

# Symmetric Key Cryptography

- Block ciphers (DES)
  - Substitution cipher
  - Transposition cipher
  - Product cipher
  - Feistel cipher
- Stream cipher = block cipher with (RC4)  
 $| \text{block} | = 1$

# Substitution ciphers

simple

a b c d e f g h i j k l m n o p q r s t u v w x y z  
d e f g h i j k l m n o p q r s t u v w x y z a b c

M= this cipher is certain    ynots    secure

C= wklvf    lskhu    lvfhu    wdlqo    bqrwv    hfxuh

# Shift ciphers

Es. *shift cipher*

$|A| = s$ ,  $m_i \in A$  with  $0 \leq i \leq s-1$  then

$$C_i = e(m_i) = m_i + k \bmod s$$

$$m_i = d(C_i) = C_i - k \bmod s$$

**CAESAR** cipher  $s=26$ ,  $k=3$

$m =$  BrunoCrispo

$c =$  EuxqrFulsr

# Polyalphabetic substitutions

$|A| = s$ , period  $t$ , keys  $k_i$ ,  $0 \leq i \leq t-1$

$t$  keys consisting of permutations

$$C_i = e(m_i) = m_i + k_i \bmod s$$

$$m_i = d(C_i) = C_i - k_i \bmod s$$

# Vigenere ciphers

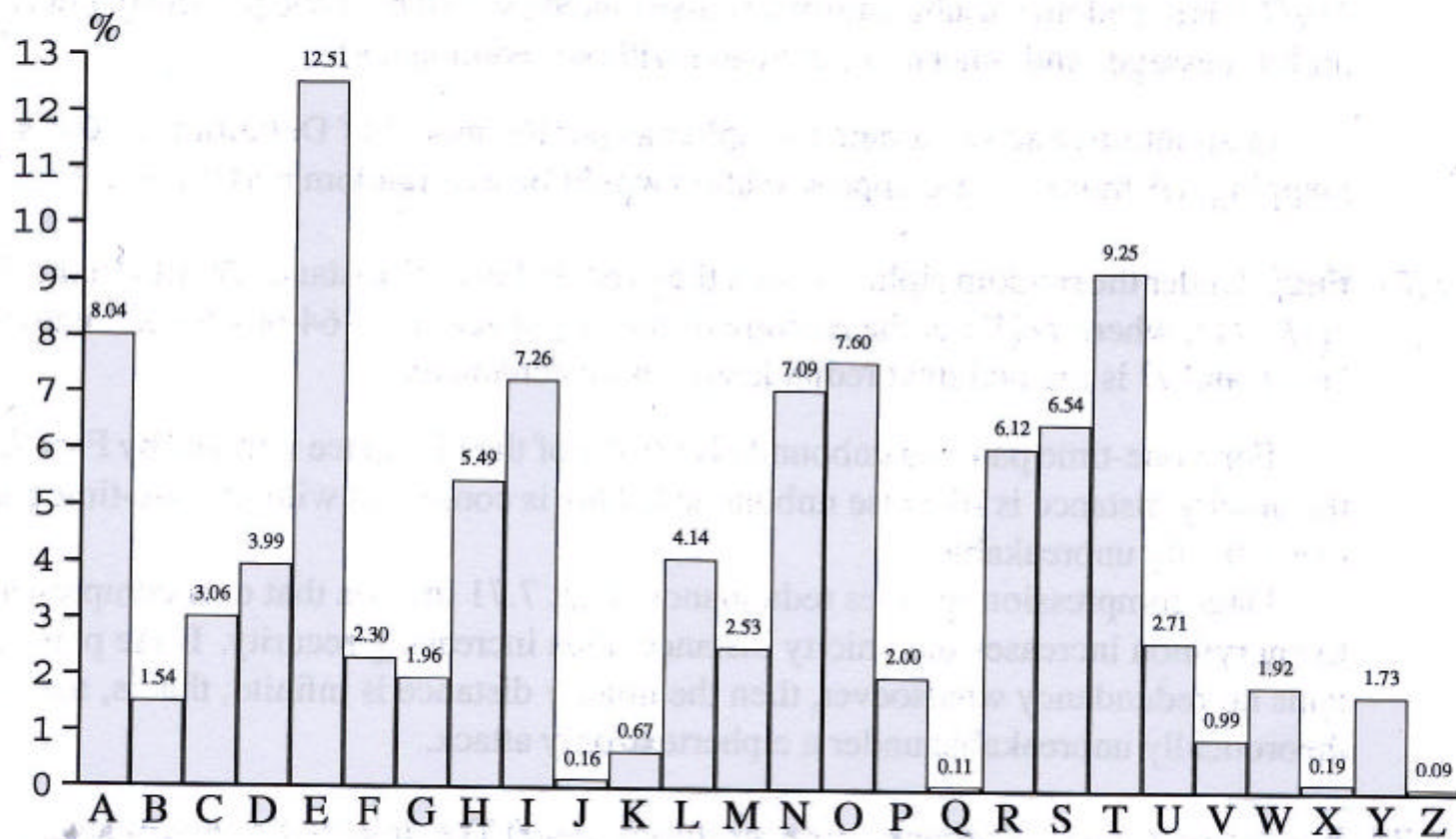
VIGENERE cipher  $t=3$

$k_0=1, k_1=2, k_2=3$

$m=$  THI SCI PHE RIS NOT SEC URE

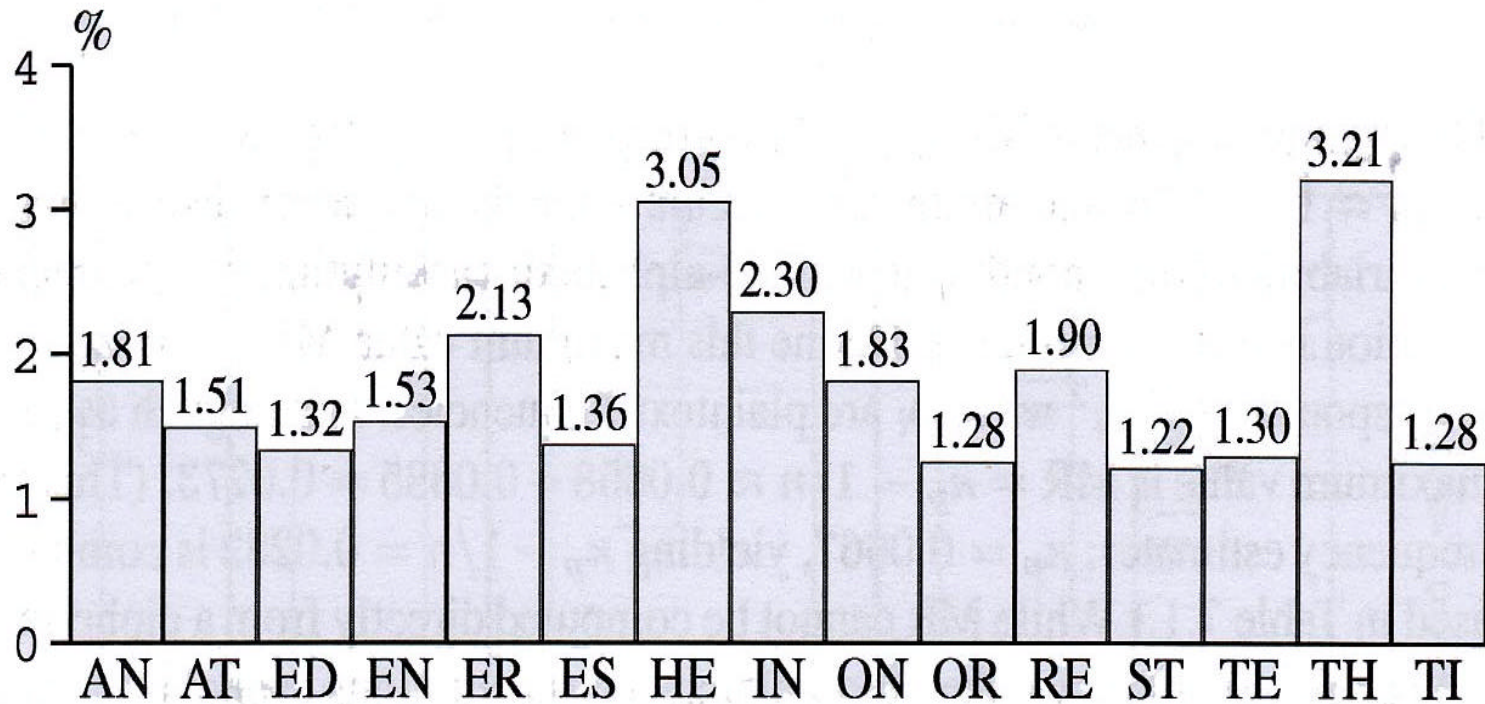
$c =$  UJL TEL QJH SKV OQW TGF WTH

# Language statistics



**Figure 7.5:** Frequency of single characters in English text.

# Language statistics



**Figure 7.6:** Frequency of 15 common digrams in English text.

# Polygram ciphers

## Playfair

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

