20. Symmetric Encryption and Message Confidentiality

Prof. Seunghyun Park (sp@hansung.ac.kr)

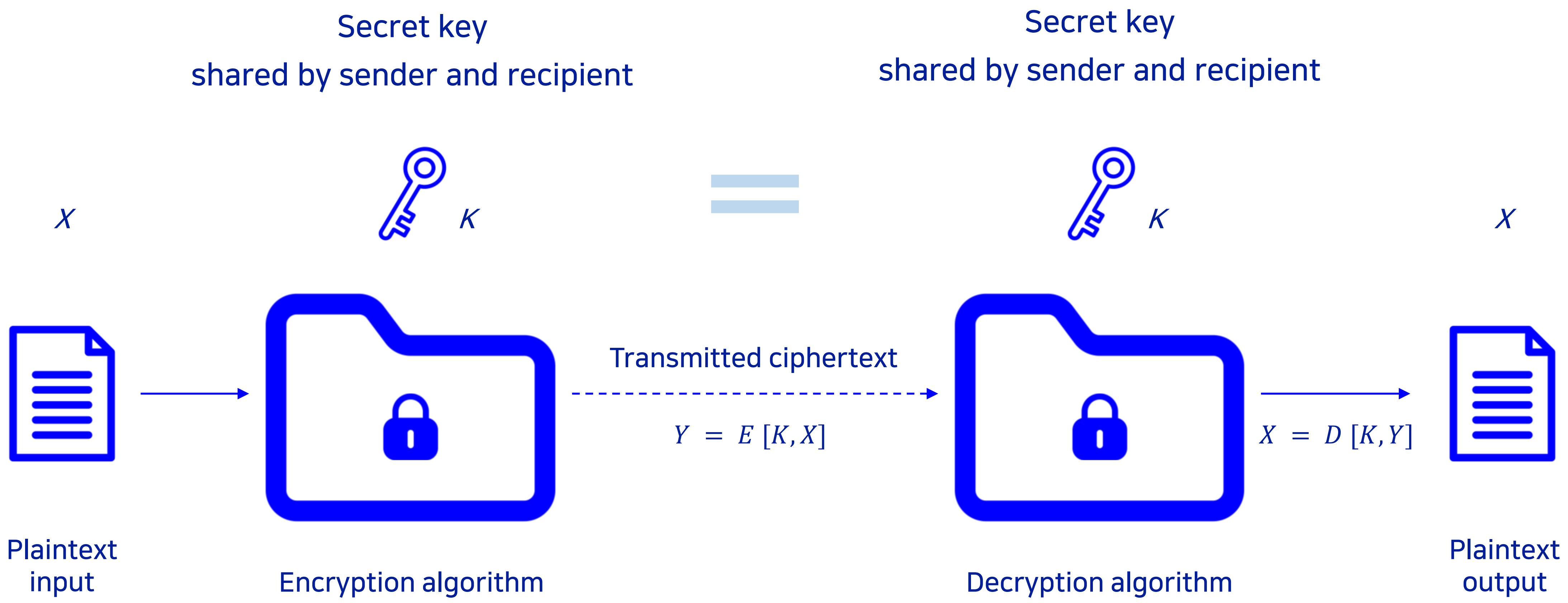
Division of Computer Engineering

한성대학교 HANSUNG UNIVERSITY

Objectives

- We are able to …
  - explain the basic principles of symmetric encryption.
  - understand the significance of the Feistel cipher structure.
  - describe the structure and function of DES.
  - distinguish between two-key and three-key triple DES.
  - describe the structure and function of AES.
  - distinguish among the major block cipher modes of operation.
  - discuss the issues involved in key distribution.

Symmetric encryption



Cryptography classified along 3 independent dimensions

- The number of keys
  - Symmetric: Sender and receiver use **same key**
  - Asymmetric: Sender and receiver each use a **different key**
- The type of operations
  - Substitution: each element in the plaintext is **mapped into another element**
  - Transposition: elements in plaintext are **rearranged**
- The way in which the plaintext is processed
  - Block cipher: processes input **one block** of elements **at a time**
  - Stream cipher: processes the input elements **continuously**

Types of attacks on encrypted messages (table 20.1)

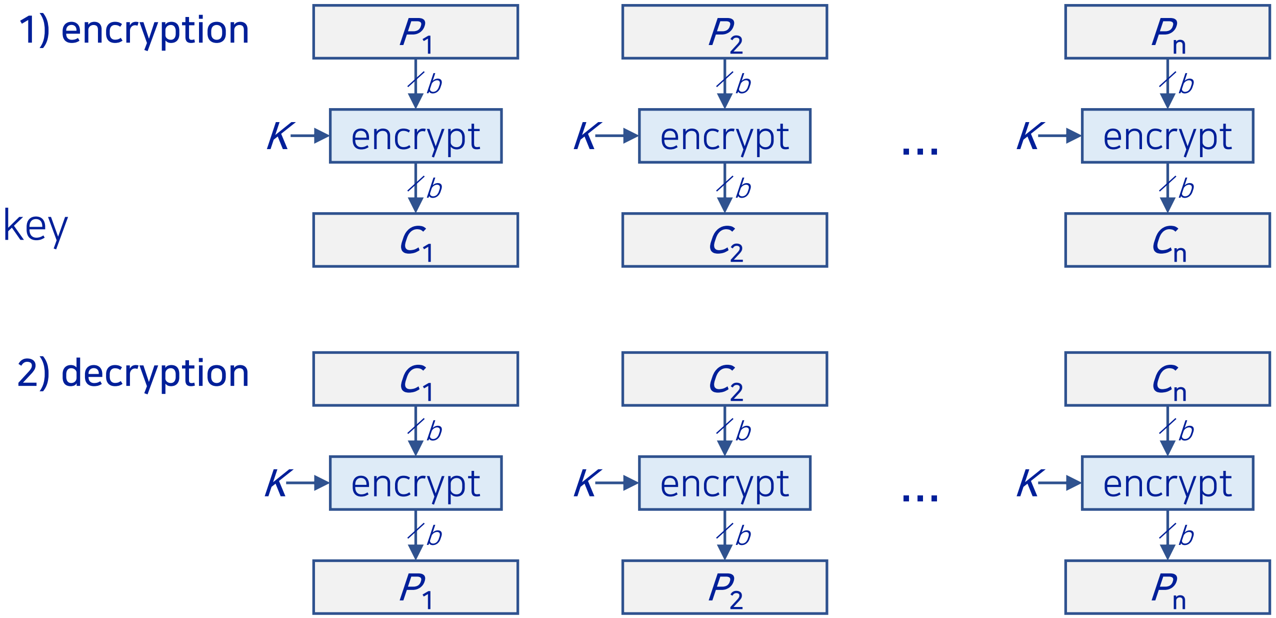
Type of attack	Known to cryptanalyst
Ciphertext only	• None ※ we assume that cryptanalyst knows encryption algorithm and ciphertext
Known plaintext	• One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	• Purported ciphertext chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen text	• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Purported ciphertext chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key

