Chap. 2 Symmetric Encryption and Message Confidentiality

- Cryptography and Cryptanalysis
- Symmetric Encryption Algorithms
- Modes of Operation
- Key Distribution

Cryptography

- Cryptography relies on
  - Ciphers: *mathematical functions used for encryption and decryption of a message*
  - ***Encryption*** : the process of disguising a message in such a way as to hide its substance
  - Ciphertext: an encrypted message
  - ***Decryption*** : the process of returning an encrypted message back into plaintext.

Ciphers

- The security of a cipher which depends on the secrecy of its *restricted* algorithm is not good
  - When a user leaves a group, the algorithm must change; designing a new alg. is difficult
  - Secrecy can be broken by people smarter than you
- Modern cryptography relies on *keys*
  - *key: a selected value from a large set (a key-space); (e.g.) a 1024-bit key => 2^{1024} values!*
  - Security is based on secrecy of the key, not the details of the algorithm
  - Change of authorized participants requires only a change in key

Cryptosystem

- Conventional cryptosystem
  - Secret-key cryptosystem, symmetric cryptosystem

- Public-key cryptosystem
  - Asymmetric cryptosystem

Cryptosystem

- For some message *M*, let's denote the encryption of that message into cipher text using key *k* as

$$C = E_k(M)$$

- Similarly, the decryption into plain text as

$$M = D_k(C)$$

- Symmetric key algorithms

$$D_k(E_k(M)) = M$$

- Public-key algorithms

$$D_{k2}(E_{k1}(M)) = M$$

Example Ciphers

- Shift cipher:
  - k-shift cipher: each plaintext character is replaced by a character *k* to the right
  - When *k=3*, it's a Caesar cipher: "Watch out for Brutus!" => "Zdwfk rxw iru Euxwxv!"
  - Only 25 choices! Not hard to break by brute force
- Substitution Cipher:
  - each character in plaintext is replaced by a corresponding character of ciphertext

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

Cryptanalysis

- Cryptanalysis
  - the science of recovering the plaintext of a ciphertext without access to the key
- Encryption algorithm is open to the public (known to the opponents !!!)
- Cryptanalyst
  - knows the encryption and decryption algorithm
  - has many information except keys
  - uses computers and his intelligence

Cryptanalysis

- Ciphertext-only attack
  - Attacker has to recover the plaintext from only the ciphertext
  - Brute-force attack: trying all possible keys

- Known-plaintext attack
  - Some pairs of the (ciphertext, plaintext) are known for the secret key or analysts know when certain plaintext patterns will appear in a message

Cryptanalysis

Chosen-plaintext attack

- The attacker can access the cryptosystem and get some (plaintext, ciphertext) pairs for the plaintexts chosen by him

Chosen text attack

- The attacker can know some (plaintext, ciphertext) pairs for the plaintexts chosen by him, and also
- some (ciphertext, plaintext) pairs for the ciphertexts chosen by him

Cryptanalysis

- Ideally, the attacker has to use brute force in an *exhaustive search* of the key-space

- Unconditionally secure cryptosystem:
  - The ciphertext generated by the system does not contain enough information to determine the plaintext, no matter how much ciphertext is available

Cryptanalysis

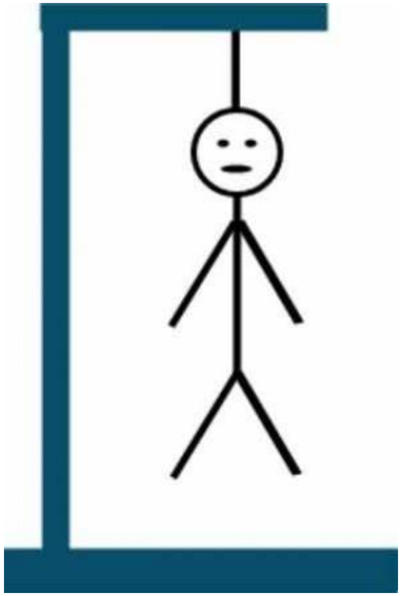
- Computationally secure cryptosystem
  - The time required to break the cipher exceeds the useful lifetime of the information
  - The cost of breaking the cipher exceeds the value of the encrypted information

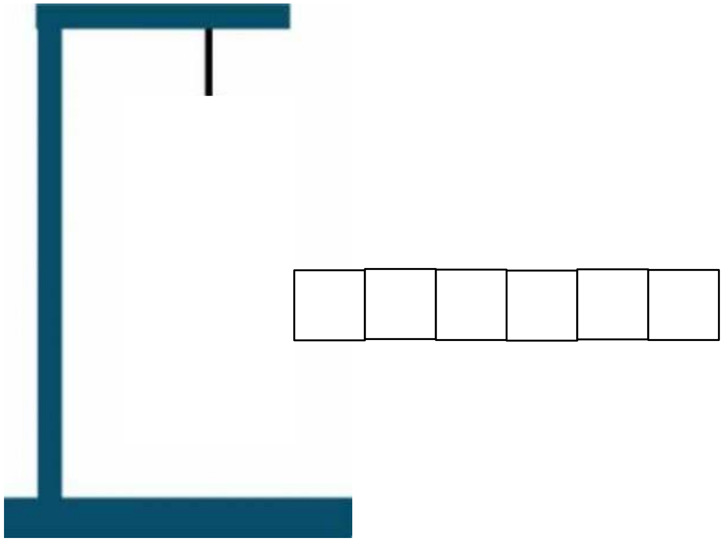
Cryptanalysis

- It is the complexity of launching the attack that secures us:
  - Data complexity: a large number of expected inputs (e.g., ciphertext) required
  - Storage complexity: a large amount of storage units required
  - Processing complexity: a large number of computations required

