CS577: Introduction to Blockchain and Cryptocurrency

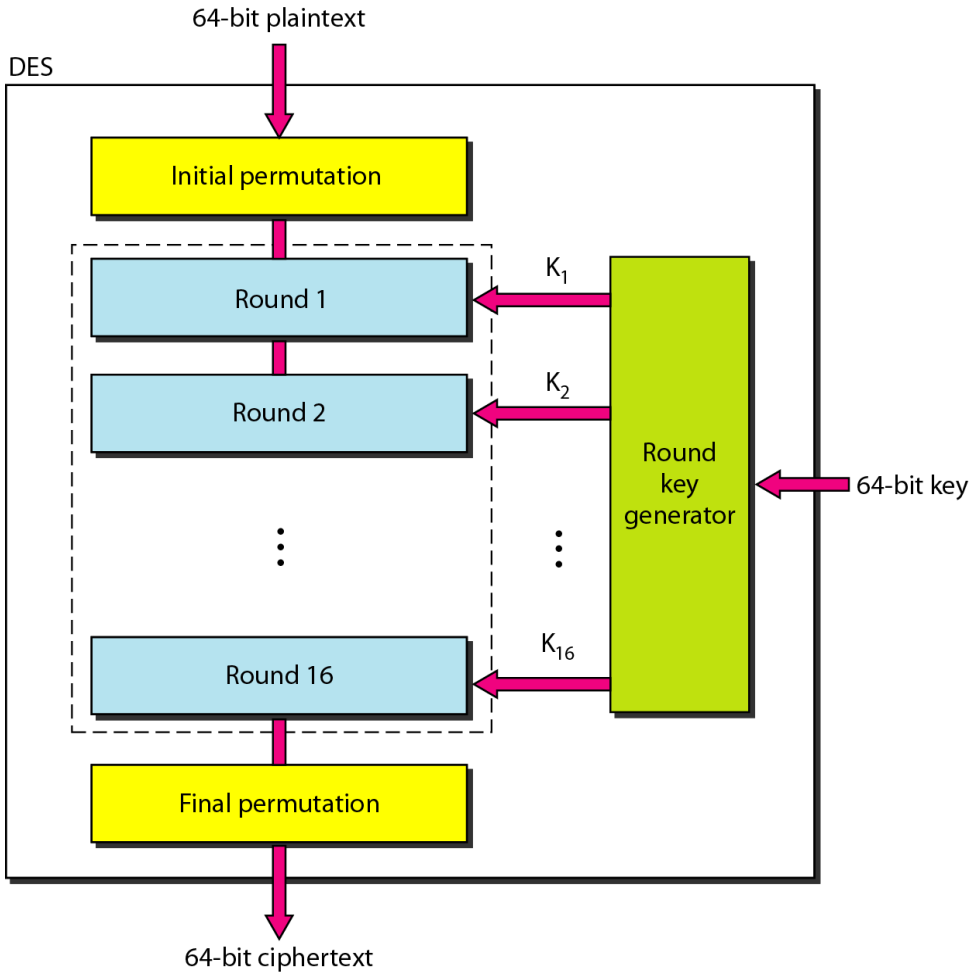
Symmetric Cryptography

Dr. Raju Halder

Block vs Stream Ciphers

- Stream ciphers process messages a bit or byte at a time when en/decrypting.
- Block ciphers process messages in into blocks, each of which is then en/decrypted.
  - Like a substitution on very big characters: 64-bits or more
- Many current ciphers are block ciphers, one of the most widely used types of cryptographic algorithms

DES (Data Encryption Standard)



DES (Data Encryption Standard)

The Initial Permutation (IP)

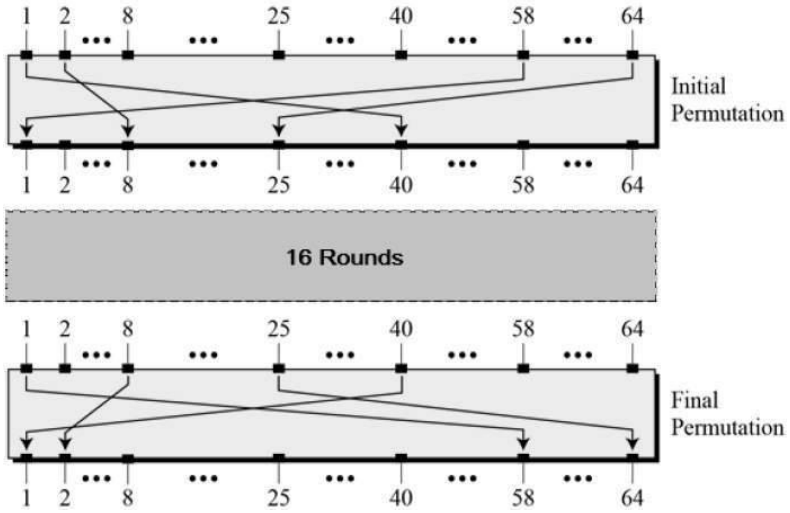
The following tables describe for each output bit the number of the input bit whose value enters to the output bit. For example, in IP, the 58'th bit in the input becomes the first bit of the output.

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

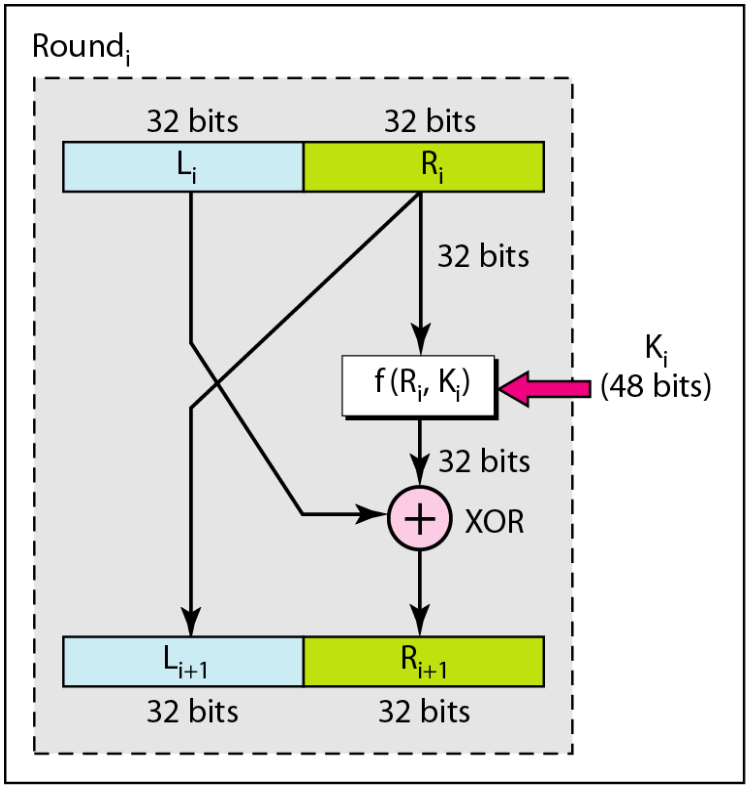
FP=IP^{-1}:

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

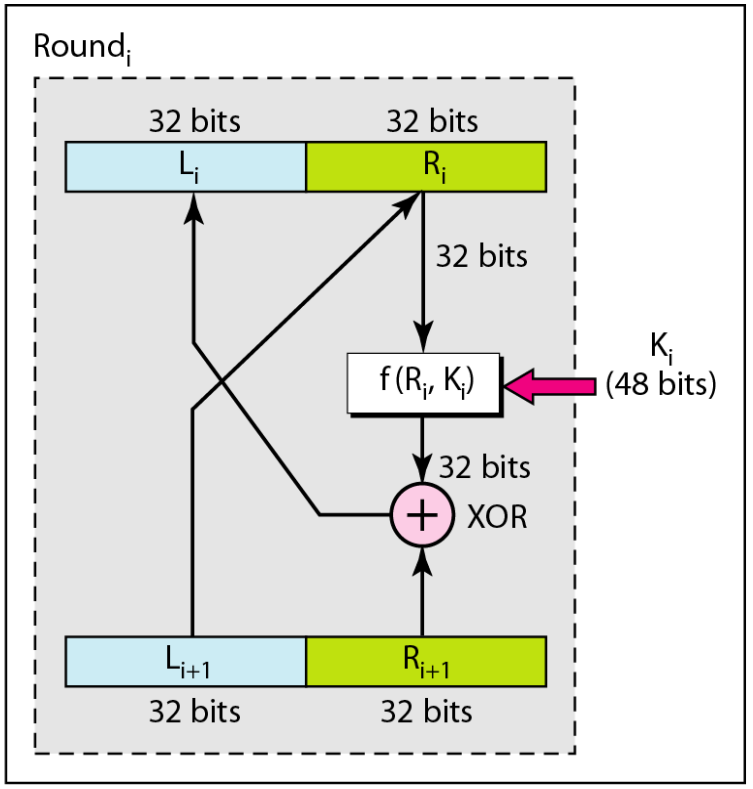


DES (Data Encryption Standard)

One round in DES ciphers

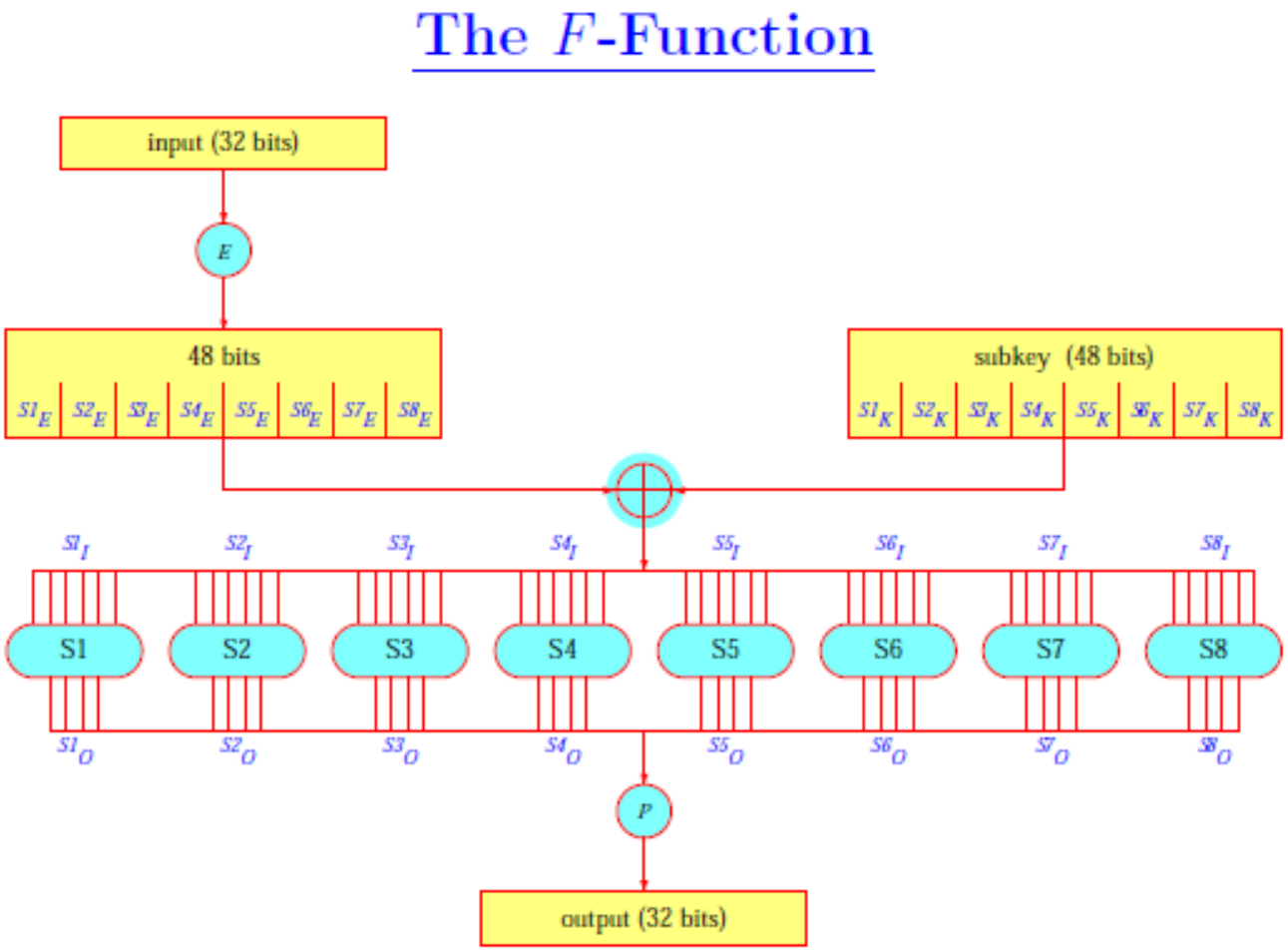


a. Encryption round



b. Decryption round

DES (Data Encryption Standard)



DES (Data Encryption Standard)

The P Permutation and the E Expansion

P Permutes the order of 32 bits. E Expands 32 bits to 48 bits by duplicating 16 bits twice.

P:

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

E:

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

DES (Data Encryption Standard)

The S Boxes

S box 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

S box 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

DES (Data Encryption Standard)

The S Boxes (cont.)

S box 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

S box 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

DES (Data Encryption Standard)

The S Boxes (cont.)

S box 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

S box 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

DES (Data Encryption Standard)

The S Boxes (cont.)

S box 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

S box 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

DES (Data Encryption Standard)

The S Boxes (cont.)

How to interpret the S boxes:

The representation of the S boxes use the first and sixth bits of the input as a line index (between 0 and 3), and the four middle bits as the row index (between 0 and 15).

Thus, the input values which correspond to the standard description of the S boxes are

0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62
33	35	37	39	41	43	45	47	49	51	53	55	57	59	61	63

DES (Data Encryption Standard)

The S Boxes (cont.)

Note that all the operations are linear, except for the S boxes. Thus, the strength of DES crucially depends on the choice of the S boxes.

If the S boxes would be affine, the cipher becomes affine, and thus easily breakable.

The S boxes were chosen with some criteria to prevent attacks.

DES (Key Scheduling)

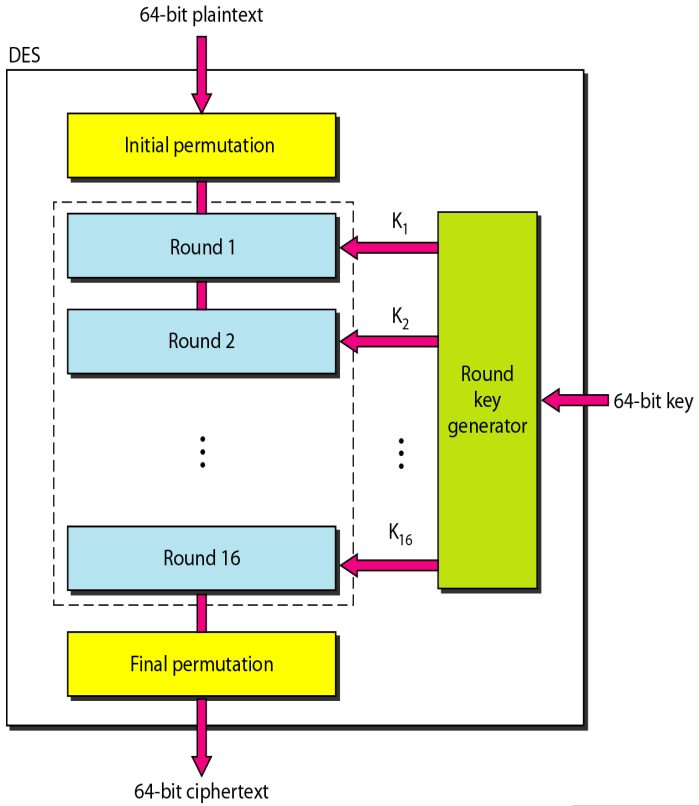


Table 3.4 DES Key Schedule Calculation

(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

(b) 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

(c) Permuted Choice Two (PC-2)