Computationally secure encryption schemes

- Encryption is computationally secure if:
  - Cost of breaking cipher exceeds value of information
  - Time required to break cipher exceeds the useful lifetime of the information

Block Cipher Structure

- Symmetric block cipher consists of:
  - A sequence of rounds
  - With substitutions and permutations controlled by key
- Parameters and design features:
  - Block size
  - Key size
  - Number of rounds
  - Subkey generation algorithm
  - Round function
  - Fast software encryption/decryption
  - Ease of analysis

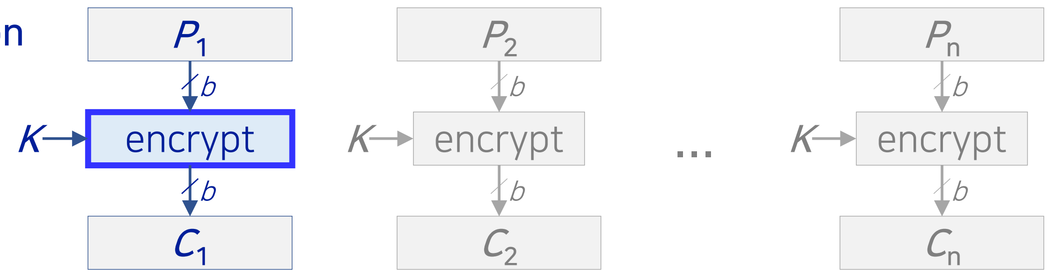


	DES	Triple DES	AES
Block size (bit)	64	64	128
Key size (bit)	56	112 or 168	128, 192 or 256

Data Encryption Standard (DES)

- Most widely used encryption scheme
- Adopted in 1977 by National Bureau of Standards (Now NIST)
- FIPS PUB 46
- Algorithm: Data Encryption Algorithm (DEA)
- Minor variation of the Feistel network

1) encryption



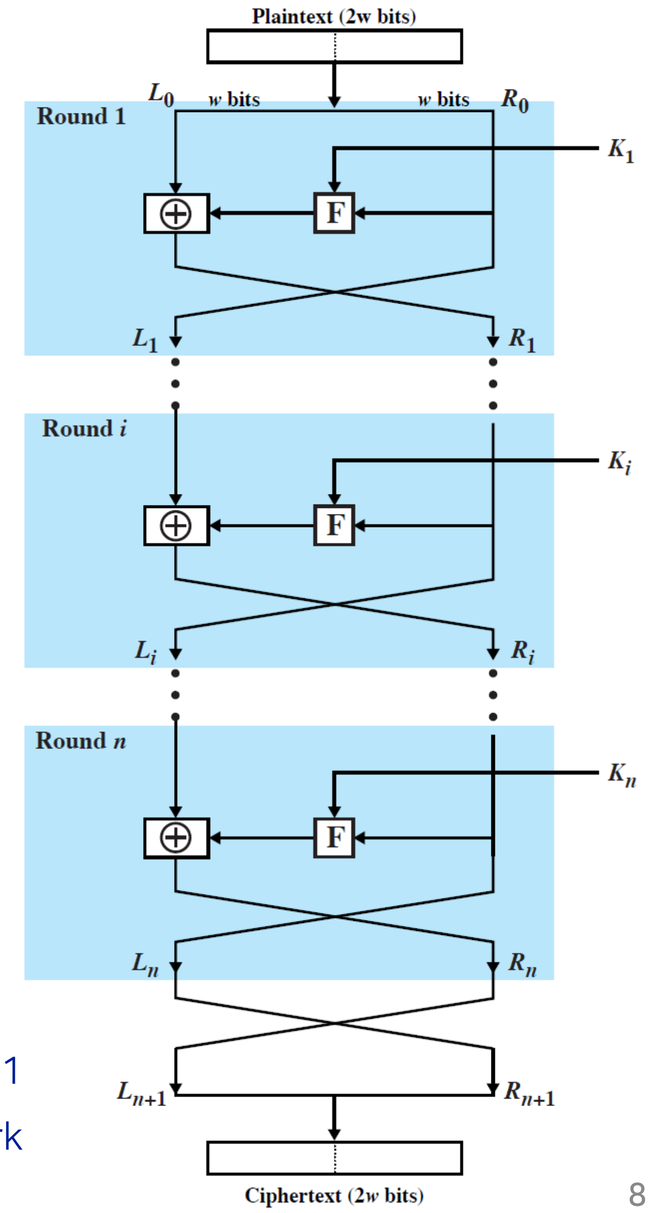
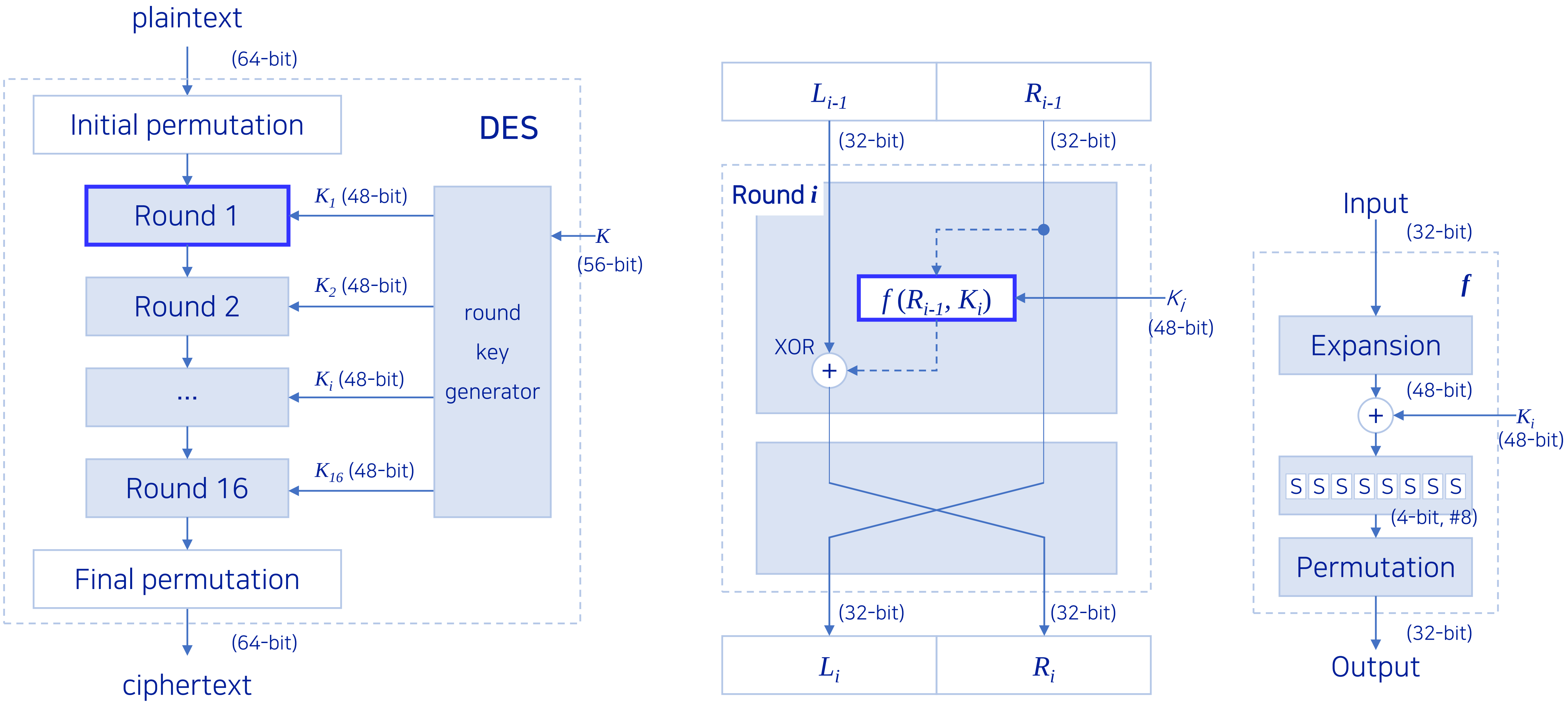