Cryptanalysis

- A simple substitution cipher over a natural language can not be so difficult
  - (e.g.) “Vkj’u muumbf. Rc mocj’u ocmvw.”
  - Hangman game:





Cryptanalysis

- Special characters (spaces and punctuations) are not encrypted
- Frequency of each letter is different in normal English texts:
  - "e" and "t" are the most frequent:
- You can also analyze clusters of letters
  - Analyze the frequency of two-letter combinations (digram)
  - "th" and "he" are common: of the 26^2 digrams, the top 15 account for 27% of all occurrences

Cryptanalysis

- A simple substitution cipher over a natural language is not so difficult
  - (e.g.) “Vkj’u muumbf. Rc mocj’u ocmvw.”

```
“Don’t attack. We aren’t ready.”
```

Polyalphabetic ciphers

- Substitutions with a single alphabet

  → monoalphabetic substitutions

- A more complex alternative is to use different substitution mappings on various portions of the plaintext

  → Polyalphabetic substitutions

Polyalphabetic ciphers: Vigenère ciphers

- Vigenère cipher:
  - each character of plaintext is encrypted with a different cipher key using Vigenère tableau
- E.g.: key="deceptive"

```
Plaintext : b e c a r e f u l i a m a h a c k e r
Key       : d e c e p t i v e d e c e p t i v e
Ciphertext: E I E E G .. ..
```

Vigenère ciphers

Vigenère table

	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
a	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
b	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	A
c	C	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
d	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
e	E	F	G	H	I	J	K	L	M																	D
f	F	G	H	I	J	K	L	M	N																	E
g	G	H	I	J	K	L	M	N	O																	F
h	H	I	J	K	L	M	N	O	P																	G
i	I	J	K	L	M	N	O	P	Q																	H
j	J	K	L	M	N	O	P	Q	R																	I
k	K	L	M	N	O	P	Q	R	S																	J
l	L	M	N	O	P	Q	R	S	T																	K
m	M	N	O	P	Q	R	S	T	U																	L
n	N	O	P	Q	R	S	T	U	V																	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

Plaintext : b e c a r e f u l i

Key : d e c e p t i v e d

Ciphertext: E I E E G .. ..

Breaking the Vigenère cipher

- Kasiski method
  - Cipher keys with length *t* is repeatedly used with period *t*

  → if we find the period, we can attack each shift cipher independently

- Ciphertext:

```
QER ASX AS SD QER SKFWD WE QER SDFWED
```

with high probability:

Plaintext:	t	h	e		t	h	e	t	h	e
Key: :	k	m	n		k	m	n	k	m	n

distance=10

Breaking the Vigenère cipher

- We must look for occurrences in the ciphertext that is repeated in a multiple of the cipher key

```
QER ASX AS SD QER SKFWD WE QER SDFWED
```

Plaintext: t h e t h e t h e

Key: : k m n k m n k m n

distance=10

- Period = 10
  - Key length: 10 or divisor of 10

Breaking the Vigenère cipher

- We can apply statistical measures, like auto-correlation, to the ciphertext
  - Intuitively, guess key length is less than L
  - For each letter of ciphtertext, C_i , count how often $C_i = C_{i+T}$, where $1<T<L$
  - Plot the counts for all T's, the period will appear as a spike on the graph

Permutation/Transposition

- Permutation: take the input, rearrange the output in a specific way; also referred to as *transposition*
  - (e.g.) Write the letters in a rectangle, row by row, and reading it column by column

```
 1 3 2 4 5 6 7 8
 t h e l a u n c
 h c o d e i s i
 n t h e d e s k
= thh eoh hct lde aed uie nss cik
```

```
the launch code is
in the desk
```

- Using the technique simply is weak as it preserves the frequencies of the letters

Permutation

- A double permutation

1	3	2	4	5	6	7	8
t	h	e	l	a	u	n	c
h	c	o	d	e	i	s	i
n	t	h	e	d	e	s	k

→ thheohhctldeaeduienssciк

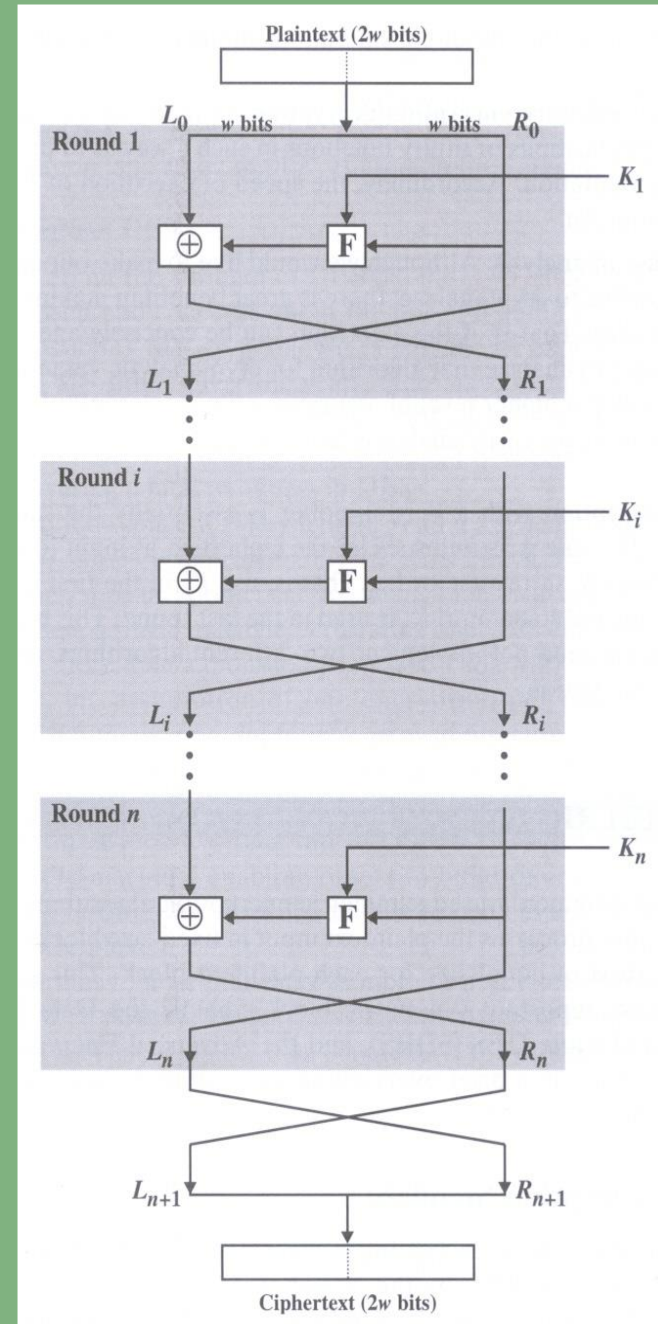
1	3	2	4	5	6	7	8
t	h	h	e	o	h	h	c
t	l	d	e	a	e	d	u
i	e	n	s	s	c	i	k