M= ea hs ar mu

C= IM BP RM CM



# Statistical cryptanalysis

- **Unicity distance (UD)**: minimum amount of ciphertext to recover a key given unlimited computational power

carried information  $\lg 26 = 4.7 \text{ bit/char}$

entropy = 1.5    redundancy =  $D = 4.7 - 1.5 = 3.2$

Es. simple sub.

$$UD = H(K)/D = \lg(26!)/D = 88.4/3.2 \approx 28$$

$H(k)$  entropy of the key space

# Transposition ciphers

M= attack postponed until two am

Key:                   4 3 1 2 5 6 7

Plaintext:           a t t a c k p  
                      o s t p o n e  
                      d u n t i l t  
                      w o a m x y z

Cipher: ttnaaptmtsuoaoawcoixknlypetz

# Exercises

M=?

C=ftqcguowndaizrajvgymbahqdf tqxmlkpas

M=?

C=uzqsovuohxmopvgpozpevs gzw szopf pesx  
udbmetsxaizvuephzhmdzshzowsfpappdtsv  
pquzwymxuzuh sxepyepopdzszufpo

*English trigram: the, and, tha, ent, ion*

# Product ciphers

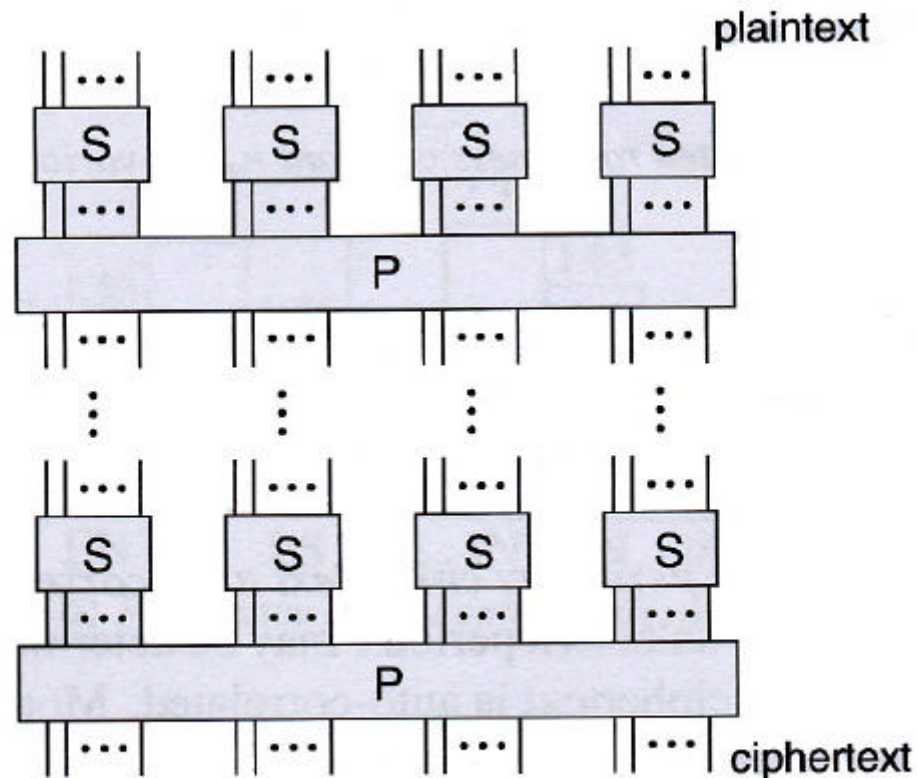
- Substitution  $\rightarrow$  confusion  $K \leftrightarrow C$
- Permutation  $\rightarrow$  diffusion  $M \leftrightarrow C$

The diagram illustrates the combination of substitution and permutation in a product cipher. It shows three rows of letters:

- Row 1: a b c d e f g h i j k l m n o p q r s t u v w x y z
- Row 2: d e f g h i j k l m n o p q r s t u v w x y z a b c
- Row 3: b q f d z i j m l k n y v h x c w u p e r o t a g s