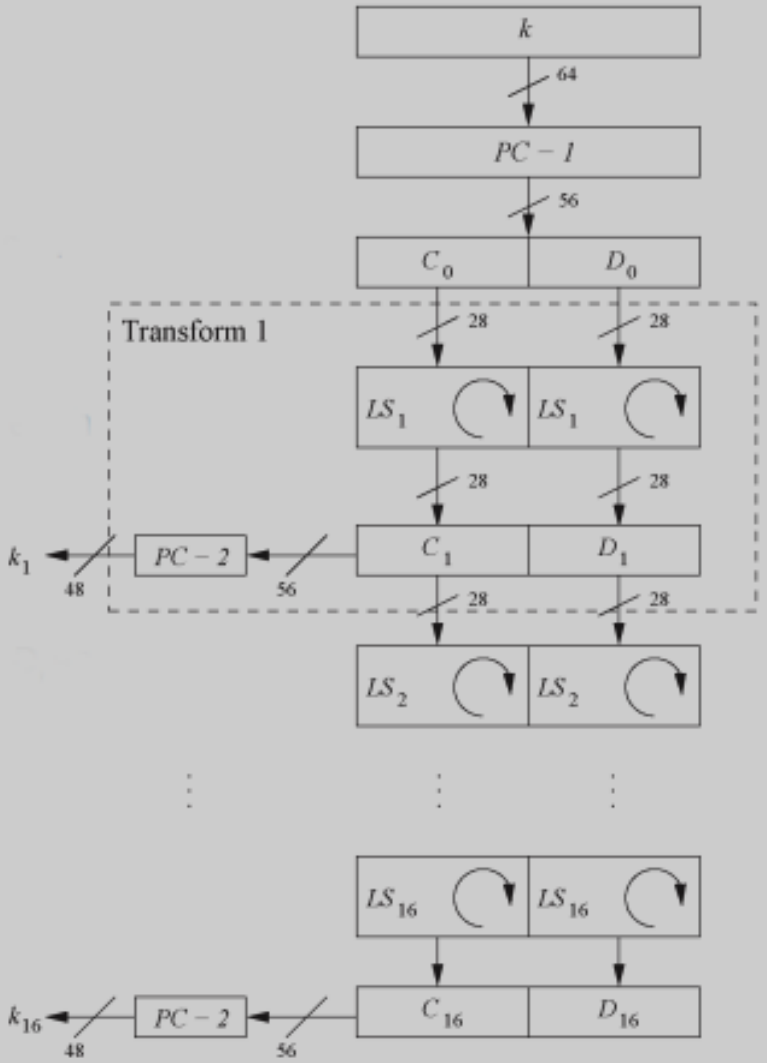
14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

(d) 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

DES (Key Scheduling)

PC – 2							
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 (Data Encryption Standard)

Decryption

Decryption is done by the same algorithm as encryption, except that the order of the subkeys is reversed (i.e., K16 is used instead of K1, K15 instead of K2, . . . , and K1 instead of K16.).

Strength of DES – Key Size

- 56-bit keys have $2^{56} = 7.2 \times 10^{16}$ values
- Brute force search looks hard
- Recent advances have shown is possible
  - in 1997 on a huge cluster of computers over the Internet in a few months
  - in 1998 on dedicated hardware called “DES cracker” by Electronic Frontier Foundation (EFF) in a few days ($220,000)
  - in 1999 above combined in 22hrs!

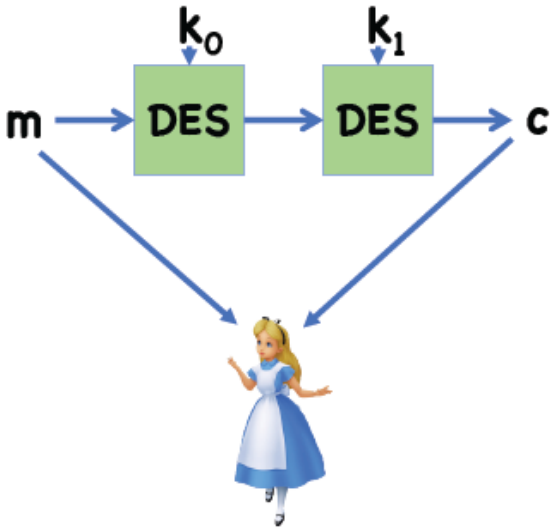
DES Replacement

- Double-DES (2DES): Man-in-the-middle attack.

Meet In The Middle Attacks

For 2DES, can actually find key in 2^{56} time

- Also $\approx 2^{56}$ space



DES Replacement

Meet In The Middle Attacks

k_0	$d = DES(k_0,m)$
0	52
1	93
2	03
3	96
4	20
5	49
…	…

k_1	$d = DES^{-1}(k_1,m)$
0	69
1	10
2	86
3	49
4	99
5	08
…	…

On 2DES, roughly same time complexity as brute force on DES

DES Replacement

- Triple-DES (3DES)
  - 168-bit key, no brute force attacks
  - Underlying encryption algorithm the same, no effective analytic attacks
  - Drawbacks
    - Performance: no efficient software codes for DES/3DES
    - Efficiency/security: bigger block size desirable

Triple-DES

Triple-DES is an improvement to DES which use the same DES hardware/ software but encrypt the plaintext three times.

Triple DES has two variants:

1. **Three-key triple-DES**: the plaintext is encrypted three times under three different DES keys K_1, K_2, and K_3.

$$C = \mathrm{DES}_{K_3}(\mathrm{DES}^{-1}_{K_2}(\mathrm{DES}_{K_1}(P))).$$

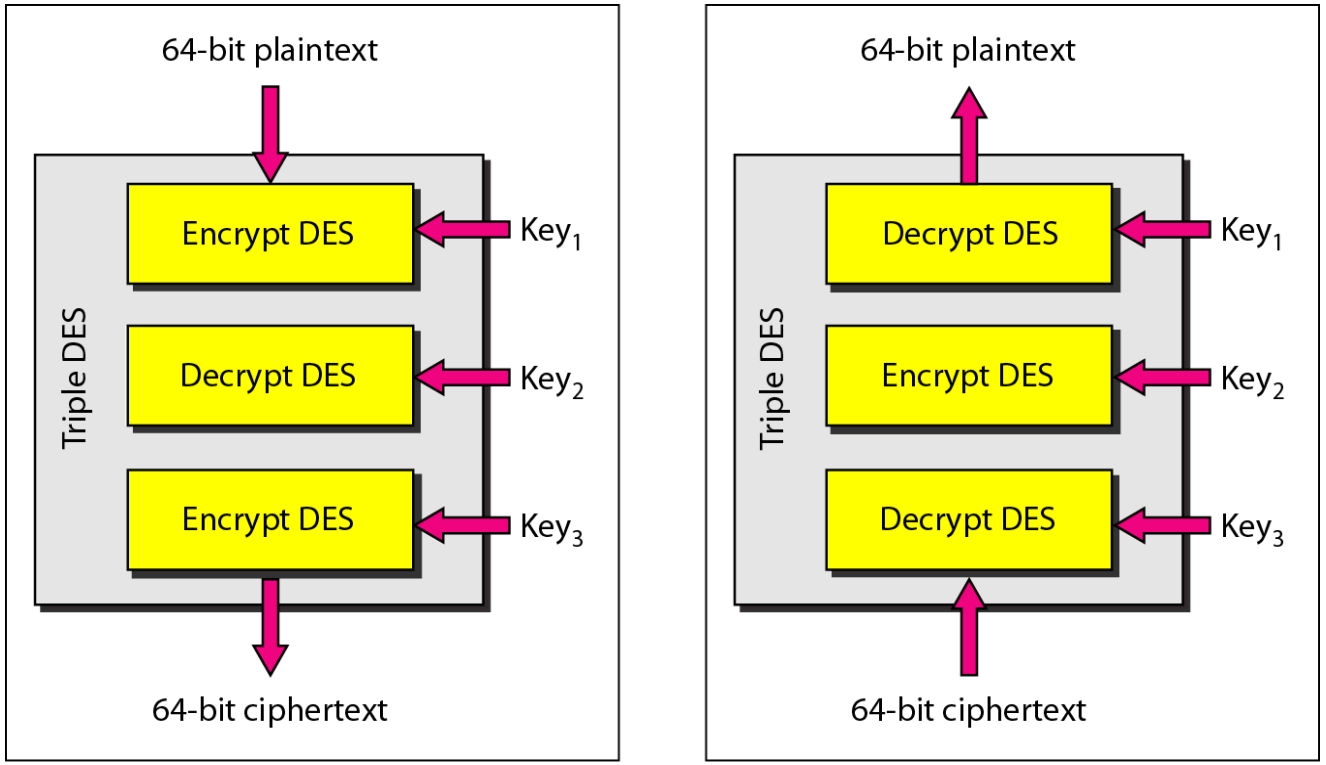
   The total key length is $3 \cdot 56 = 168$ bits.