→ ttihlehdneesoashechdicuk

- Product cipher:
  - Use two cipher alg. and apply cipher alg. β after α
  - modern ciphers combine permutations and substitutions

Fiestel Cipher Structure

- Repetition of substitution and permutation
- Block cipher structure
  - Block size : 2w bits
  - F : round function (combination of permutation and substitution)



Symmetric Cipher Algorithms

- Block ciphers
  - Plaintext is treated as *n*-bit blocks of data
  - Ciphertext is the same length as plaintext
- Stream ciphers
  - Encrypts one bit/byte at a time
  - Often easier to analyze mathematically

DES (Digital Encryption Standard)

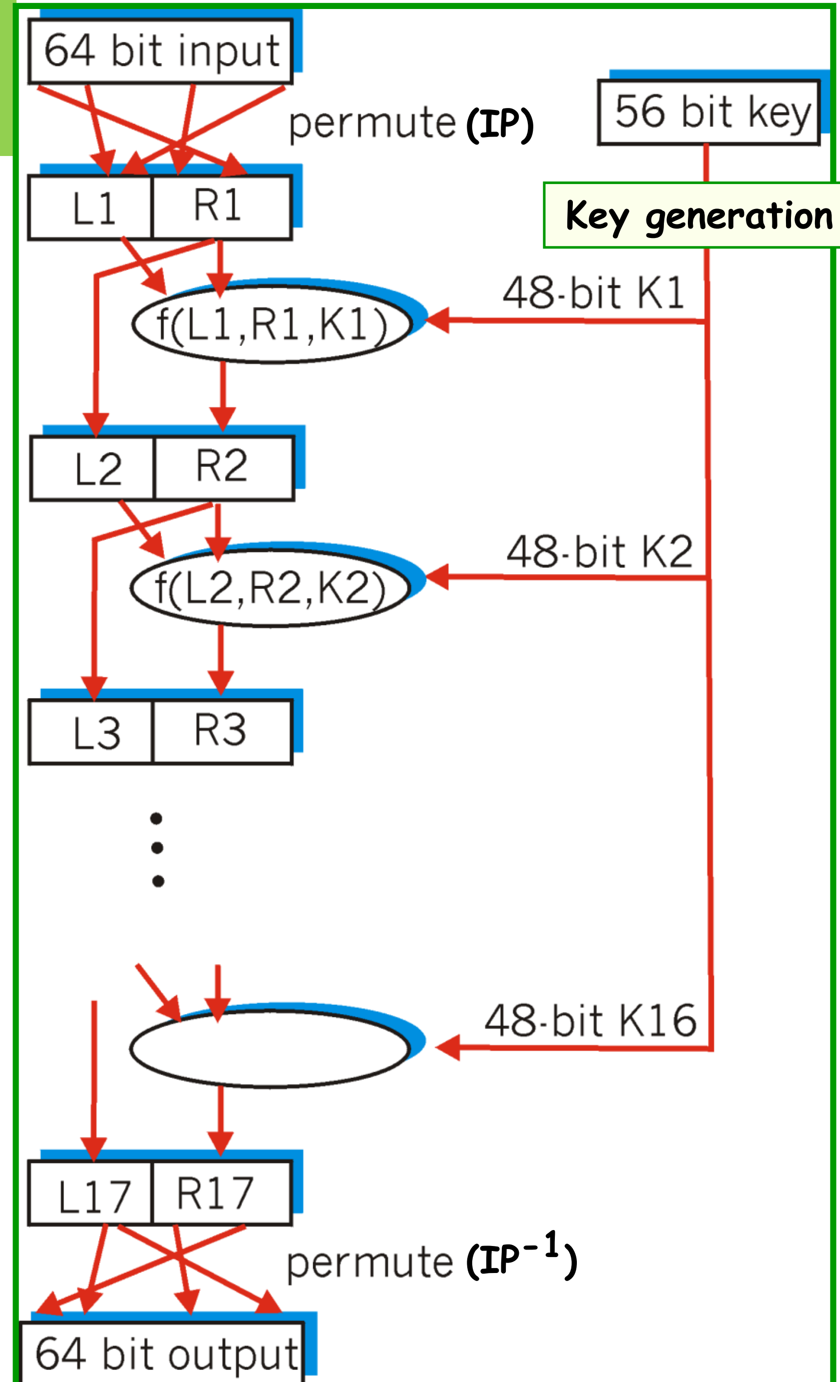
- Adopted by the US NIST in 1976 as a standard
- A 16-round of substitutions and permutations
- Block size : 64-bits
- Key size : 56-bit key is transformed in to 16 48-bit subkeys
- Same algorithm for encryption and decryption (sub-keys are used in reverse order for decryption)