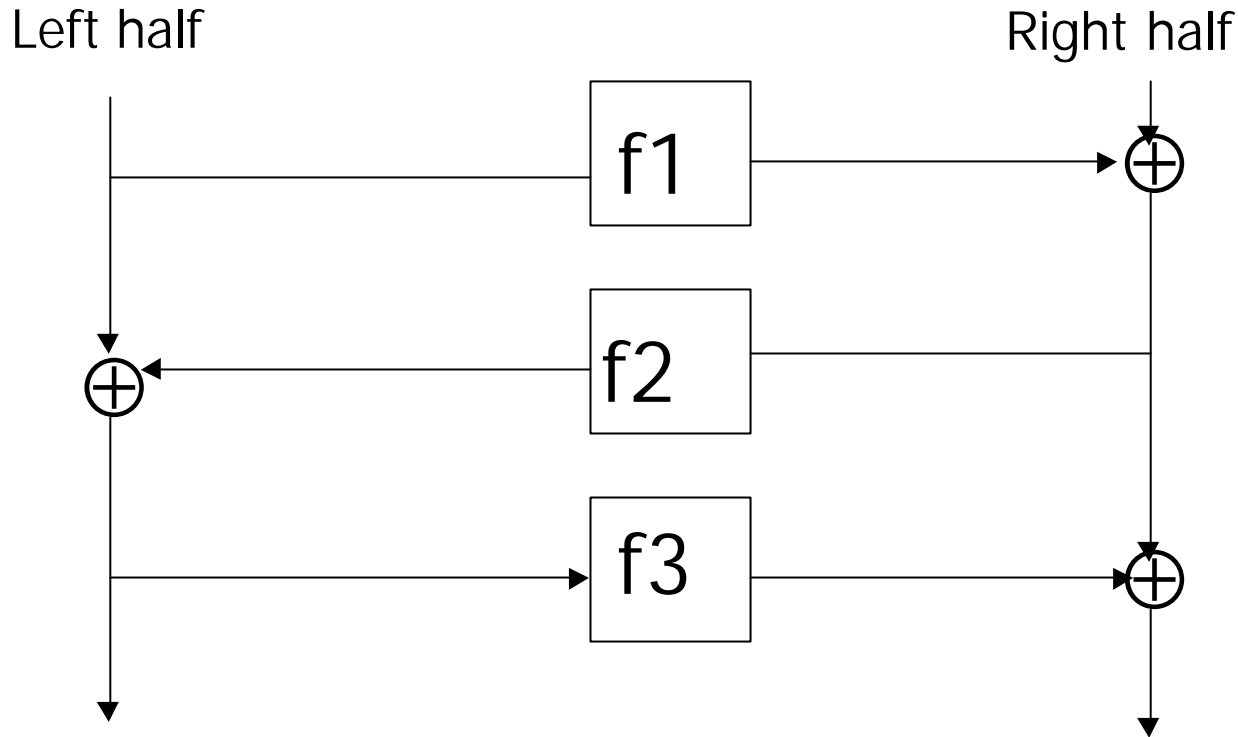
Red arrows indicate the mapping from Row 1 to Row 3, showing a permutation. Blue letters (b, e, e) in Row 3 correspond to blue letters (b, e, e) in Row 1, indicating a substitution. The red arrows show that the letters in Row 1 are first permuted to form Row 2, and then each letter in Row 2 is substituted to form Row 3.