2. **Two-key triple-DES**: the plaintext is encrypted three times under two different DES keys K_1, and K_2, where K_1 is used in the first and third application of DES, and K_2 in the second application.

$$C = \mathrm{DES}_{K_1}(\mathrm{DES}^{-1}_{K_2}(\mathrm{DES}_{K_1}(P))).$$

   The total key length is $2 \cdot 56 = 112$ bits.

Triple-DES



a. Encryption Triple DES

b. Decryption Triple DES

Triple-DES

Note that the second application of DES performs decryption. This is done to allow compatibility to older systems which use DES: if the two or three keys are all equal, then the triple encryption actually performs a single encryption with that key.

Speed:

Triple-DES is about three times slower than DES. (It is slightly faster than a third of the speed of DES as the initial and final permutation in the borders between the first/second and the second/third DES applications can be eliminated).

Status:

Triple-DES replaced DES as the de-facto standard a few years ago. AES is now the standard for new applications, while Triple-DES remains in many old applications.

AES (Advanced Data Encryption Standard)

- Advanced Encryption Standards (AES)
  - US NIST issued call for ciphers in 1997
  - Rijndael was selected as the AES in Oct-2000
- Private key symmetric block cipher
- Stronger & faster than Triple-DES
- In AES, all operations are performed on 8-bit bytes. In particular, the arithmetic operations of addition, multiplication, and division are performed over the finite field GF(2^8).

AES (Advanced Data Encryption Standard)

Note

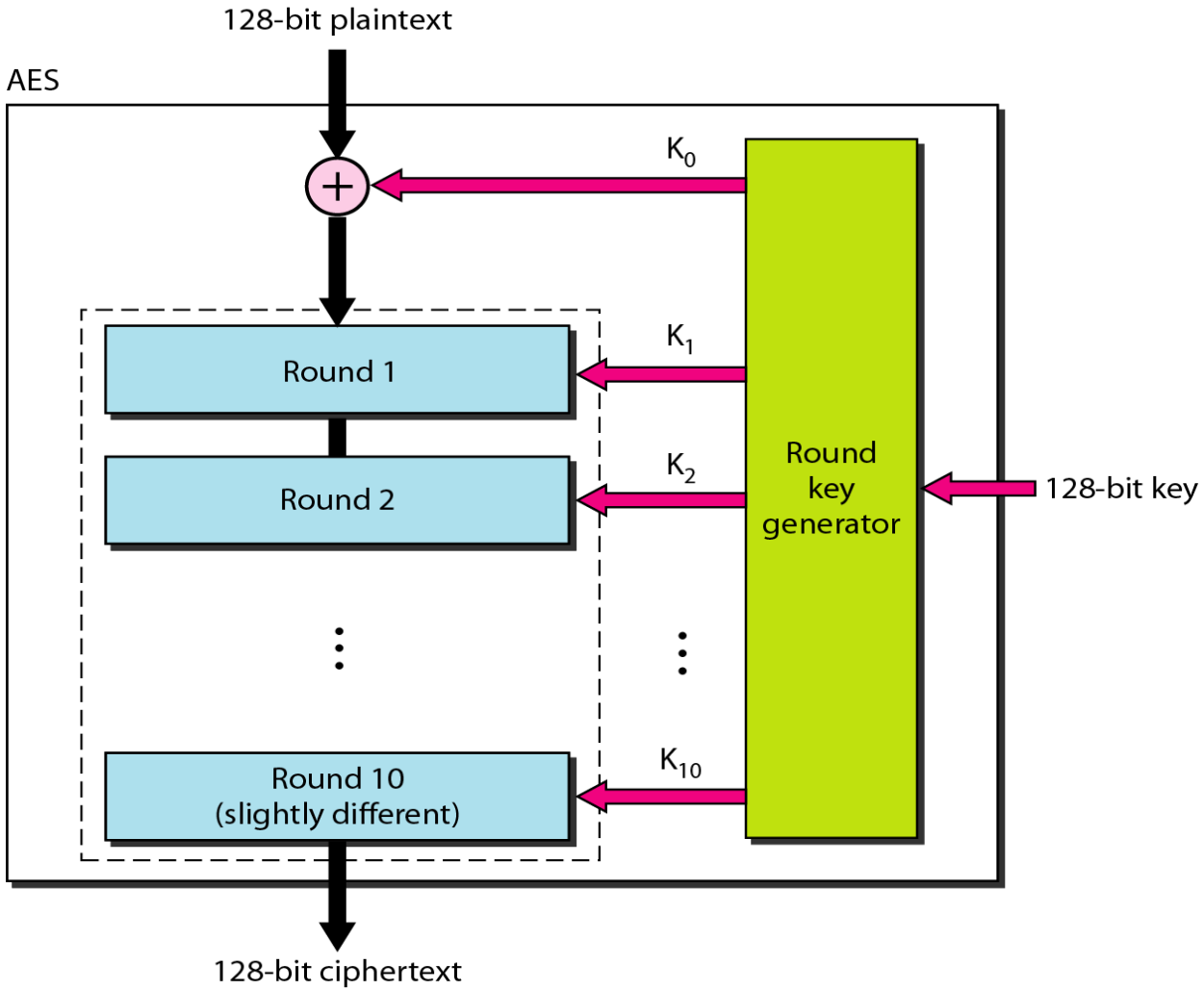
AES has three different configurations with respect to the number of rounds and key size.