Figure 20.1

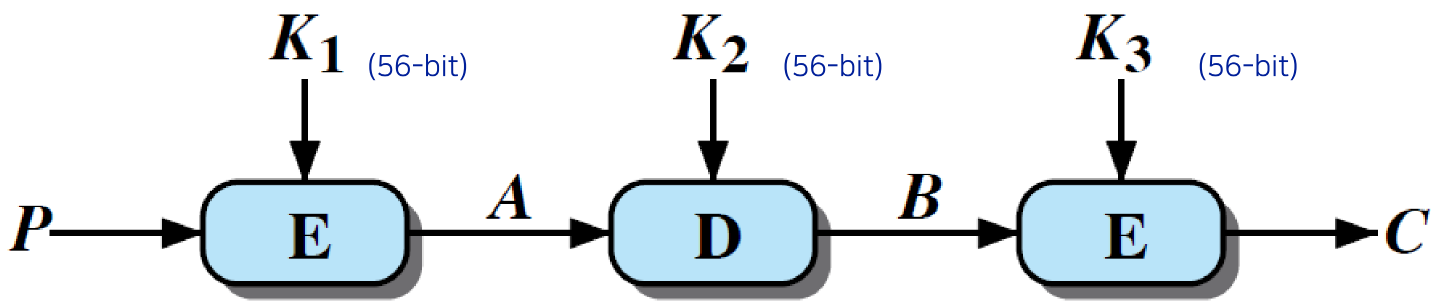
Classical Feistel network

DES

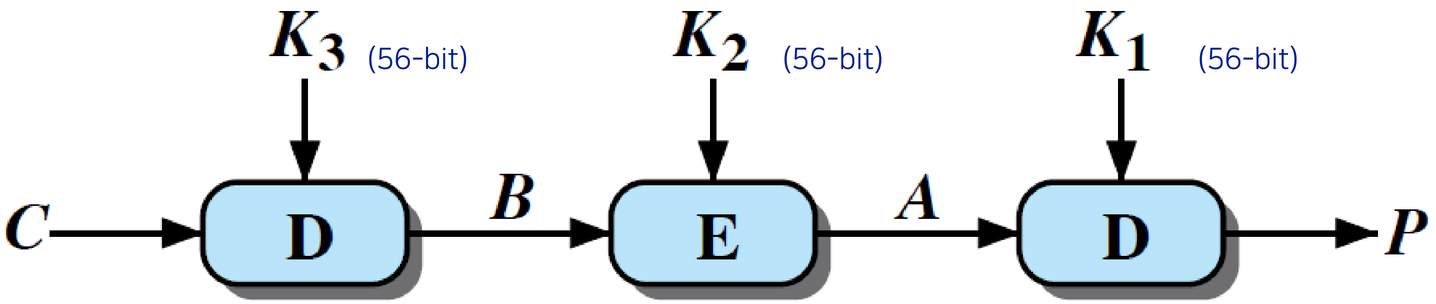


plaintext
(64-bit)
Initial permutation
DES
Round 1
K_1 (48-bit)
Round 2
K_2 (48-bit)
...
K_i (48-bit)
Round 16
K_{16} (48-bit)
round
key
generator
K
(56-bit)
Final permutation
(64-bit)
ciphertext
L_{i-1}
R_{i-1}
(32-bit)
(32-bit)
Round i
$f(R_{i-1}, K_i)$
K_i
(48-bit)
XOR
(32-bit)
(32-bit)
L_i
R_i
Input
(32-bit)
f
Expansion
(48-bit)
K_i
(48-bit)
S S S S S S S S
(4-bit, #8)
Permutation
(32-bit)
Output

Triple-DES (Figure 20.2)



(a) encryption



(b) decryption

for 3DES with 3 keys,

$$C = \mathrm{E}\left(K_3, \mathrm{D}\left(K_2, \mathrm{E}(K_1, P)\right)\right)$$