# SP-Networks



**Figure 7.7:** Substitution-permutation (SP) network.

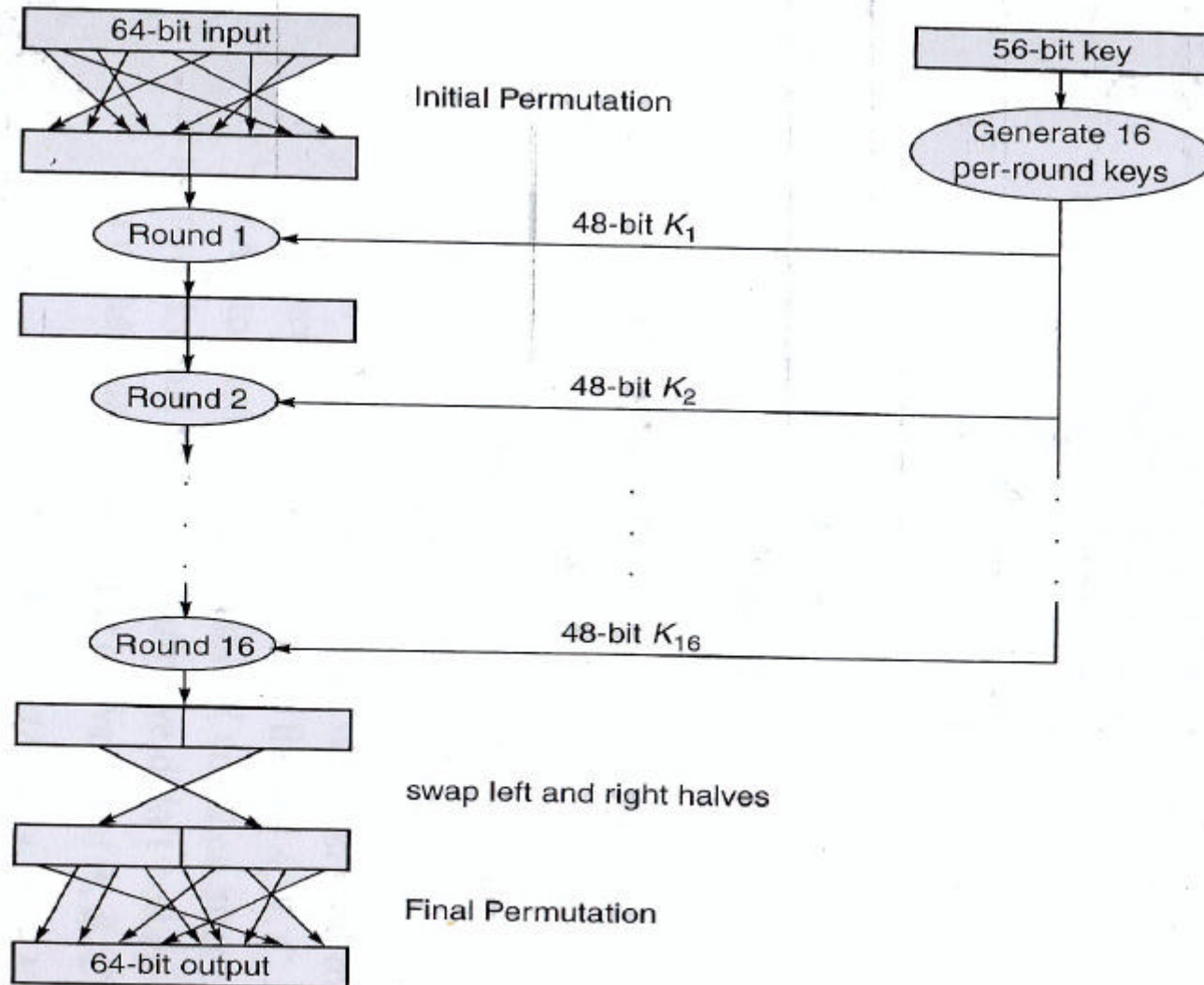
# Feistel ciphers



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

$$\Psi^{-1}(f1, f2, f3) = \Psi(f3, f2, f1)$$

# DES: Data Encryption Standard



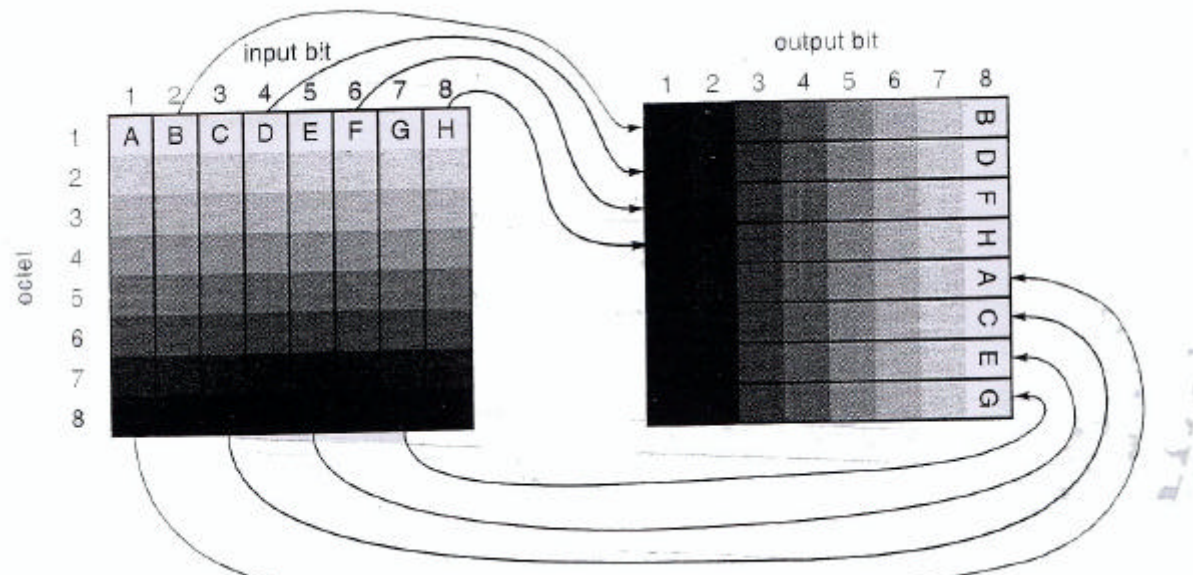
# DES Permutations

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

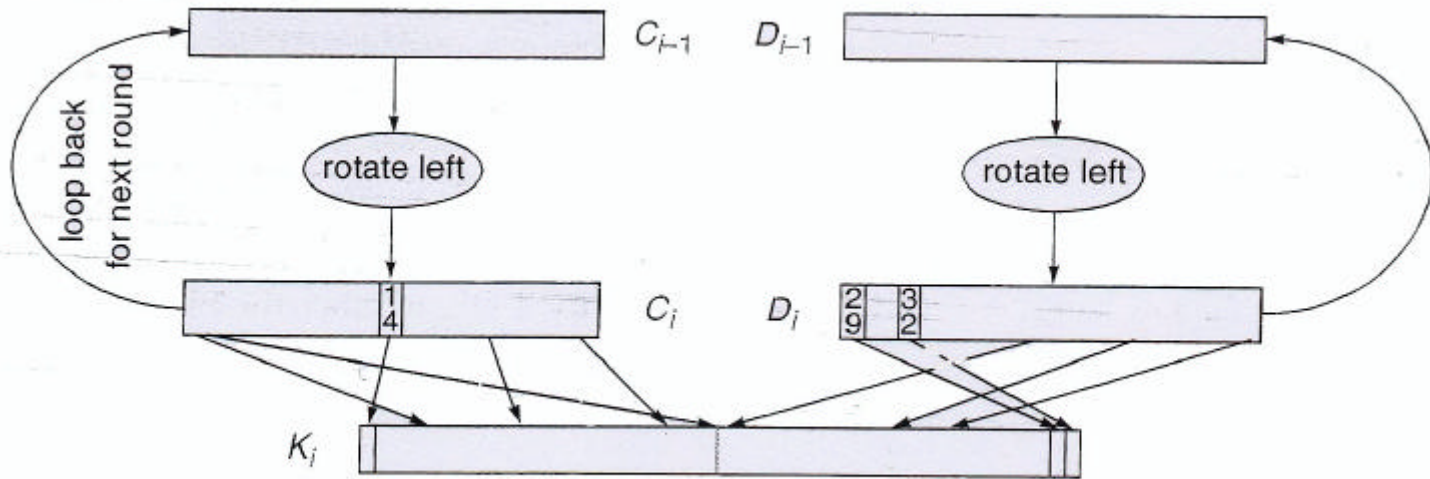
Final Permutation ( $IP^{-1}$ )