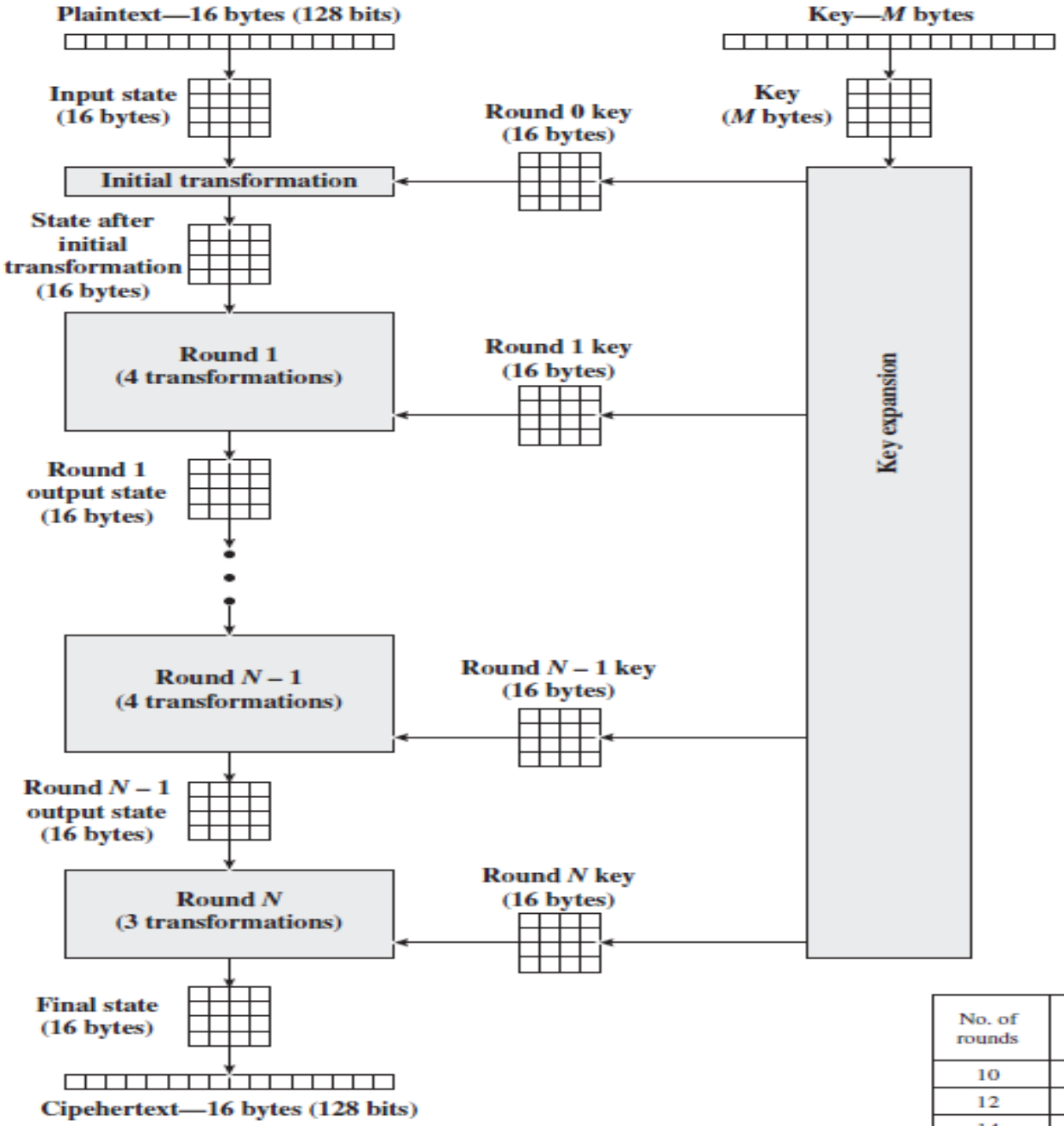
AES (Advanced Data Encryption Standard)

AES configuration

Size of Data Block	*Number of Rounds*	*Key Size*
128 bits	10	128 bits
	12	192 bits
	14	256 bits

AES (Advanced Data Encryption Standard)



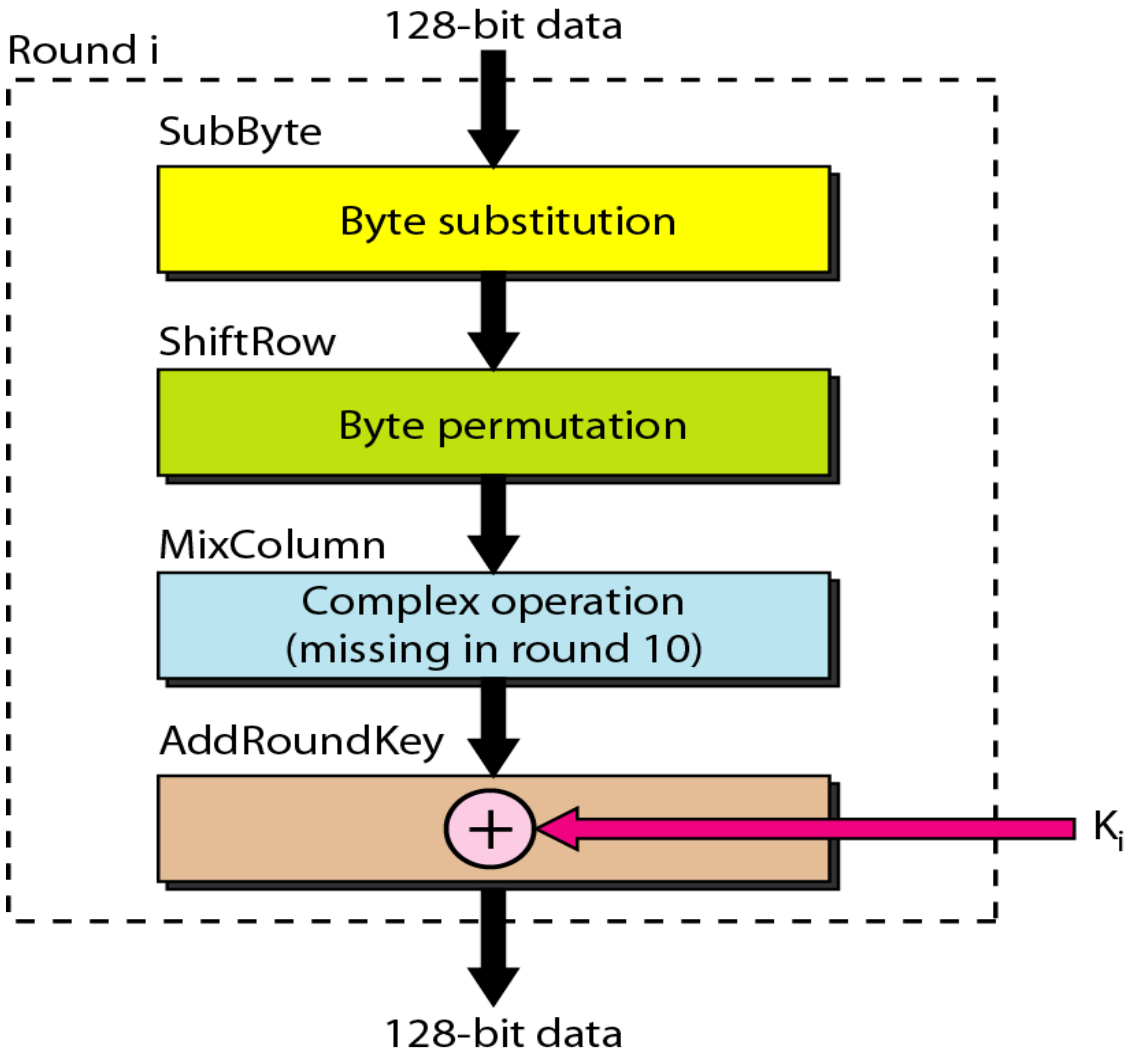


No. of rounds	Key Length (bytes)
10	16
12	24
14	32

Figure 5.1 AES Encryption Process

AES (Advanced Data Encryption Standard)