DES

- Key generation
- An initial permutation (IP)
- 16 rounds of manger function (f)
  - Expansion permutation of input
  - S-box substitution
  - P-box permutation

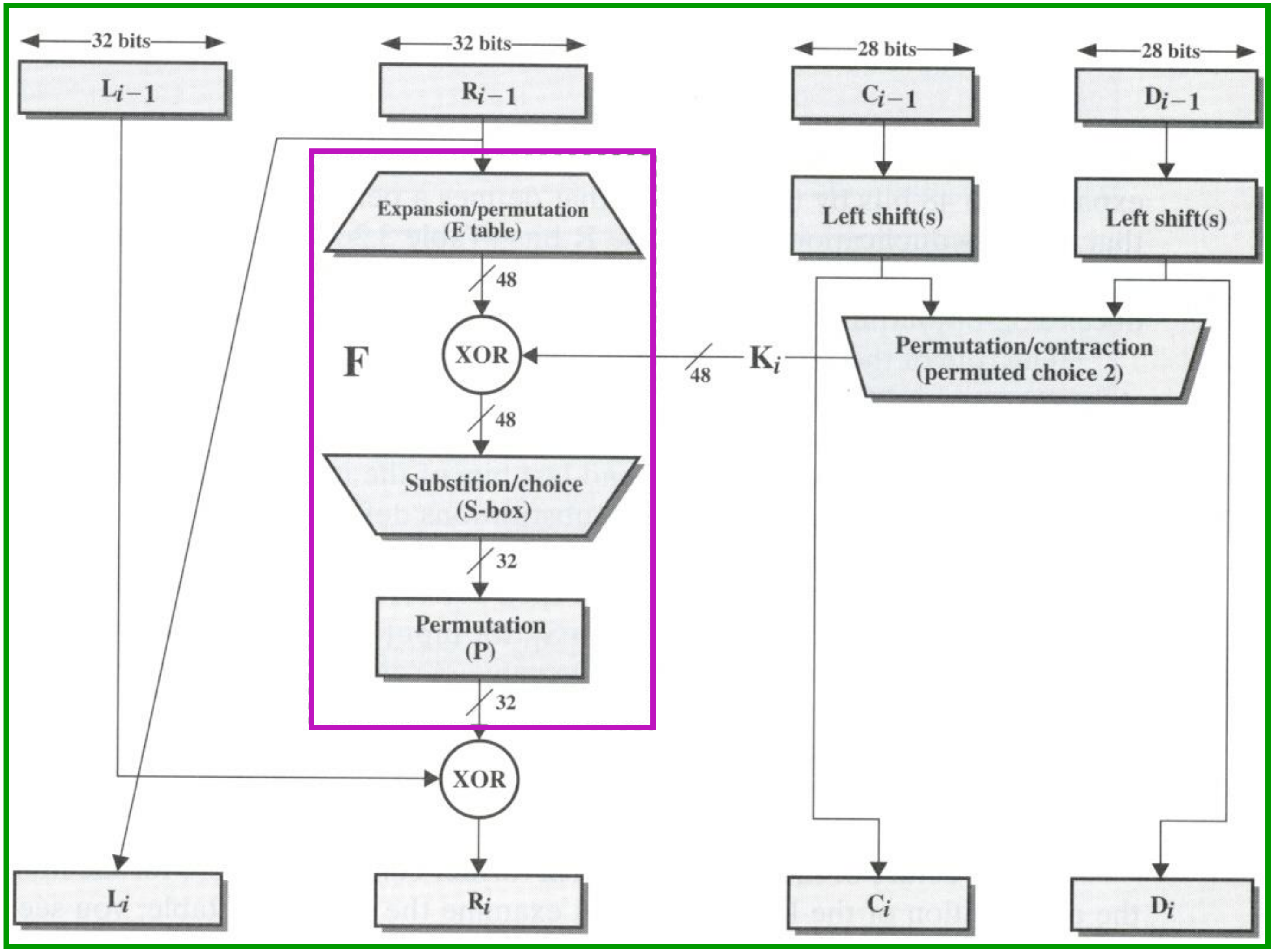
    -> $L_i = R_{i-1}$

    $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$
- A final permutation (IP^{-1})



DES

Single round of DES



DES

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

- S-boxes
  - DES uses 8 (4 row, 16 column) S-boxes
  - Each S-box contains 64 4-bit values
  - 6 input bits yields 4 output bits
  - Example: Given bits 110011 as input and S-box 6 from DES

Take first and last bits "11" to choose row 3
Take middle four bits "1001" to choose column 9
The value from S-box 6 of DES is 5 ("0101")
Substitute "0101" for "110011"

DES

- Avalanche effect:
  - small change in the plaintext or the key produce a significant change in the ciphertext
- Key space is too small
  - 56 bit keys provide 2^{56} possible keys → successfully attacked by brute force
- DES cracker by EFF :
  - attack possible in less than 1 day

Triple DES

- Triple-DES (using 3 keys)
  - Choose two different 64-bit keys K_1 , K_2 and K_3
  - $C = E_{k3}(D_{k2}(E_{k1}(P)))$
  - $P = E_{k1}(D_{k2}(E_{k3}(C)))$
  - Provides us with a key space of 2^{168} possible keys
- Triple-DES (using 2 keys)
  - Choose two different 64-bit keys K_1 and K_2
  - $C = E_{k1}(D_{k2}(E_{k1}(P)))$
  - Provides us with a key space of 2^{112} possible keys