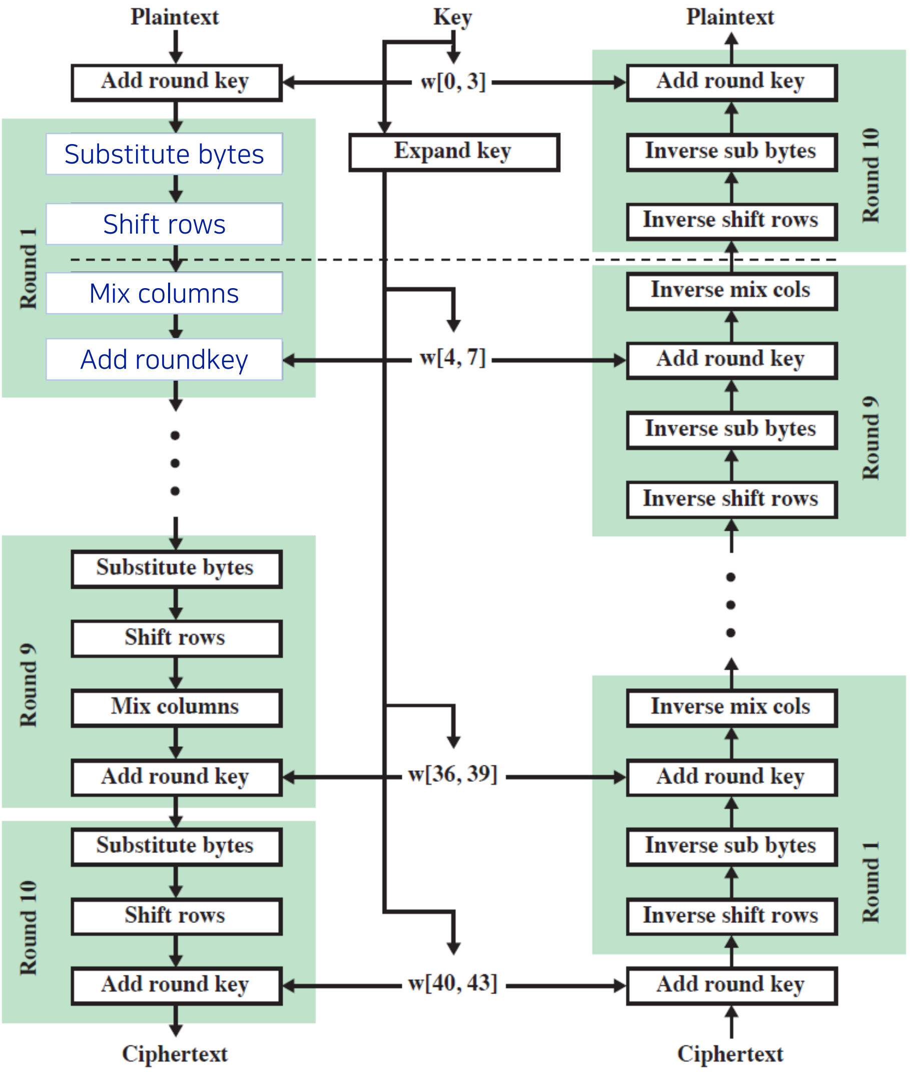
for 3DES with 2 keys,

$$C = \mathrm{E}\left(K_1, \mathrm{D}\left(K_2, \mathrm{E}(K_1, P)\right)\right)$$

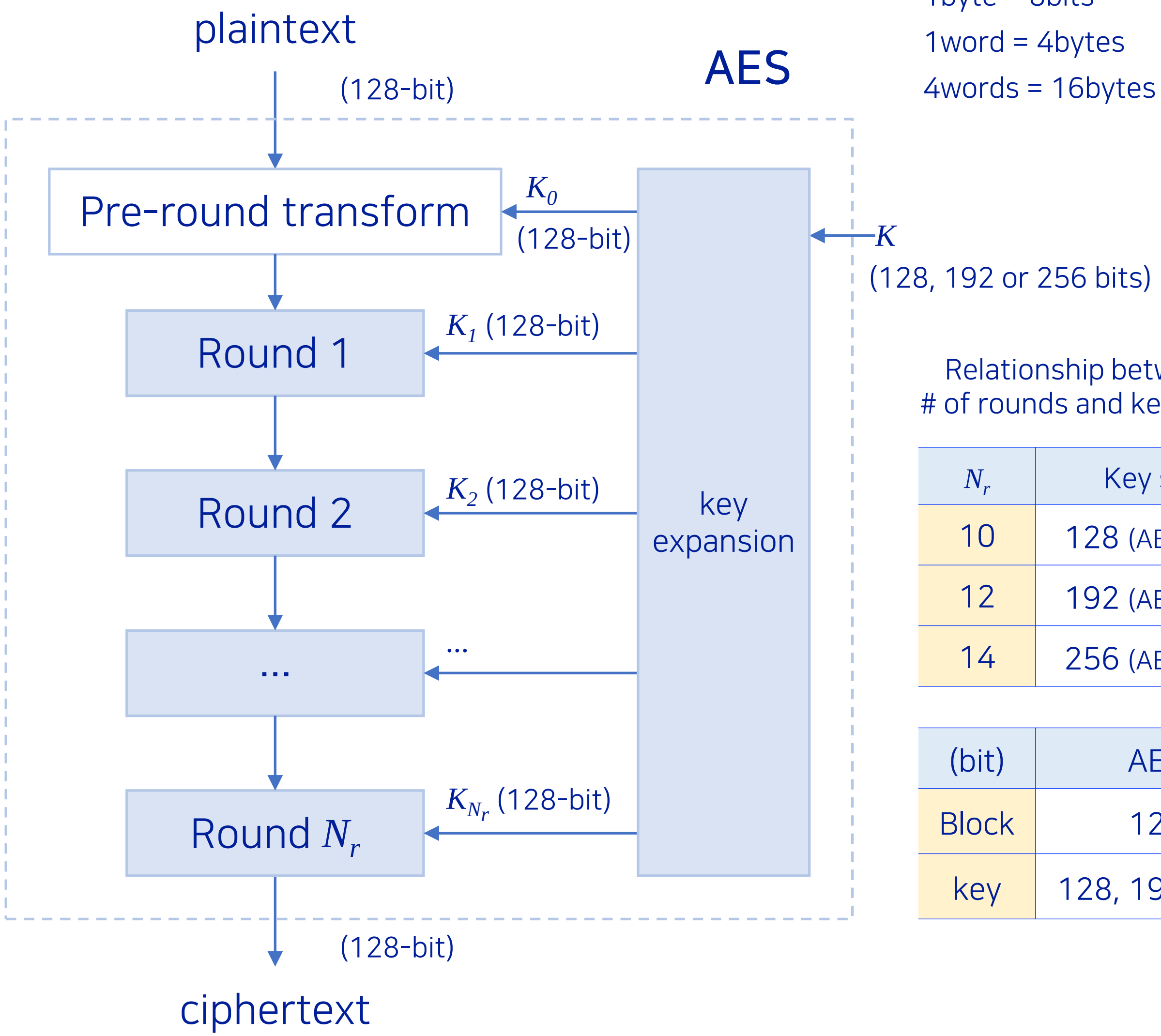
$$P = \mathrm{D}\left(K_1, \mathrm{E}\left(K_2, \mathrm{D}(K_3, C)\right)\right)$$

	DES	Triple DES
Block size (bit)	64	64
Key size (bit)	56	112 or 168

AES encryption and decryption (Figure 20.3)