Structure of each round



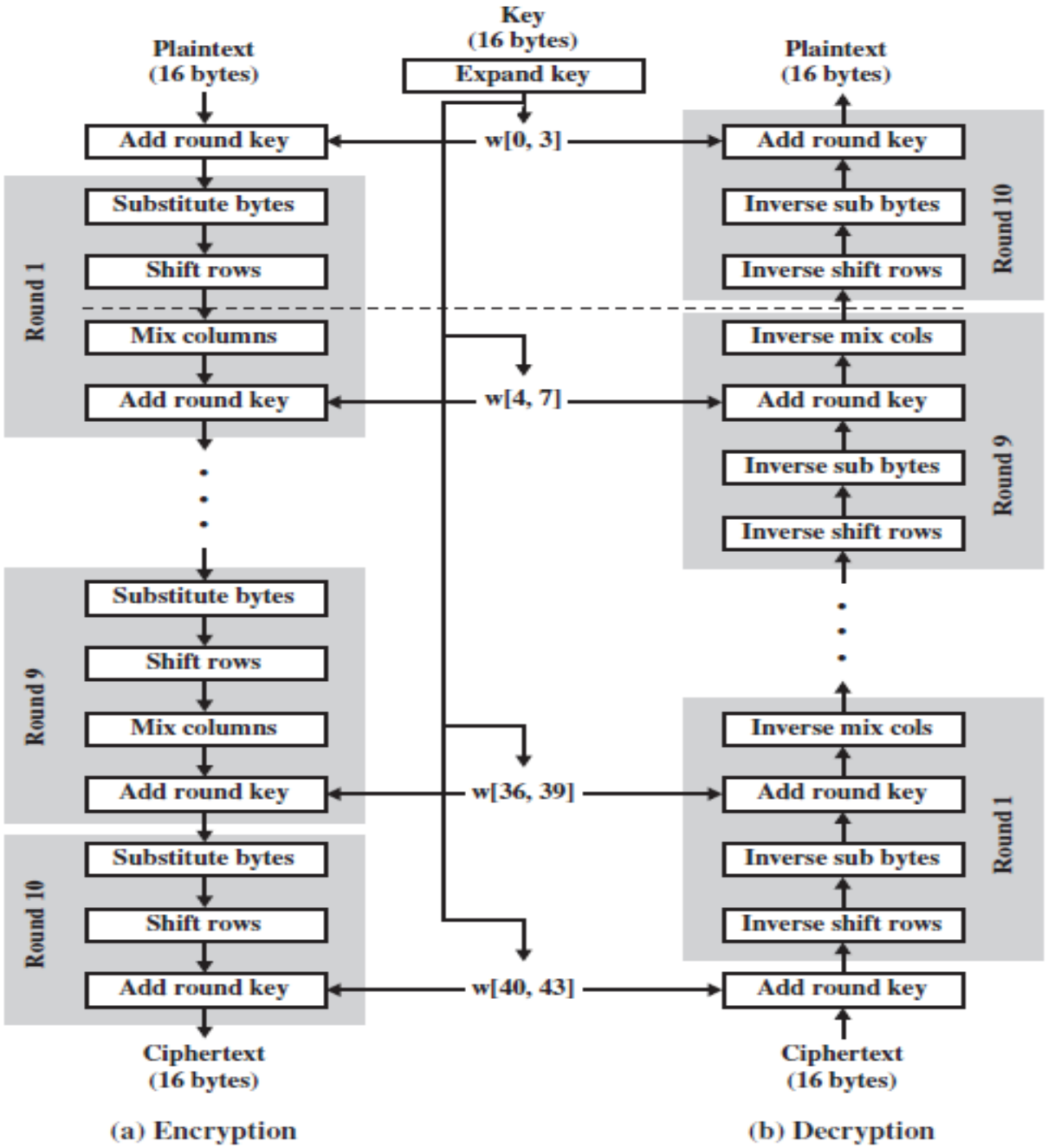


Figure 5.3 AES Encryption and Decryption

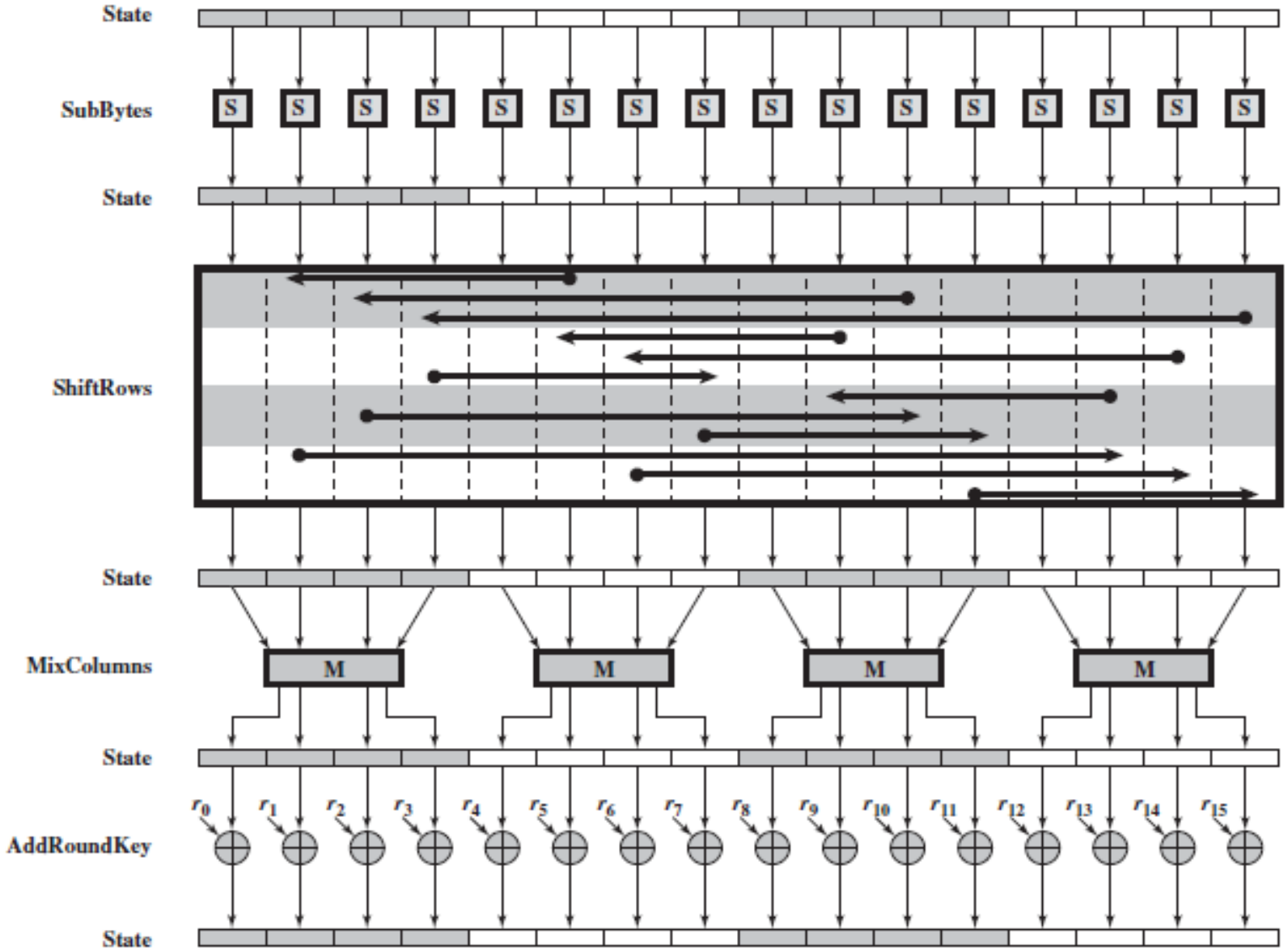
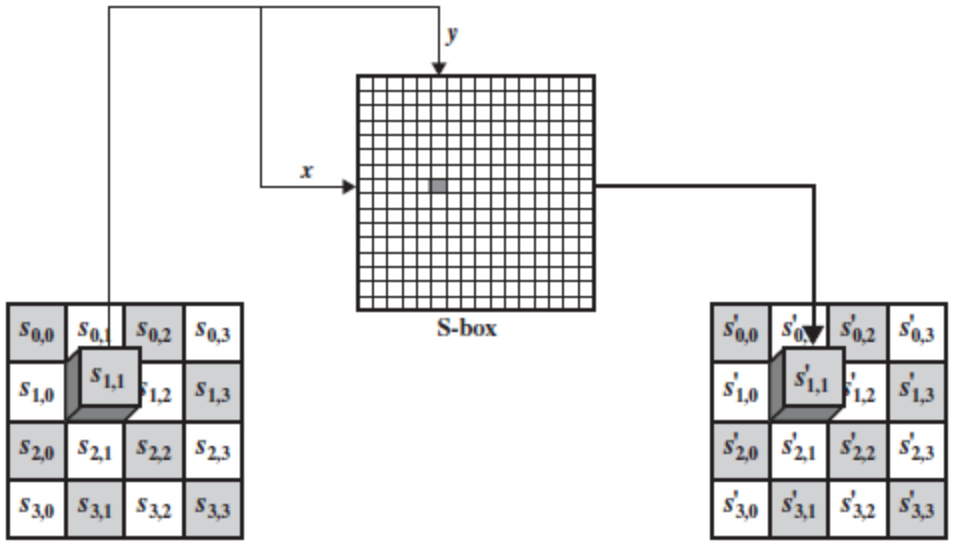
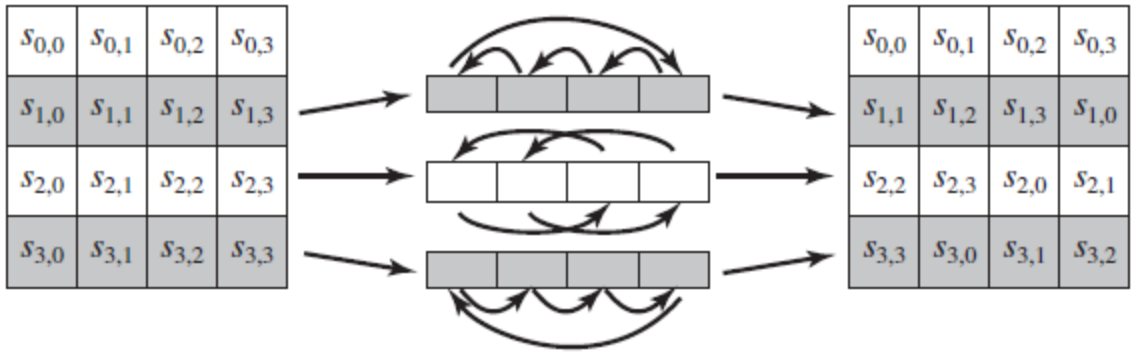