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





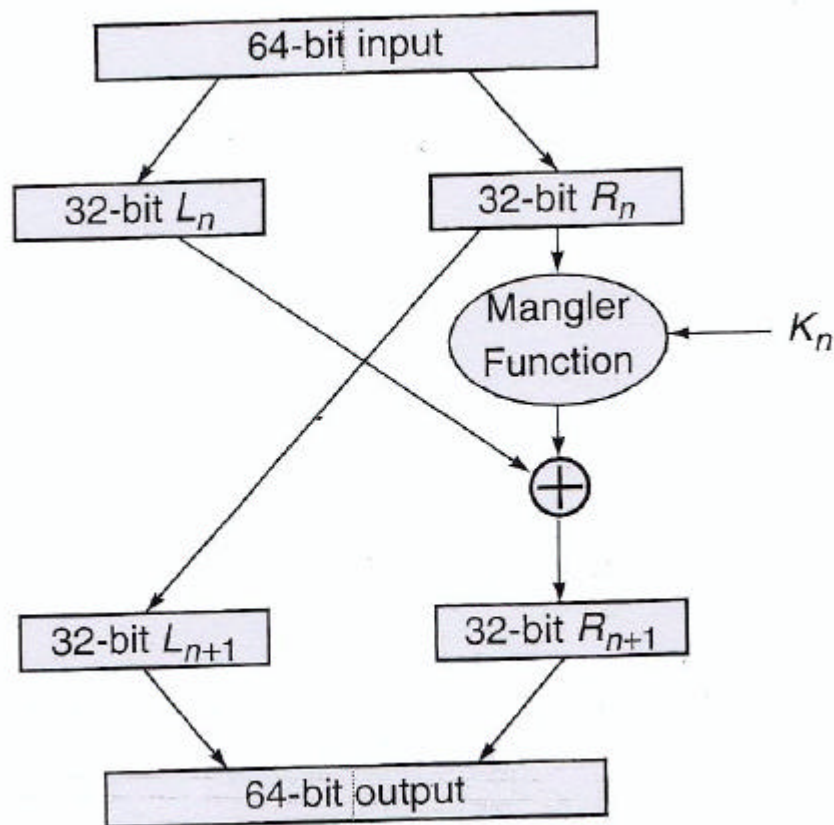
# DES per-round keys



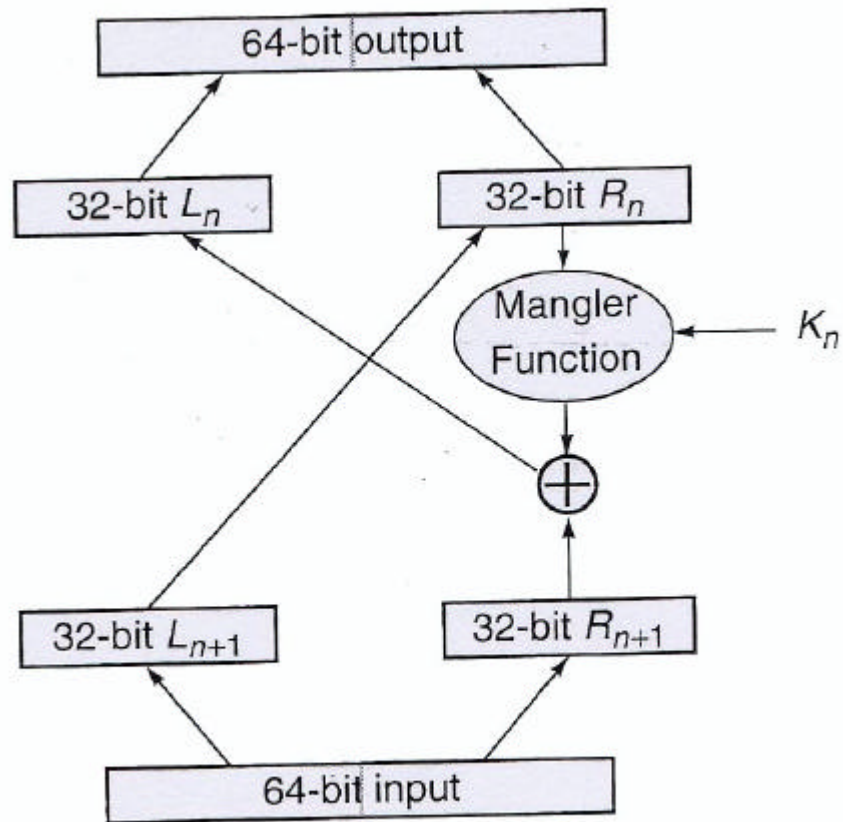
**Figure 3-5.** Round  $i$  for generating  $K_i$

$C_0$							$D_0$						
57	49	41	33	25	17	9	63	55	47	39	31	23	15
1	58	50	42	34	26	18	7	62	54	46	38	30	22
10	2	59	51	43	35	27	14	6	61	53	45	37	29
19	11	3	60	52	44	36	21	13	5	28	20	12	4

# DES round



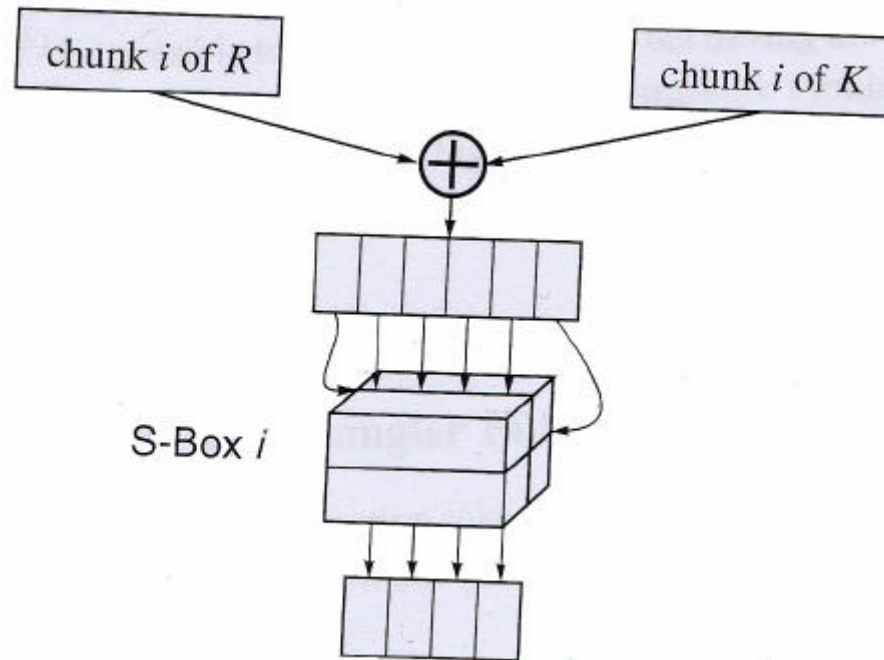
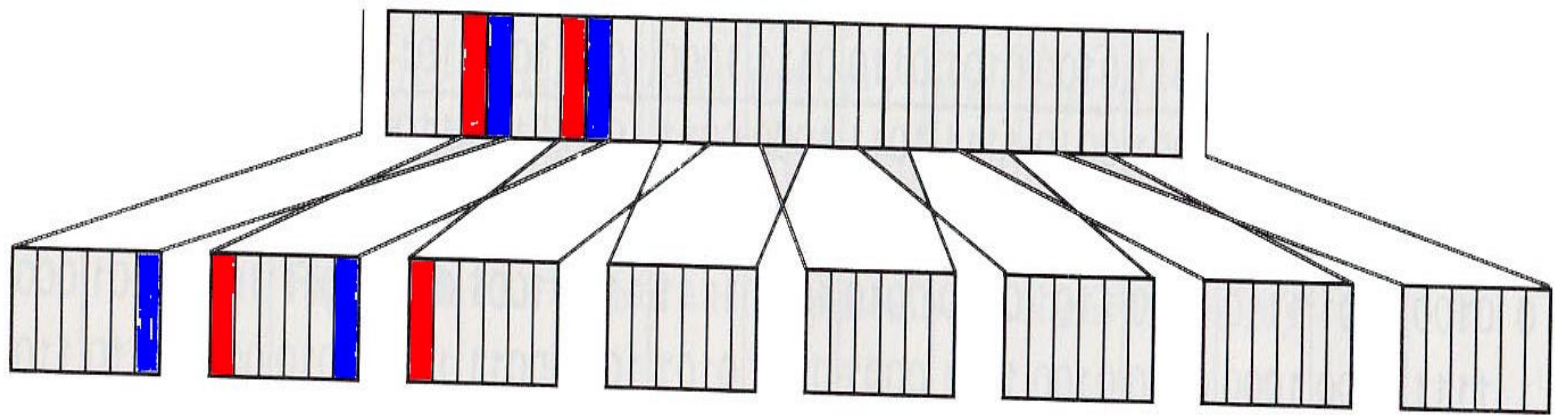
Encryption