(a) encryption (b) decryption



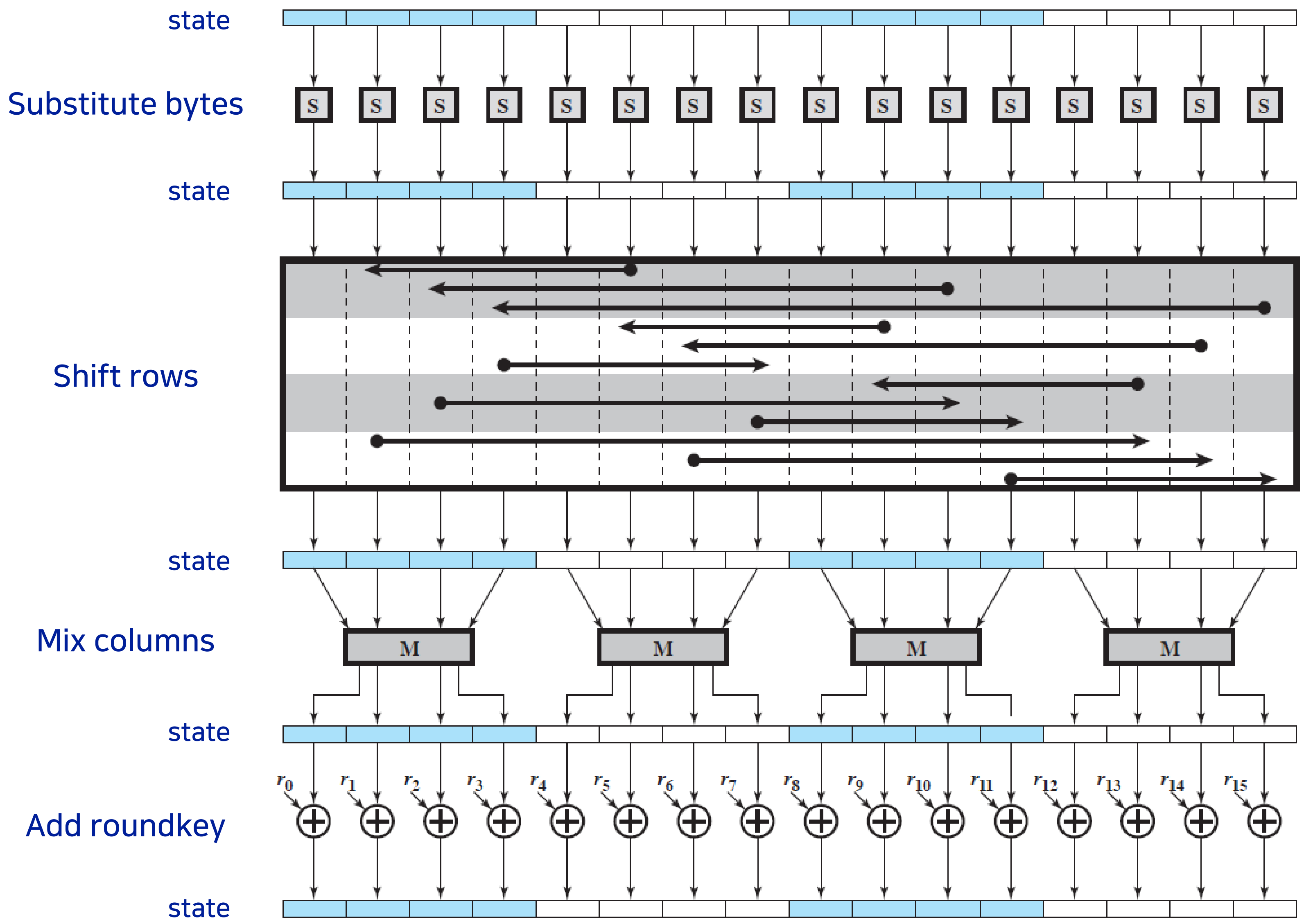
1byte = 8bits
1word = 4bytes
4words = 16bytes = 128bits

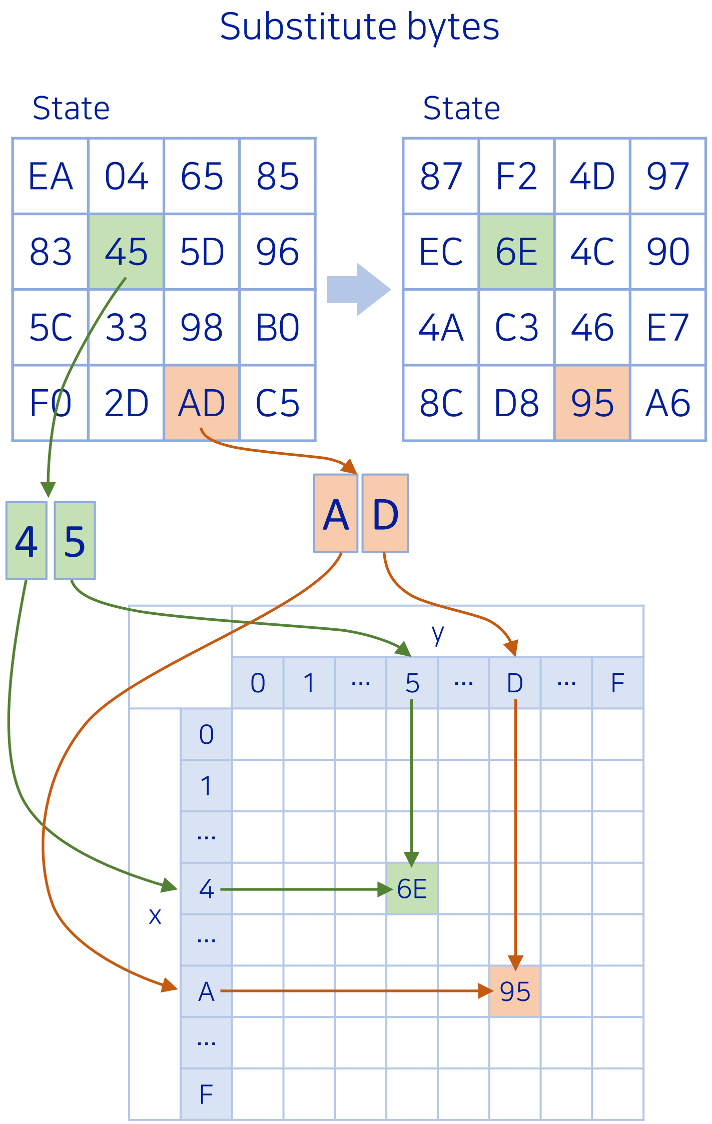
Relationship between
\# of rounds and key sizes

N_r	Key size
10	128 (AES-128)
12	192 (AES-192)
14	256 (AES-256)

(bit)	AES
Block	128
key	128, 192, 256

AES encryption round (Figure 20.4)





AES S-Boxes (Table 2)

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

(a) AES S-box

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
	1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
	2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
	3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
	5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
	B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
	C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
	D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
	E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
	F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

(b) AES Inverse S-box

AES shift rows

- on encryption left rotate each row of State by 0,1,2,3 bytes respectively
- decryption does reverse
- to move individual bytes from one column to another and spread bytes over columns

State					State			
87	F2	4D	97	Shift 0	87	F2	4D	97
EC	6E	4C	90	Shift 1	6E	4C	90	EC
4A	C3	46	E7	Shift 2	46	E7	4A	C3
8C	D8	95	A6	Shift 3	A6	8C	D8	95

AES mix columns

- Operates on each column individually
- Mapping each byte to a new value that is a function of all four bytes in the column
- Use of equations over finite fields
- To provide good mixing of bytes in column