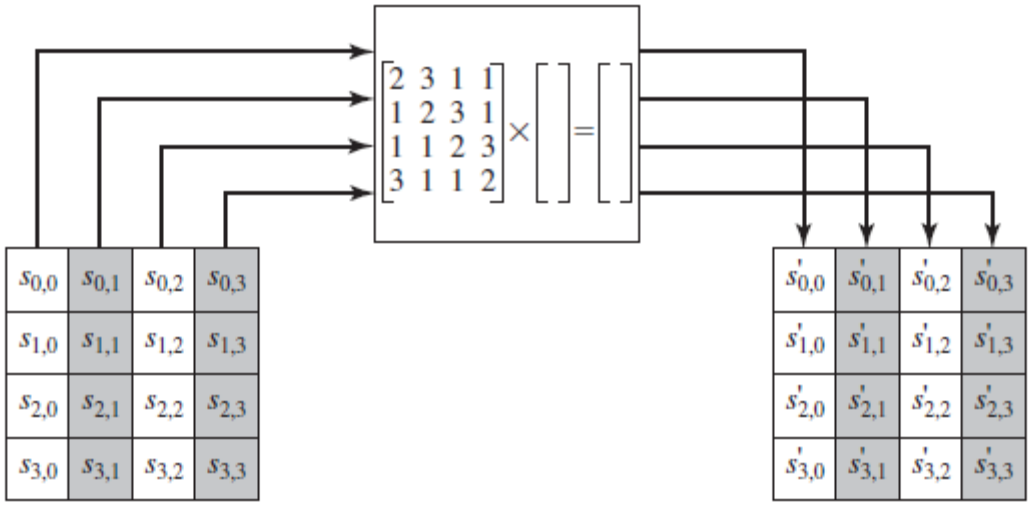
Figure 5.4 AES Encryption Round



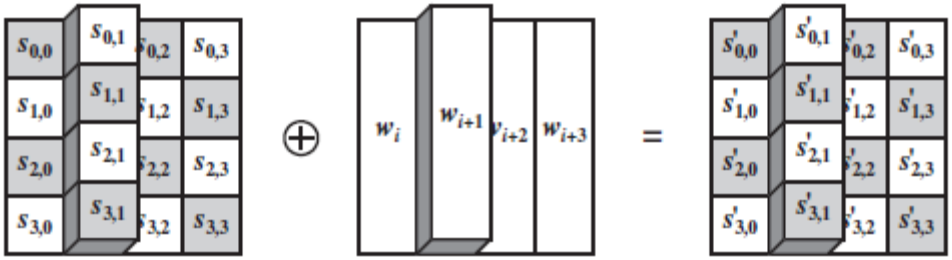
(a) Substitute byte transformation



(a) Shift row transformation



(b) Mix column transformation



(b) Add round key transformation

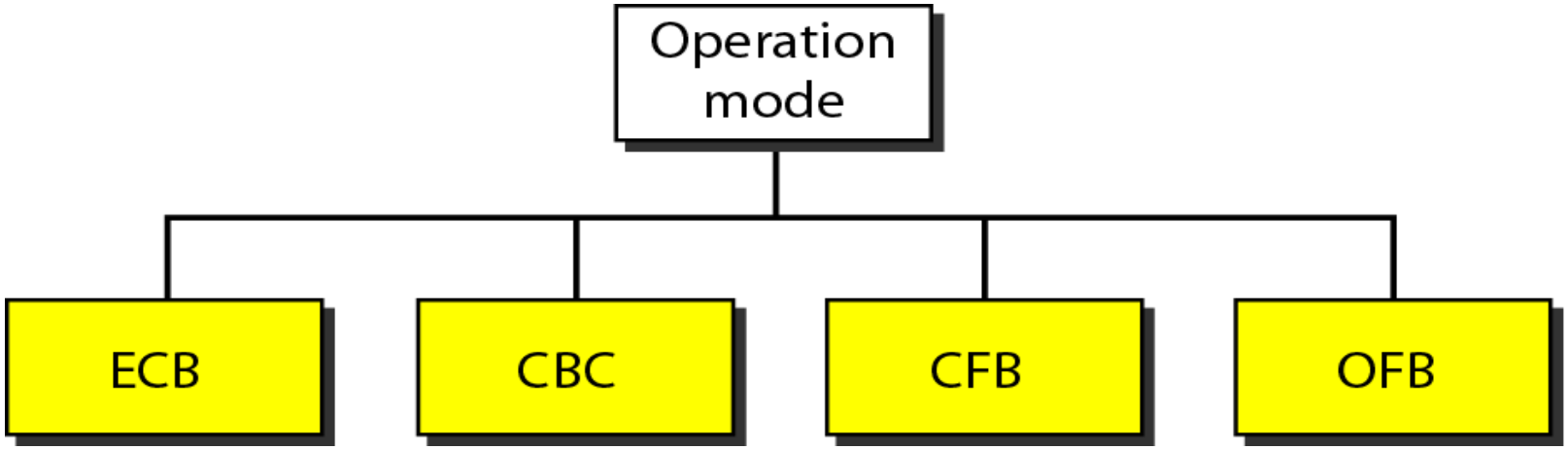
Figure 5.5 AES Byte-Level Operations

Modes

Modes of Operation

Long messages of several blocks are encrypted using one of the **modes of operation**. In the modes of operation, the messages M are divided into N-bit blocks $M_1 M_2 \dots M_n$, each block M_i is encrypted (as defined by the mode of operation) to C_i, and the results are concatenated into the ciphertext $C = C_1 C_2 \dots C_n$.

Many modes of operation actually transform the block ciphers into stream ciphers, by adding memory (external to the block cipher).