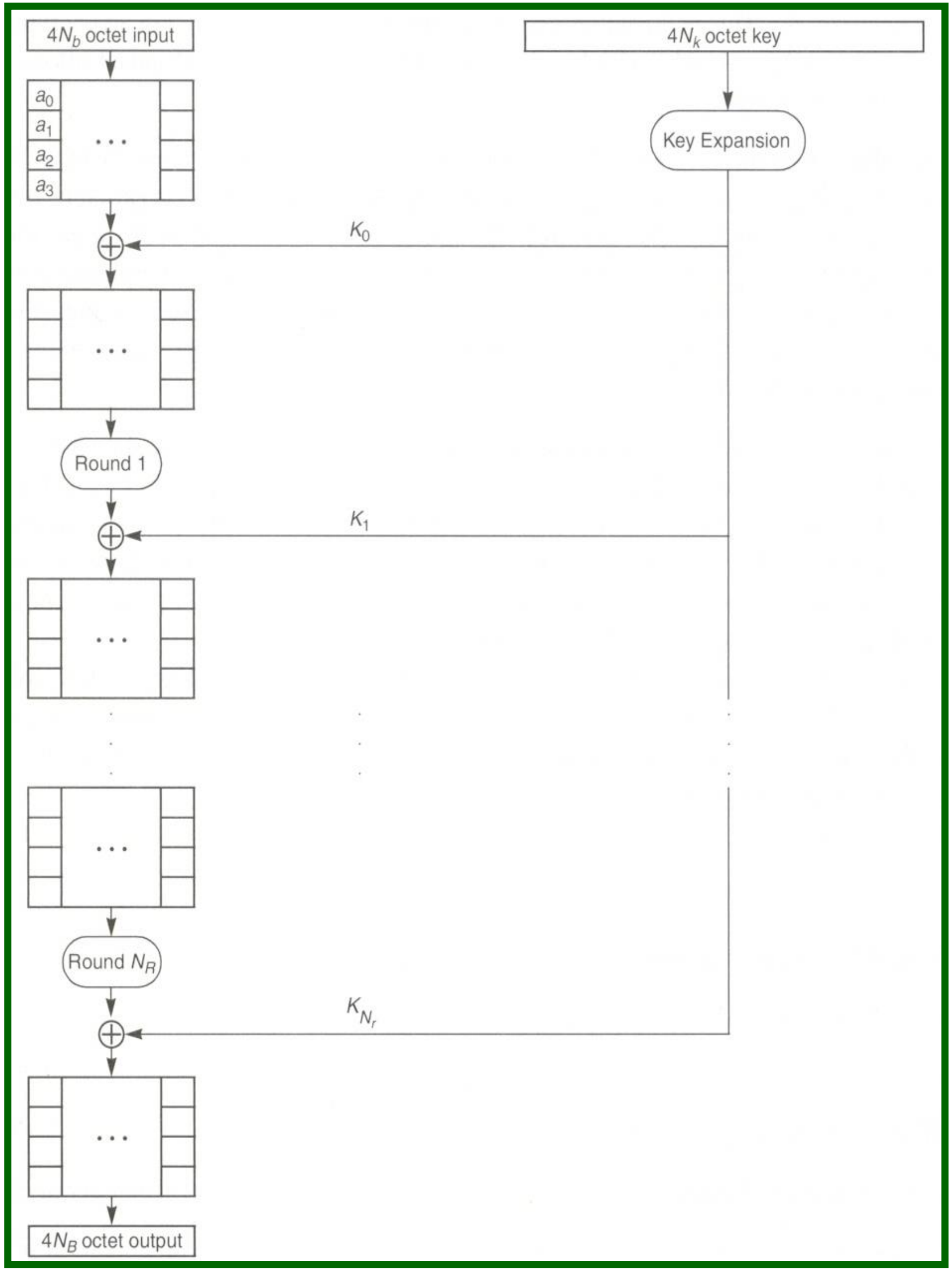
AES (Advanced Encryption Standard)

- Designed to replace DES by NIST at November 2001
- Design goal: efficiency, flexibility, security
- Rijndael (by J. Daemen and V. Rijmen)
- Low memory requirements (smart cards)
- Block size : 128 bits
- Flexible key size : 128, 192, 256 bits
- Variable number of rounds