$87_{(16)} \times 02 = 1000\ 0111 \times 10$

$(x^7 + x^2 + x + 1)\cdot(x)$

$= (x^8 + x^3 + x^2 + x)$, overflow

if overflow, adding $(x^8 + x^4 + x^3 + x + 1)$

$\therefore\ (\cancel{x^8} + \cancel{x^3} + x^2 + \cancel{x}) + (\cancel{x^8} + x^4 + \cancel{x^3} + \cancel{x} + 1)$

$= x^4 + x^2 + 1$

$= 0001\ 0101$

$6E_{(16)} \times 03 = 0110\ 1110 \times 11$

$(x^6 + x^5 + x^3 + x^2 + x)\cdot(x + 1)$

$= (x^7 + \cancel{x^6} + x^4 + \cancel{x^3} + \cancel{x^2})$

$+\ (\cancel{x^6} + x^5 + \cancel{x^3} + \cancel{x^2} + x)$

$= x^7 + x^5 + x^4 + x$

$= 1011\ 0010$

$46_{(16)} \times 01 = 0100\ 0110$

$A6_{(16)} \times 01 = 1010\ 0110$

constant matrix

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

×

State

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

=

State

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

$$
\begin{array}{rr}
 & 0001\ 0101 \\
 & 1011\ 0010 \\
 & 0100\ 0110 \\
\oplus) & 1010\ 0110 \\
\hline
 & 0100\ 0111 \quad = 47_{(16)}
\end{array}
$$

AES add round key

- Simply XOR State with bits of expanded key
- Security from complexity of round key expansion and other stages of AES

State

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

$\oplus$

Round key

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
ED	A5	A6	BC

$=$

State

EB	59	8B	1B
40	2E	A1	C3
F2	38	13	42
1E	84	E7	D2

$$47_{(16)} = 0100\ 0111$$
$$\oplus)\ AC_{(16)} = 1010\ 1100$$
$$1110\ 1011 = EB_{(16)}$$

$$E4_{(16)} = 1110\ 0100$$
$$\oplus)\ DC_{(16)} = 1101\ 1100$$
$$0011\ 1000 = 38_{(16)}$$

Block cipher modes of operation (Table 20.3)

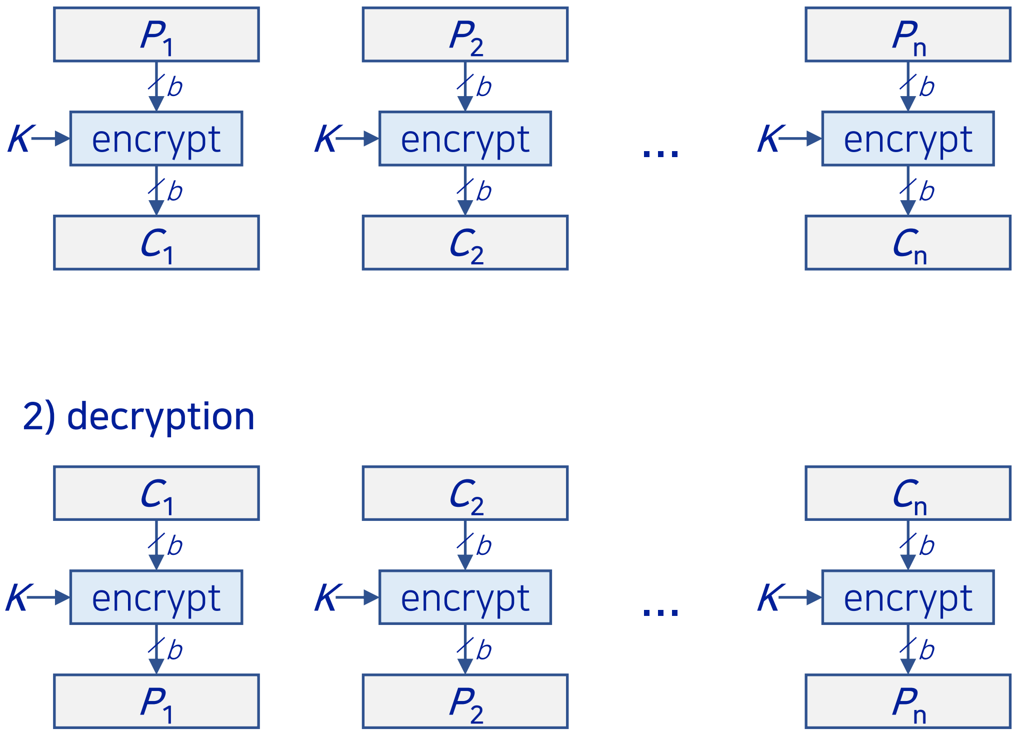
Type of attack	Description	Typical application
ECB (electronic codebook)	Each block of 64 plaintext bits is encoded independently using the same key.	• Secure transmission of single values (e.g., an encryption key)
CBC (Cipher block chaining)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	• General-purpose block-oriented transmission • Authentication
CFB (cipher feedback)	Input is processed s bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission • Authentication
OFB (output feedback)	Similar to CFB, except that the input to the encryption algorithm is the preceding DES output.	• Stream-oriented transmission over noisy channel (e.g., satellite comm.)
CTR (counter)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General-purpose block-oriented transmission • Useful for high-speed requirements

Electronic Codebook (ECB)