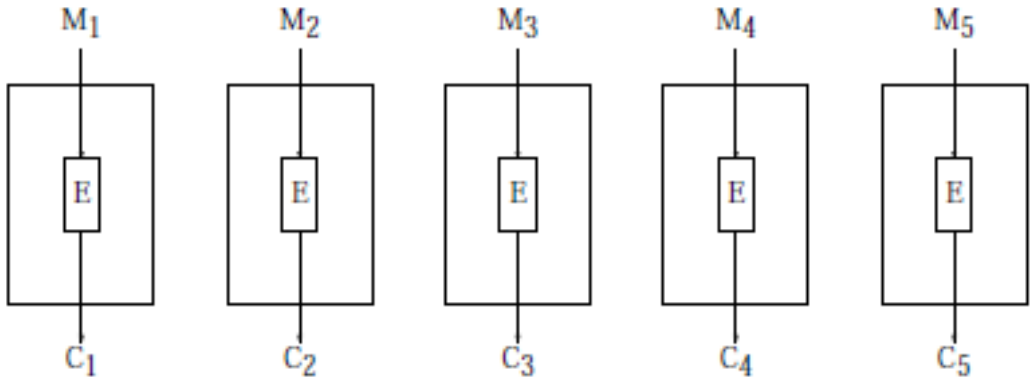
Electronic Code Book (ECB) Mode

In this mode, each plaintext block M_i is encrypted simply by

$$C_i = E_K(M_i).$$

Decryption is done by

$$M_i = D_K(C_i).$$



The main drawback of ECB is that $M_i = M_j$ iff $C_i = C_j$. Thus, Eve can easily identify which plaintext blocks are equal.

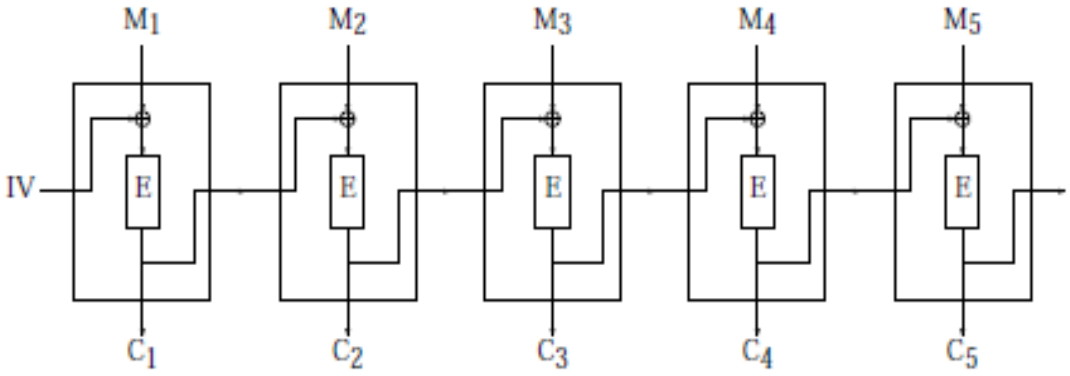
Cipher Block Chaining (CBC) Mode

Each plaintext block M_i is mixed with the previous ciphertext block before encryption:

$$C_i = E_K(M_i \oplus C_{i-1}).$$

Decryption is done by

$$M_i = D_K(C_i) \oplus C_{i-1}.$$



A (non-secret) initial value $C_0 = IV$ is chosen for each message.

Cipher Block Chaining (CBC) Mode (cont.)

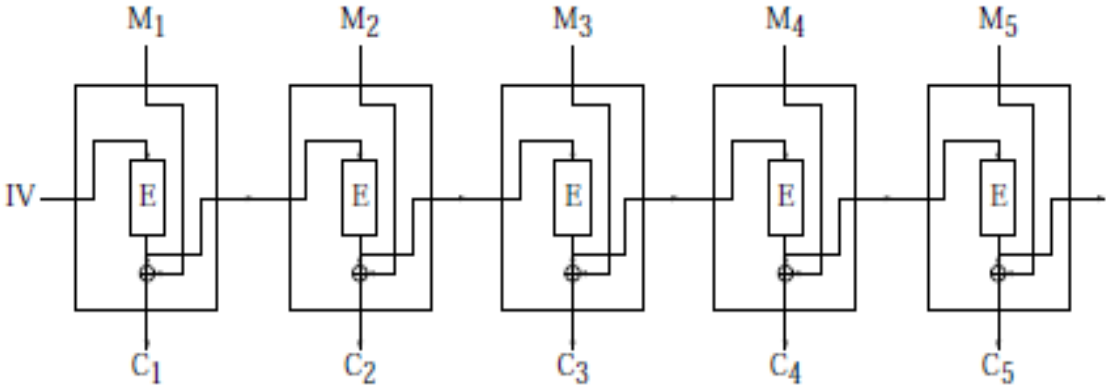
In this mode two equal message blocks are usually encrypted to different ciphertext blocks.

This mode has small error propagation: if C_i is received with errors, only M_i and M_{i+1} have errors after decryption. M_{i+2} is not affected from the error in C_i.

(64-bit) Output FeedBack (OFB) Mode

Generates a pseudo random bit stream from the key K and an initial value $V_0 = IV$ by

$$V_i = E_K(v_{i-1}).$$



Encryption is done by

$$C_i = M_i \oplus V_i.$$

Decryption is done by

$$M_i = C_i \oplus V_i.$$

(64-bit) Output FeedBack (OFB) Mode (cont.)

This mode has no error propagation (one bit error in C causes only one bit error in the message during decryption).

An advantage of this mode is that V_i can be computed in advance, before the plaintext/ciphertext is known.

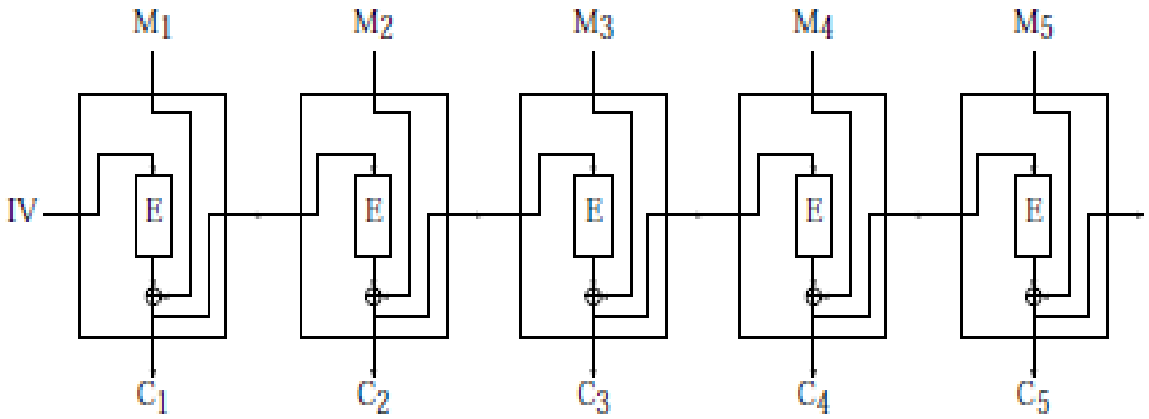
(64-bit) Cipher FeedBack (CFB) Mode

Similar to the OFB mode, but the bit stream depends on the ciphertext. Encryption is done by

$$C_i = M_i \oplus E_K(C_{i-1}).$$

Decryption is done by

$$M_i = C_i \oplus E_K(C_{i-1}).$$



Block Cipher Principles

- Most symmetric block ciphers are based on a **Feistel Cipher Structure**

Substitution-Permutation Ciphers

- Substitution-permutation (S-P) networks [Shannon, 1949]
  - modern substitution-transposition product cipher
- S-P networks are based on the two primitive cryptographic operations
  - *substitution* (S-box)
  - *permutation* (P-box)
- provide *confusion* and *diffusion* of message
- These form the basis of modern block ciphers

Confusion and Diffusion

- Cipher needs to completely obscure statistical properties of original message
- A one-time pad does this
- More practically Shannon suggested S-P networks to obtain:
- **Diffusion** – dissipates statistical structure of plaintext over bulk of ciphertext
- **Confusion** – makes relationship between ciphertext and key as complex as possible

Feistel Cipher Structure

- **Feistel cipher** implements Shannon's S-P network concept
  - based on invertible product cipher
- Process through multiple rounds which
  - partitions input block into two halves
  - perform a substitution on left data half
  - based on round function of right half & subkey
  - then have permutation swapping halves

Feistel Cipher Structure