AES

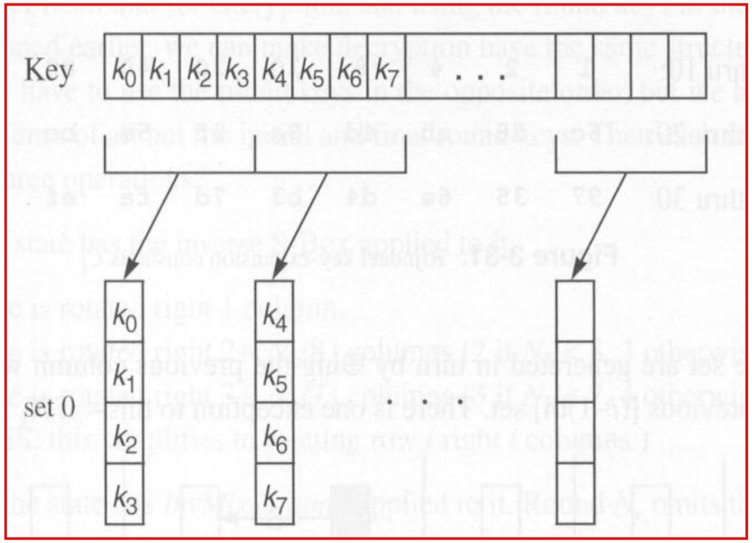
Basic structure

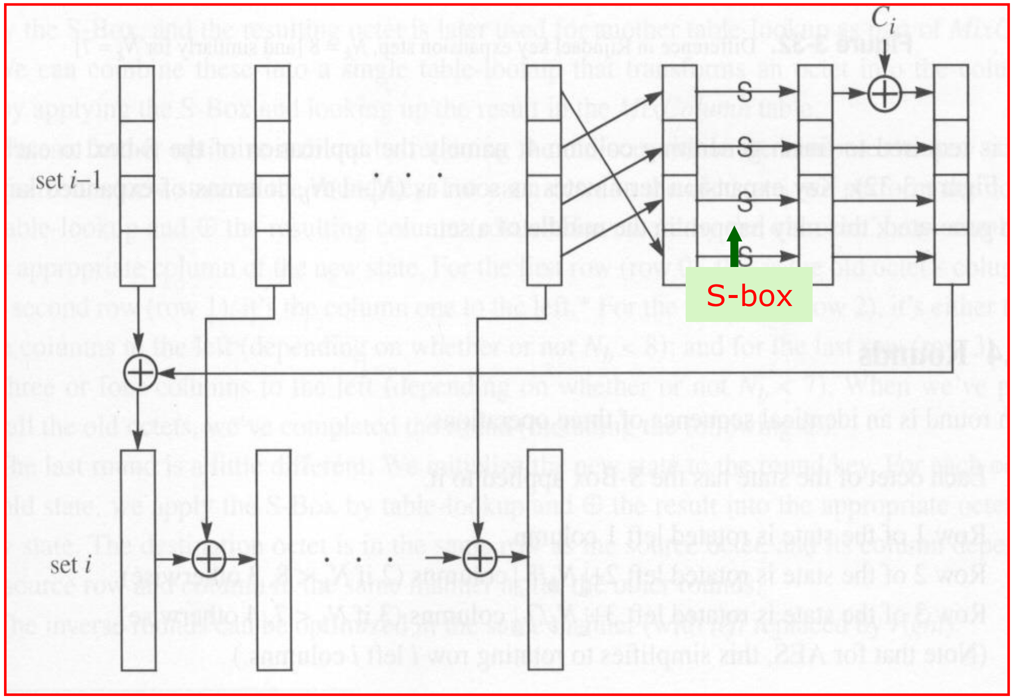
- Block size : 128 ($4*N_b$) bits
- Key size : $4*N_k$
  - $N_k = 4$ (AES-128)
  - $N_k = 6$ (AES-192)
  - $N_k = 8$ (AES-256)
- Number of rounds:
  - $N_r = 6 + \max(N_b, N_k)$



AES

- Key expansion
  - Set 0: arrange the key as 4-octet columns
  - Set i: expands the keys of set (i-1)
  - C_i = 1, 2, 4, 8, 10, 20, 40, 80, 1b, 36 where i = 1 to 10
  - Expanded keys: $4 * N_b * (N_r + 1)$





AES

AES state

- A rectangular array of octets which consists of N_b 4-octet columns
- Initialized from the $(4*N_b)$ octets of the input
- The state is transformed in N_r rounds: before round 1, between rounds, and after round N_r
- Each round transforms the state by $\oplus$-ing the next $(4*N_b)$ octets from the expanded key => read out as columns
- The final state is read out column by column (the output)

AES

Rounds (encryption)

1. Each octet of the state has the S-box applied to it
2. Row 1 of the state is rotated left 1 column,

   Row 2 of the state is rotated left (2+ $\lfloor N_b/8 \rfloor$) column

   Row 3 of the state is rotated left (3+ $\lfloor N_b/8 \rfloor$) column
3. Each column of the state has *MixColumn* applied to it (round N_r omits this operation)

AES

Basic operations

- ⊕: Bitwise-XOR
- SubBytes operation: an octet-to-octet substitution
- ShiftRows operation
- MixColumn operation : replaces a 4-octet column with another 4-octet column

The operations are reversible:

- ⊕: reversible (easy)
- S-box operation: inverse S-box
- ShiftRows operation: inverse ShiftRows operation
- MixColumn operation: inverse MixColumn table

AES

- SubBytes operation
- Octet-by-octet substitution
- (e.g) 5b -> 39

right (low-order) nibble

left (high-order) nibble

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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

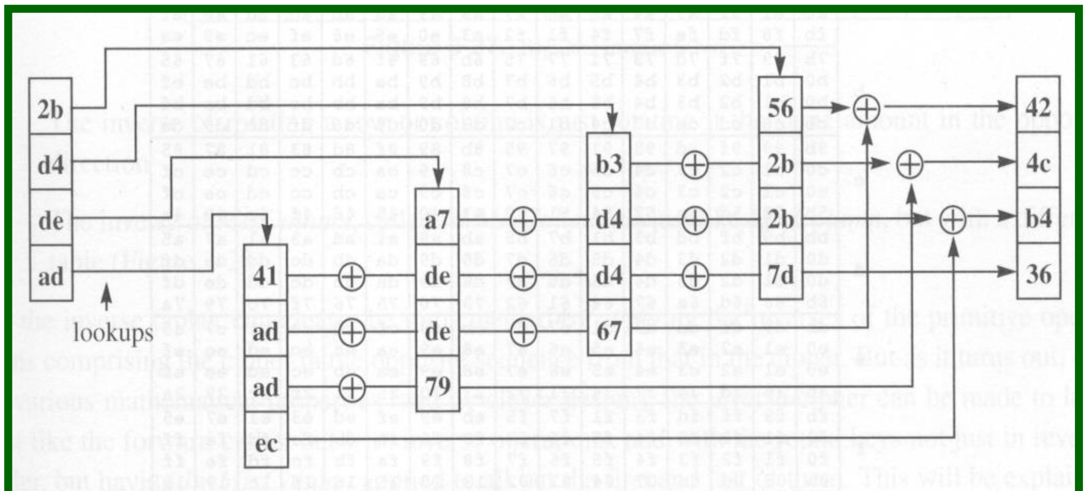
AES

- ShiftRows operation

$$\begin{bmatrix} s_{0.0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1.0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2.0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3.0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} ===> \begin{bmatrix} s_{0.0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1.1} & s_{1,2} & s_{1,3} & s_{1,0} \\ s_{2.2} & s_{2,3} & s_{2,0} & s_{2,1} \\ s_{3.3} & s_{3,0} & s_{3,1} & s_{3,2} \end{bmatrix}$$