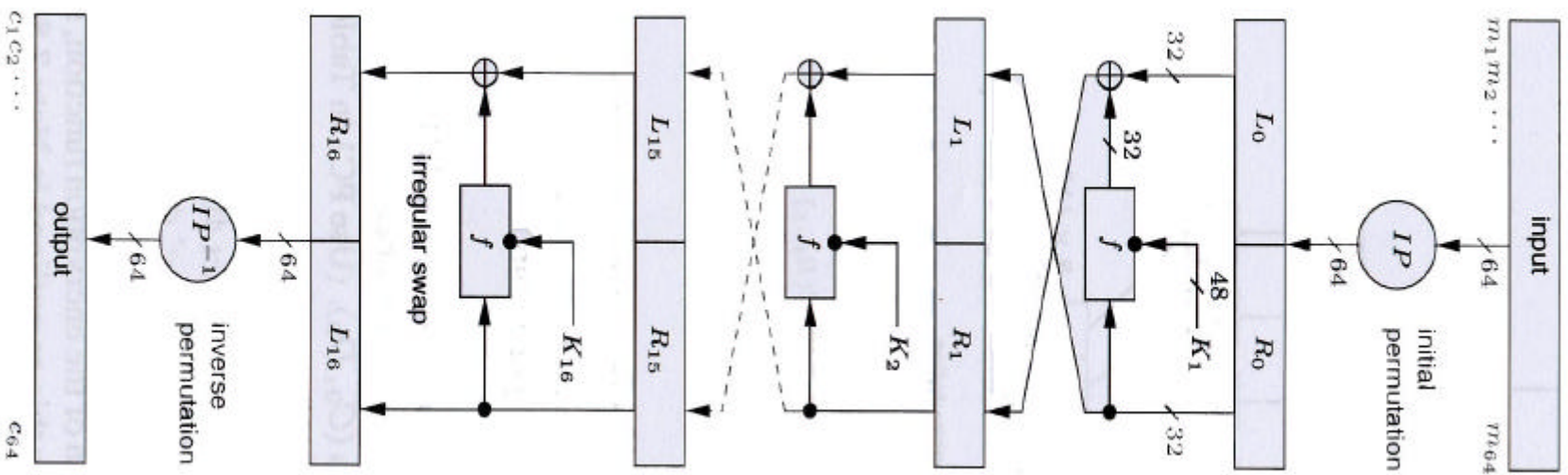
Decryption

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

# DES round



# DES

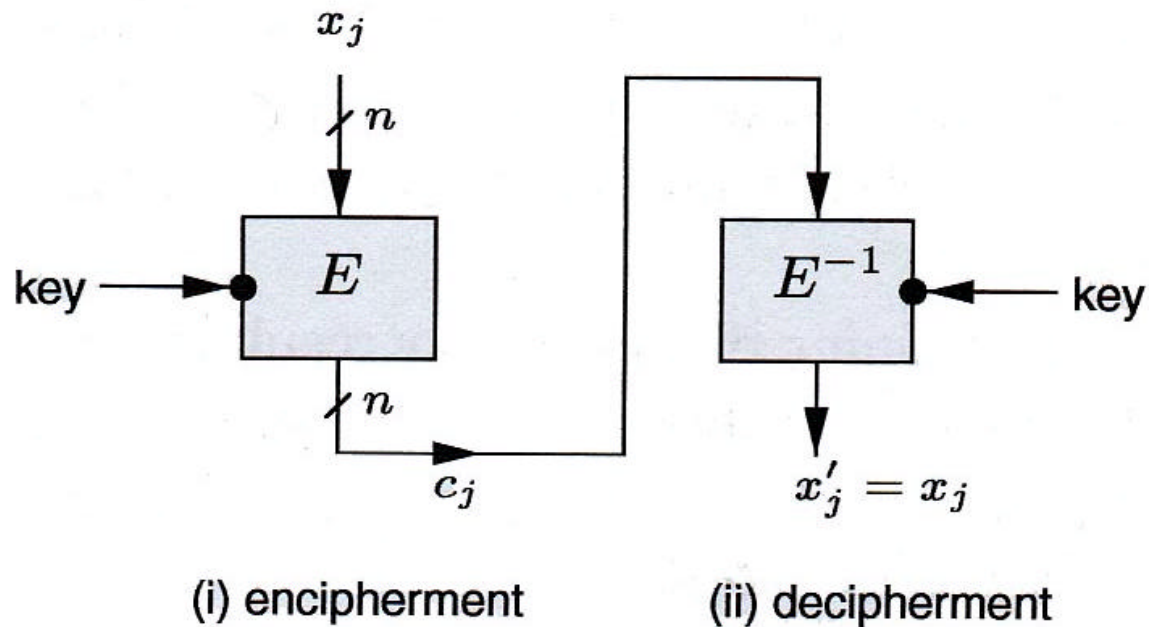


# Modes of Operation

- Electronic Codebook *ECB*
- Cipher-block Chaining *CBC*
- Cipher feedback *CFB*
- Output feedback *OFB*
  - Counter mode