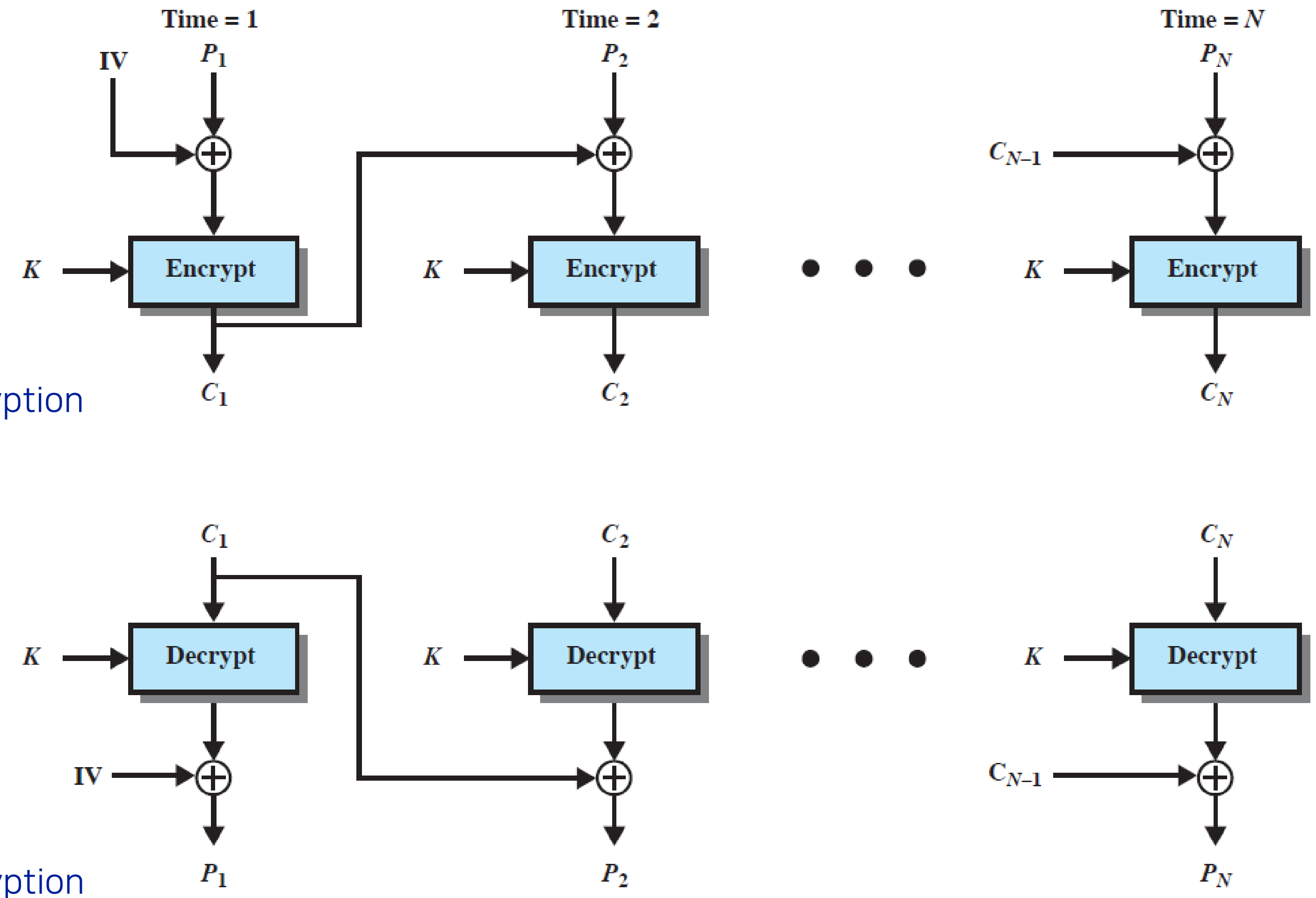
- Simplest mode
- Plaintext is handled b-bit at a time and each block is encrypted using the same key
- "Codebook" is used because there is an unique ciphertext for every b-bit block of plaintext
  - Not secure for long messages since repeated plaintext is seen in repeated ciphertext
  - To overcome security deficiencies you need a technique where the same plaintext block, if repeated, produces different ciphertext blocks

1) encryption

2) decryption



Cipher block chaining (CBC) mode (Figure 20.6)



(a) encryption

(b) decryption

for encryption,

$$C_i = \mathrm{E}(K, [P_i \oplus C_{i-1}])$$

for decryption,

$$\mathrm{D}(K, C_i) = \cancel{\mathrm{D}(K}, \cancel{\mathrm{E}(K}, [P_i \oplus C_{i-1}]))$$

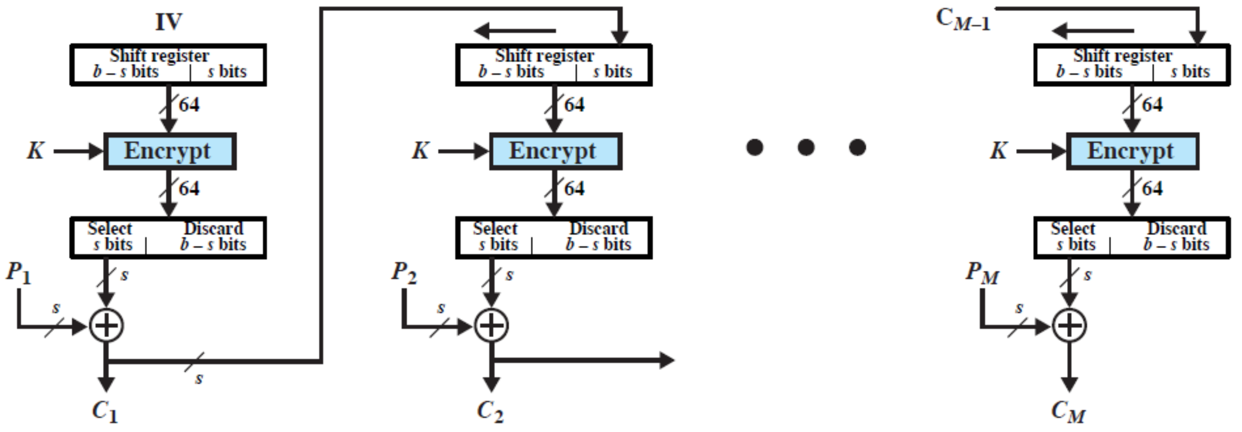
$$= P_i \oplus C_{i-1}$$

$$\therefore P_i \oplus \cancel{C_{i-1}} \oplus \cancel{C_{i-1}}$$

$$= P_i = \mathrm{D}(K, C_i) \oplus C_{i-1}$$

s-bit cipher feedback (CFB) mode (Figure 20.7)

(a) encryption



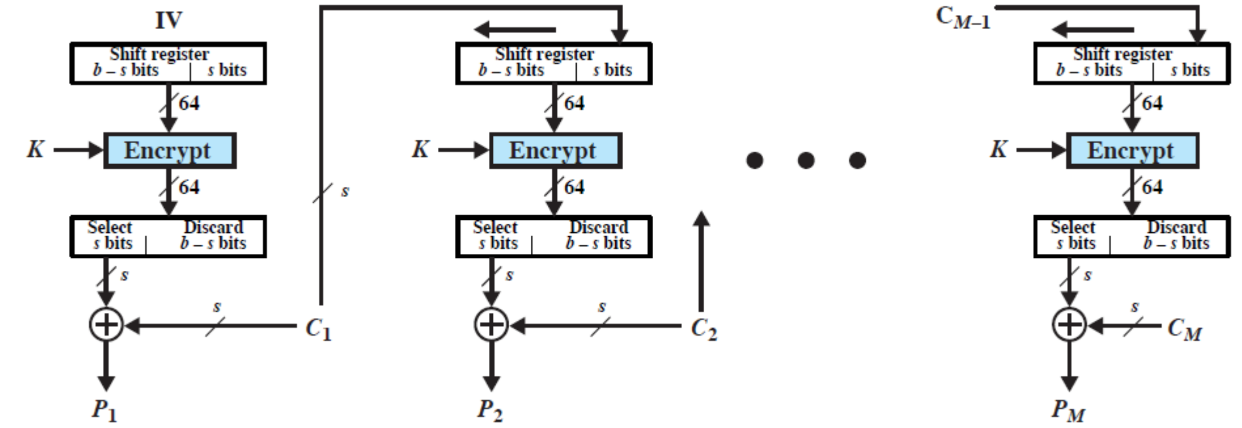
for encryption,

$$C_1 = P_1 \oplus S_b\big(\mathrm{E}(K, IV)\big)$$

$$C_i = P_i \oplus S_b\big(\mathrm{E}(K, SR_{b-s}(I_{i-1}) \parallel C_{i-1})\big)$$

$$\because \begin{cases} I_i = SR_{b-s}(I_{i-1}) \parallel C_{i-1}, & \text{for } (i > 1) \\ i_1 = \mathrm{IV} & \end{cases}$$