AES

- MixColumn operation
- Column by column substitution using table lookup



right (low-order) nibble

left (high-order) nibble	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	00 00 00 00	02 01 01 03	04 02 02 06	06 03 03 05	08 04 04 0c	0a 05 05 0f	0c 06 06 0a	0e 07 07 09	10 08 08 18	12 09 09 1b	14 0a 0a 1e	16 0b 0b 1d	18 0c 0c 14	1a 0d 0d 17	1c 0e 0e 12	1e 0f 0f 11
1	20 10 10 30	22 11 11 33	24 12 12 36	26 13 13 35	28 14 14 3c	2a 15 15 3f	2c 16 16 3a	2e 17 17 39	30 18 18 28	32 19 19 2b	34 1a 1a 2e	36 1b 1b 2d	38 1c 1c 24	3a 1d 1d 27	3c 1e 1e 22	3e 1f 1f 21
2	40 20 20 60	42 21 21 63	44 22 22 66	46 23 23 65	48 24 24 6c	4a 25 25 6f	4c 26 26 6a	4e 27 27 69	50 28 28 78	52 29 29 7b	54 2a 2a 7e	56 2b 2b 7d	58 2c 2c 74	5a 2d 2d 77	5c 2e 2e 72	5e 2f 2f 71
3	60 30 30 50	62 31 31 53	64 32 32 56	66 33 33 55	68 34 34 5c	6a 35 35 5f	6c 36 36 5a	6e 37 37 59	70 38 38 48	72 39 39 4b	74 3a 3a 4e	76 3b 3b 4d	78 3c 3c 44	7a 3d 3d 47	7c 3e 3e 42	7e 3f 3f 41
4	80 40 40 c0	82 41 41 c3	84 42 42 c6	86 43 43 c5	88 44 44 cc	8a 45 45 cf	8c 46 46 ca	8e 47 47 c9	90 48 48 d8	92 49 49 db	94 4a 4a de	96 4b 4b dd	98 4c 4c d4	9a 4d 4d d7	9c 4e 4e d2	9e 4f 4f d1
5	a0 50 50 f0	a2 51 51 f3	a4 52 52 f6	a6 53 53 f5	a8 54 54 fc	aa 55 55 ff	ac 56 56 fa	ae 57 57 f9	b0 58 58 e8	b2 59 59 eb	b4 5a 5a ee	b6 5b 5b ed	b8 5c 5c e4	ba 5d 5d e7	bc 5e 5e e2	be 5f 5f e1
6	c0 60 60 a0	c2 61 61 a3	c4 62 62 a6	c6 63 63 a5	c8 64 64 ac	ca 65 65 af	cc 66 66 aa	ce 67 67 a9	d0 68 68 b8	d2 69 69 bb	d4 6a 6a be	d6 6b 6b bd	d8 6c 6c b4	da 6d 6d b7	dc 6e 6e b2	de 6f 6f b1
7	e0 70 70 90	e2 71 71 93	e4 72 72 96	e6 73 73 95	e8 74 74 9c	ea 75 75 9f	ec 76 76 9a	ee 77 77 99	f0 78 78 88	f2 79 79 8b	f4 7a 7a 8e	f6 7b 7b 8d	f8 7c 7c 84	fa 7d 7d 87	fc 7e 7e 82	fe 7f 7f 81
8	1b 80 80 9b	19 81 81 98	1f 82 82 9d	1d 83 83 9e	13 84 84 97	11 85 85 94	17 86 86 91	15 87 87 92	0b 88 88 83	09 89 89 80	0f 8a 8a 85	0d 8b 8b 86	03 8c 8c 8f	01 8d 8d 8c	07 8e 8e 89	05 8f 8f 8a
9	3b 90 90 ab	39 91 91 a8	3f 92 92 ad	3d 93 93 ae	33 94 94 a7	31 95 95 a4	37 96 96 a1	35 97 97 a2	2b 98 98 b3	29 99 99 b0	2f 9a 9a b5	2d 9b 9b b6	23 9c 9c bf	21 9d 9d bc	27 9e 9e b9	25 9f 9f ba
a	5b a0 a0 fb	59 a1 a1 f8	5f a2 a2 fd	5d a3 a3 fe	53 a4 a4 f7	51 a5 a5 f4	57 a6 a6 f1	55 a7 a7 f2	4b a8 a8 e3	49 a9 a9 e0	4f aa aa e5	4d ab ab e6	43 ac ac ef	41 ad ad ec	47 ae ae e9	45 af af ea
b	7b b0 b0 cb	79 b1 b1 c8	7f b2 b2 cd	7d b3 b3 ce	73 b4 b4 c7	71 b5 b5 c4	77 b6 b6 c1	75 b7 b7 c2	6b b8 b8 d3	69 b9 b9 d0	6f ba ba d5	6d bb bb d6	63 bc bc df	61 bd bd dc	67 be be d9	65 bf bf da
c	9b c0 c0 5b	99 c1 c1 58	9f c2 c2 5d	9d c3 c3 5e	93 c4 c4 57	91 c5 c5 54	97 c6 c6 51	95 c7 c7 52	8b c8 c8 43	89 c9 c9 40	8f ca ca 45	8d cb cb 46	83 cc cc 4f	81 cd cd 4c	87 ce ce 49	85 cf cf 4a
d	bb d0 d0 6b	b9 d1 d1 68	bf d2 d2 6d	bd d3 d3 6e	b3 d4 d4 67	b1 d5 d5 64	b7 d6 d6 61	b5 d7 d7 62	ab d8 d8 73	a9 d9 d9 70	af da da 75	ad db db 76	a3 dc dc 7f	a1 dd dd 7c	a7 de de 79	a5 df df 7a
e	db e0 e0 3b	d9 e1 e1 38	df e2 e2 3d	dd e3 e3 3e	d3 e4 e4 37	d1 e5 e5 34	d7 e6 e6 31	d5 e7 e7 32	cb e8 e8 23	c9 e9 e9 20	cf ea ea 25	cd eb eb 26	c3 ec ec 2f	c1 ed ed 2c	c7 ee ee 29	c5 ef ef 2a
f	fb f0 f0 0b	f9 f1 f1 08	ff f2 f2 0d	fd f3 f3 0e	f3 f4 f4 07	f1 f5 f5 04	f7 f6 f6 01	f5 f7 f7 02	eb f8 f8 13	e9 f9 f9 10	ef fa fa 15	ed fb fb 16	e3 fc fc 1f	e1 fd fd 1c	e7 fe fe 19	e5 ff ff 1a

