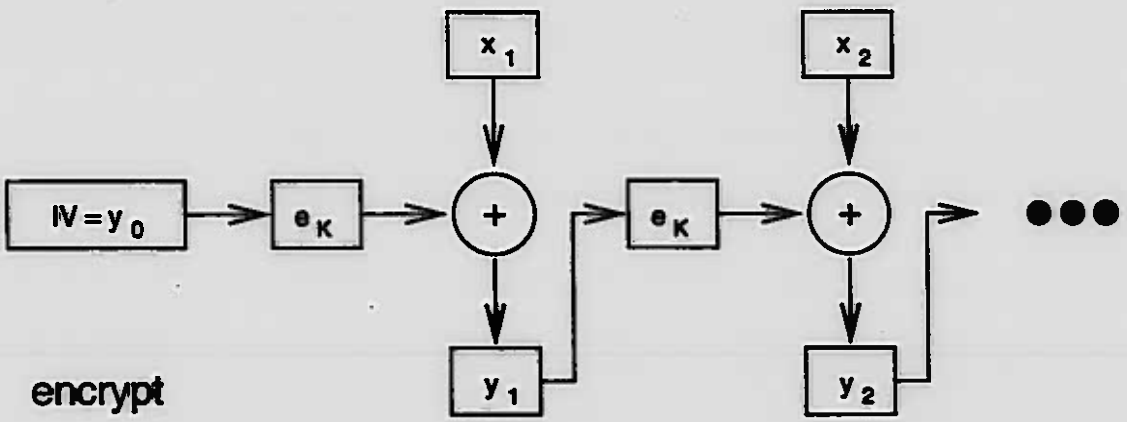


FIGURE 3.9
CBC mode

Cipher Block Chaining

$y_0 = IV$

$y_i = e_K(x_i \oplus y_{i-1})$



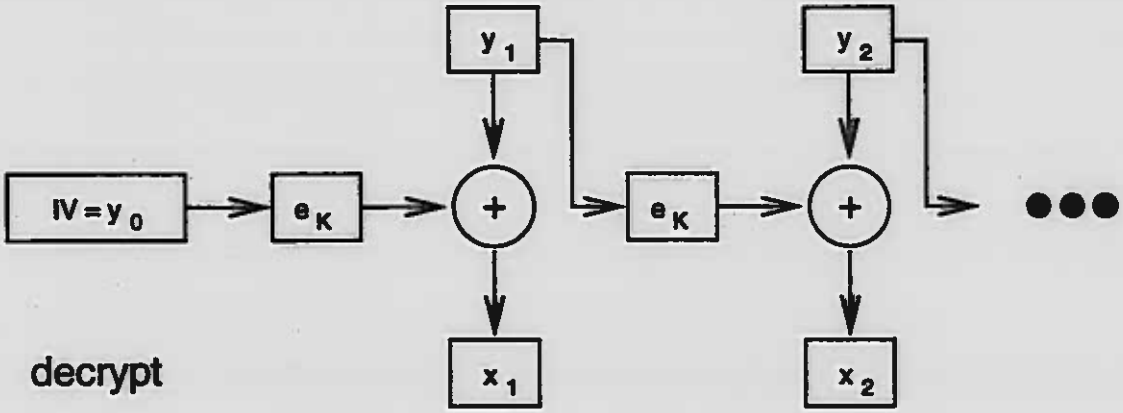


FIGURE 3.10
CFB mode

cipher feedback mode

$y_0 = IV$
$z_i = e_K(y_{i-1})$
$y_i = x_i \oplus z_i$