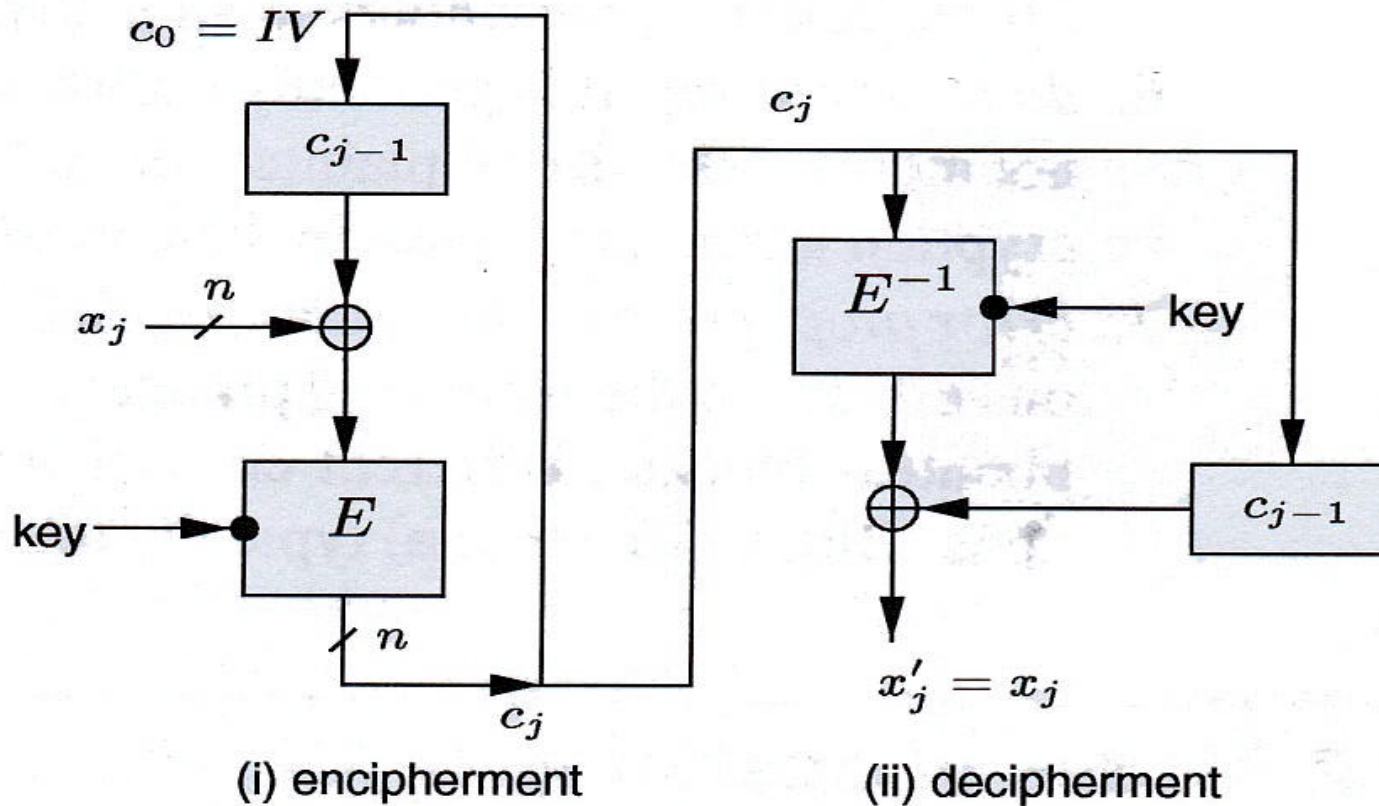
# ECB

## a) Electronic Codebook (ECB)



# CBC

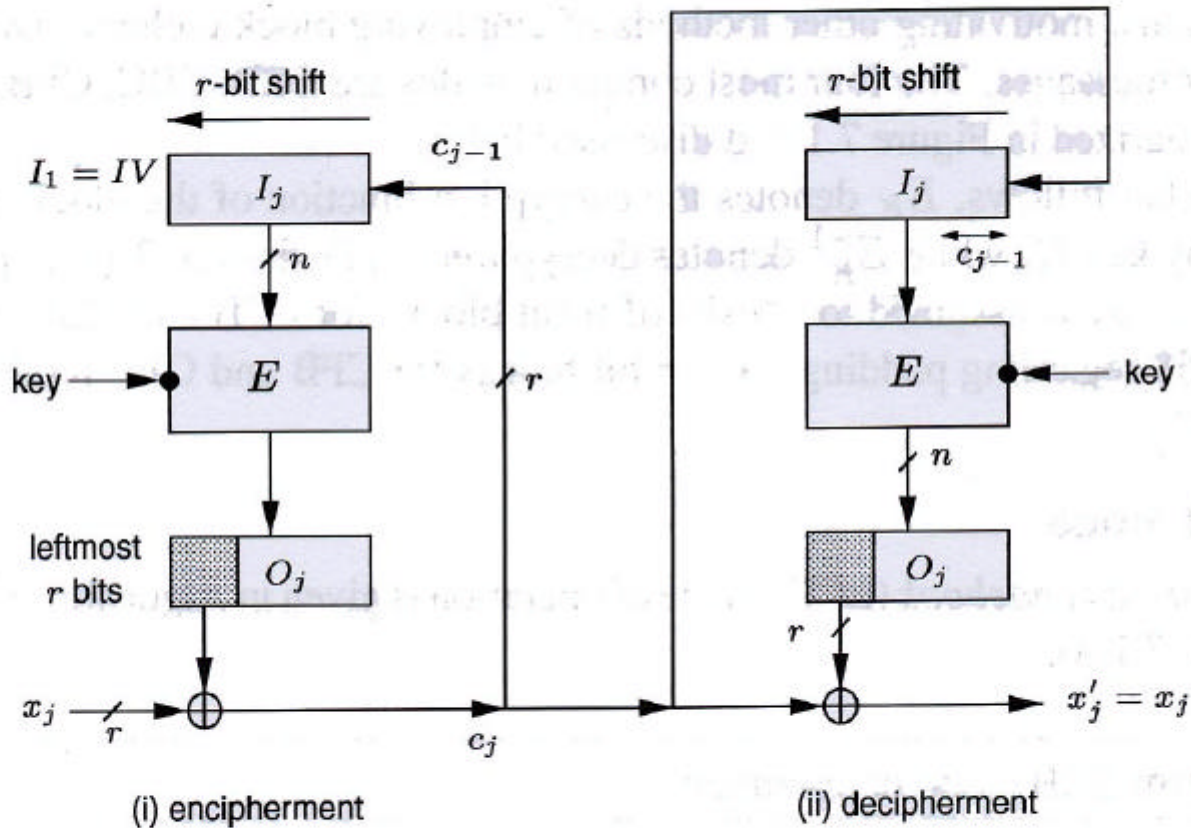
## b) Cipher-block Chaining (CBC)





# CFB

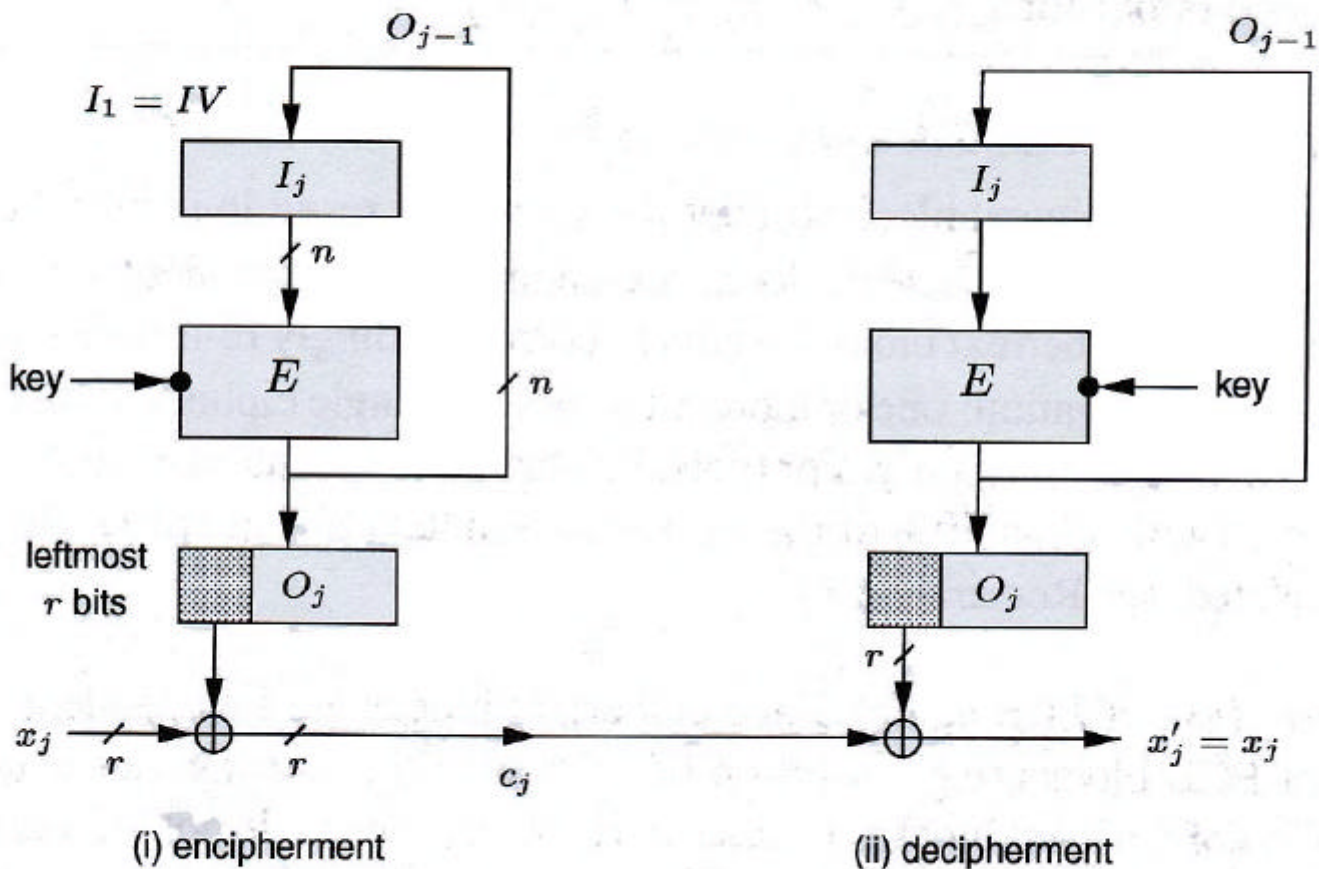
c) Cipher feedback (CFB),  $r$ -bit characters/ $r$ -bit feedback