(b) decryption



for decryption,

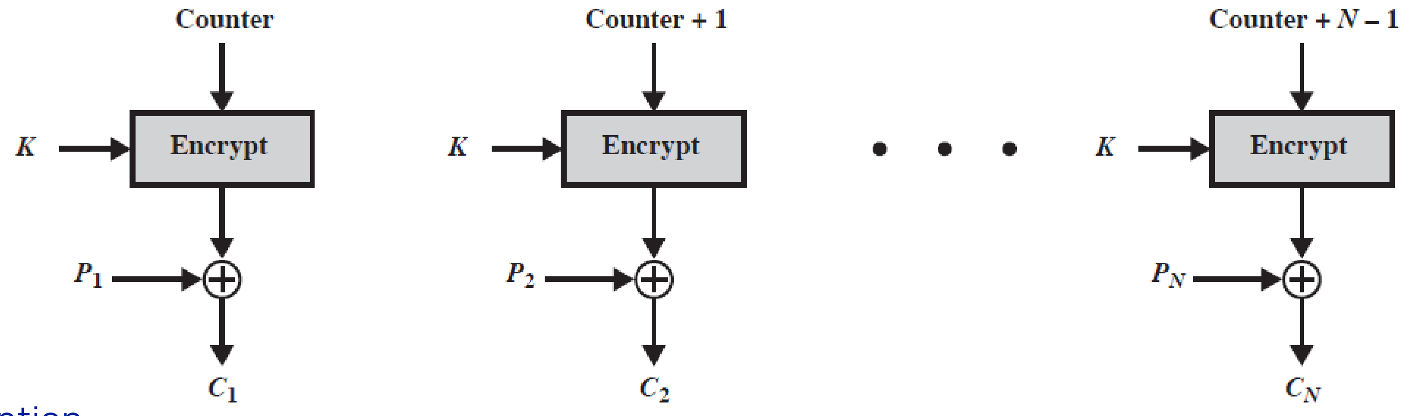
$$P_1 \oplus S_b\big(\mathrm{E}(K, IV)\big) = C_1$$

$$P_1 \oplus \cancel{S_b\big(\mathrm{E}(K, IV)\big)} \oplus \cancel{S_b\big(\mathrm{E}(K, IV)\big)}$$

$$= P_1 = C_1 \oplus S_b\big(\mathrm{E}(K, IV)\big)$$

$$P_i = C_i \oplus S_b\big(\mathrm{E}(K, SR_{b-s}(I_{i-1}) \parallel C_{i-1})\big)$$

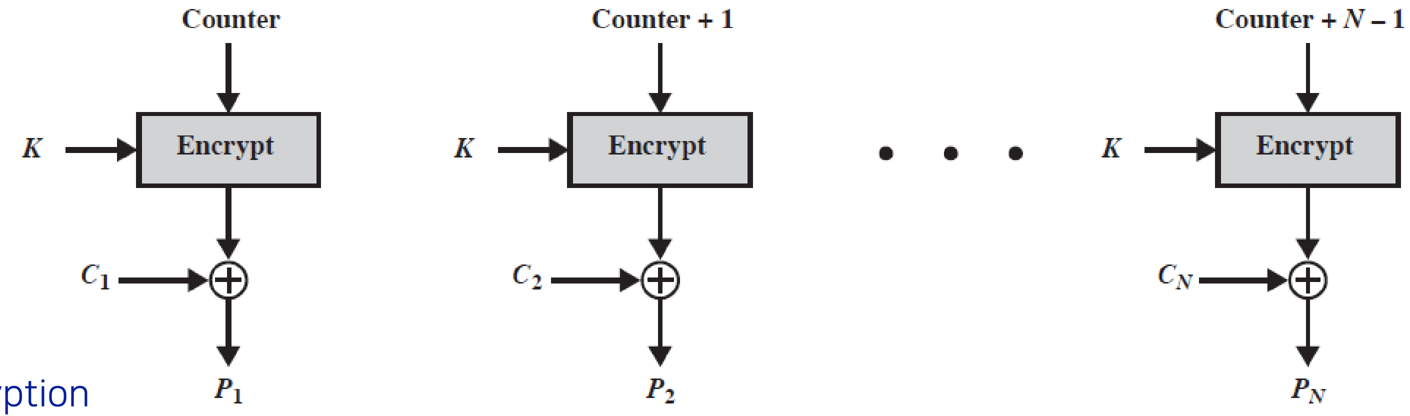
Counter (CTR) mode (Figure 20.8)



(a) encryption

for encryption,

$$C_i = P_i \oplus \mathrm{E}(K, T_i)$$



(b) decryption

for decryption,

$$P_i = C_i \oplus \mathrm{E}(K, T_i)$$

Key Distribution

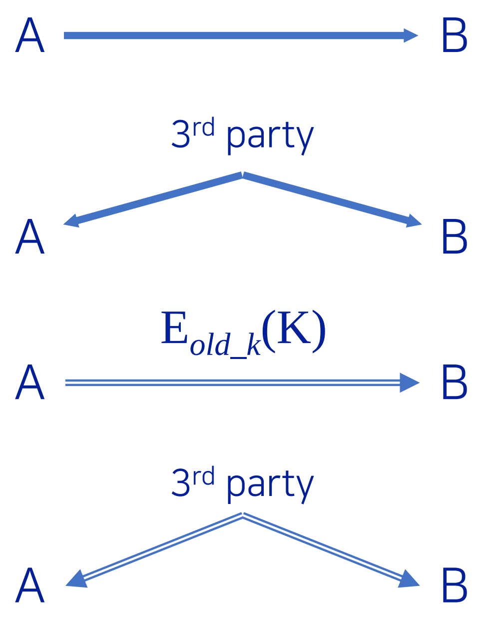
- The means of delivering a key to two parties that wish to exchange data without allowing others to see the key
  - Two parties (A and B) can achieve this by:

1) A key could be selected by A and physically delivered to B

2) A third party could select the key and physically deliver it to A and B

3) If A and B have previously and recently used a key, one party could transmit the new key to the other, encrypted using the old key

4) If A and B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B



Summary

- Symmetric encryption principles
  - Feistel cipher structure
- Data encryption standard
  - Data encryption standard
  - Triple DES
- Advanced encryption standard
  - Overview of the algorithm
  - Algorithm details
- Operation modes
  - Cipher block modes of operation
  - Electronic codebook mode
  - Cipher block chaining mode
  - Cipher feedback mode
  - Counter mode
- Key distribution