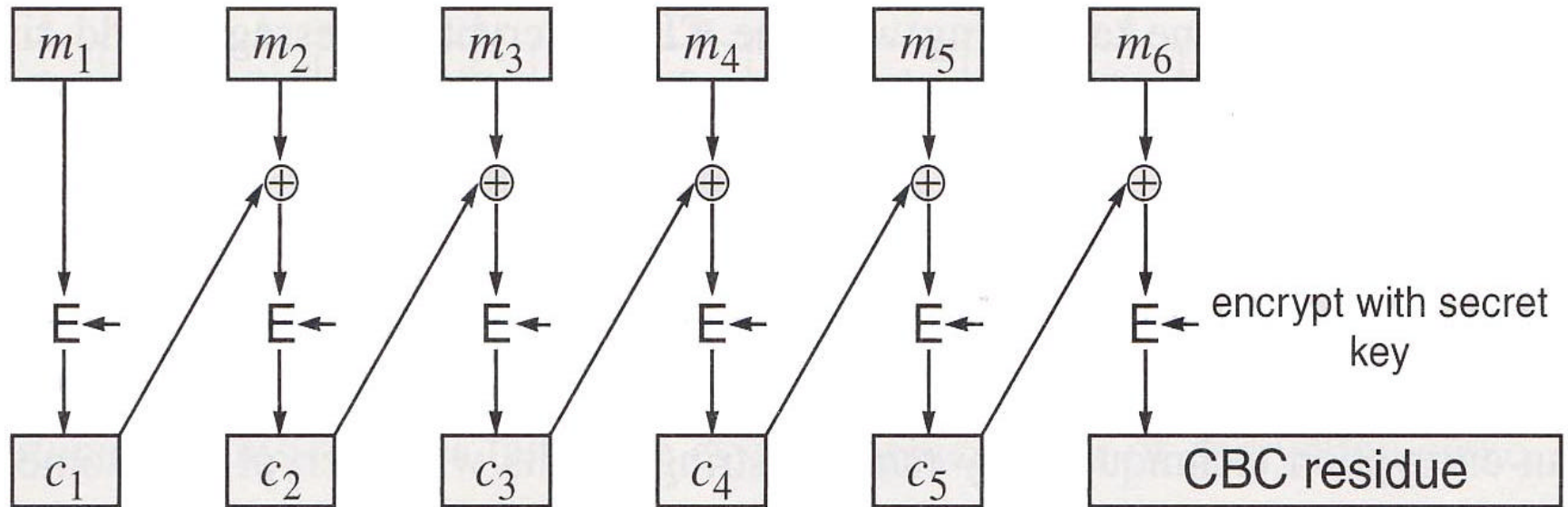
# OFB

d) Output feedback (OFB),  $r$ -bit characters/ $n$ -bit feedback



# MAC: Message Authentication Code

- DES CBC

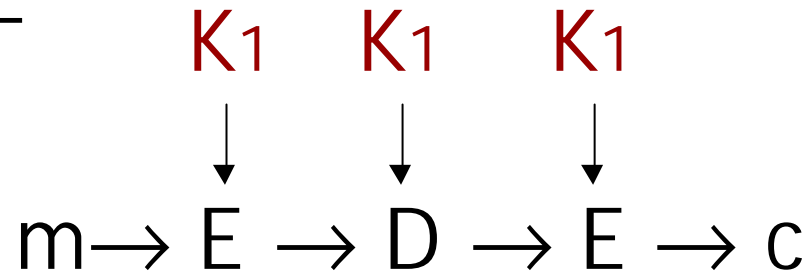


**Figure 4-11.** Cipher Block Chaining Residue

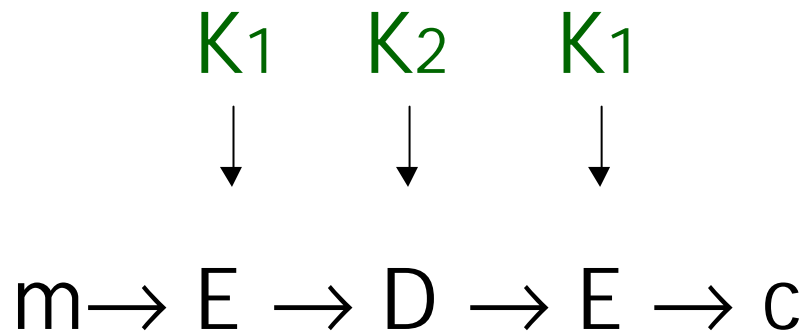
# Multiple encryption

- 3DES EDE

**56 bits**



**112 bits**



# Stream ciphers

- One time pad (OTP)

Perfect secrecy but no integrity



```

typedef unsigned char uns8;
typedef unsigned short uns16;

static uns8 state[256], x, y; /* 258 octets of state information */

void
rc4init (key, length) /* initialize for encryption / decryption */
    uns8 *key;
    uns16 length;
{
    int i;
    uns8 t;
    uns8 j;
    uns8 k = 0;

    for (i = 256; i--; )
        state[i] = i;

    for (i = 0, j = 0; i < 256; i++, j = (j + 1) % length)
        t = state[i], state[i] = state[k += key[j] + t], state[k] = t;

    x = 0;
    y = 0;
}

uns8
rc4step () /* return next pseudo-random octet */
{
    uns8 t;

    t = state[y += state[+x]], state[y] = state[x], state[x] = t;
    return (state[state[x] + state[y]]);
}

```