AES

- Decryption: perform the inverse of each operation in the opposite order and use the rounds keys in reverse order
- Each of the basic operations are reversible

Inverse Rounds (decryption)

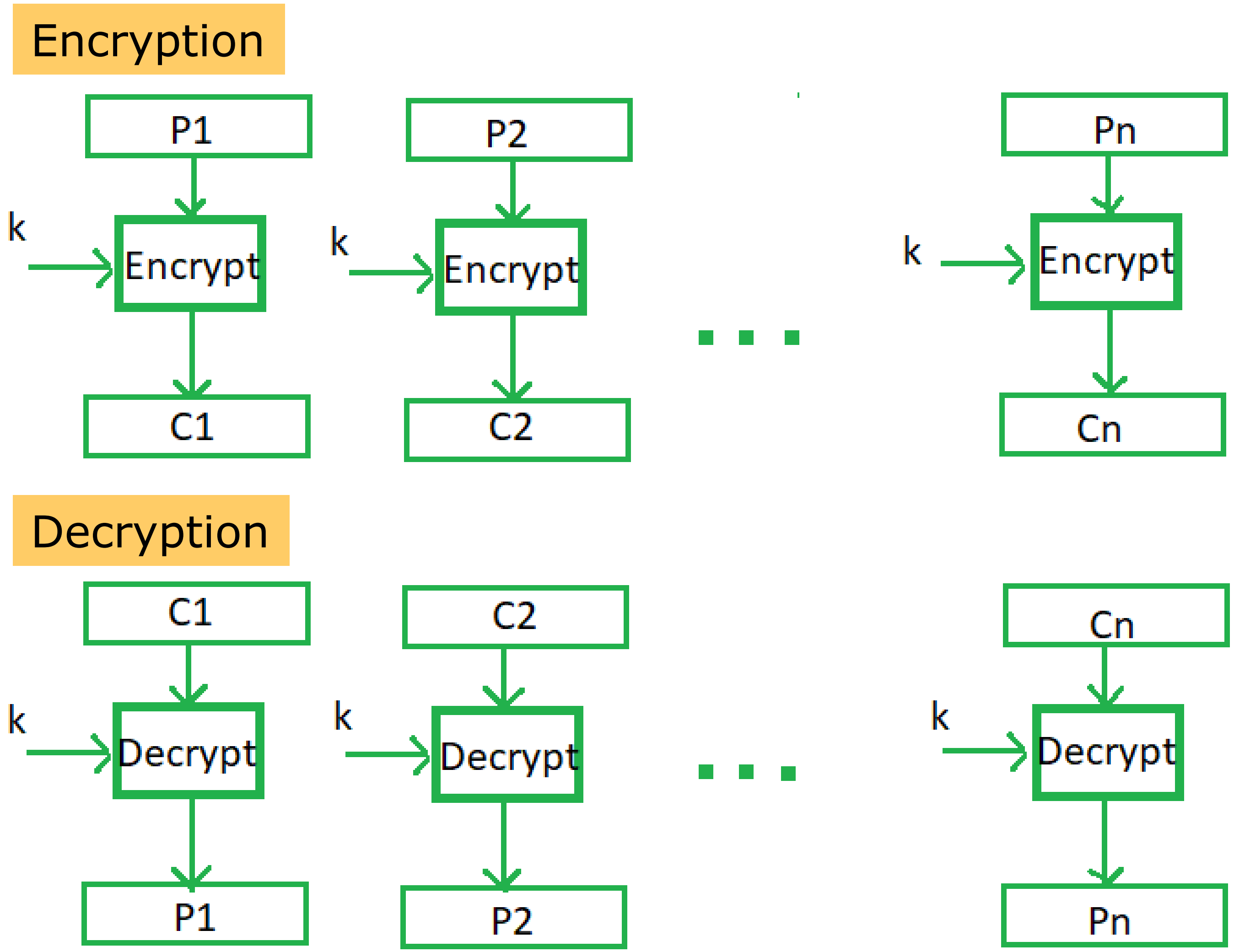
1. Each octet of the state has the inverse S-box applied to it
2. Row 1 of the state is rotated right 1 column,
   Row 2 of the state is rotated right ($2+\lfloor N_b/8 \rfloor$) column,
   Row 3 of the state is rotated right ($3+\lfloor N_b/8 \rfloor$) column
3. Each column of the state has inverse MixColumn applied to it (round N_r omits this operation)

Cipher Block Modes of Operation

- ECB (Electronic Code Book)
  - Each block of plaintext is encrypted independently.
  - A simple substitution : $C_i = E_k(P_i)$, $P_i = D_k(C_i)$
  - Subject to block replay attack

Cipher Block Modes of Operation

- ECB mode



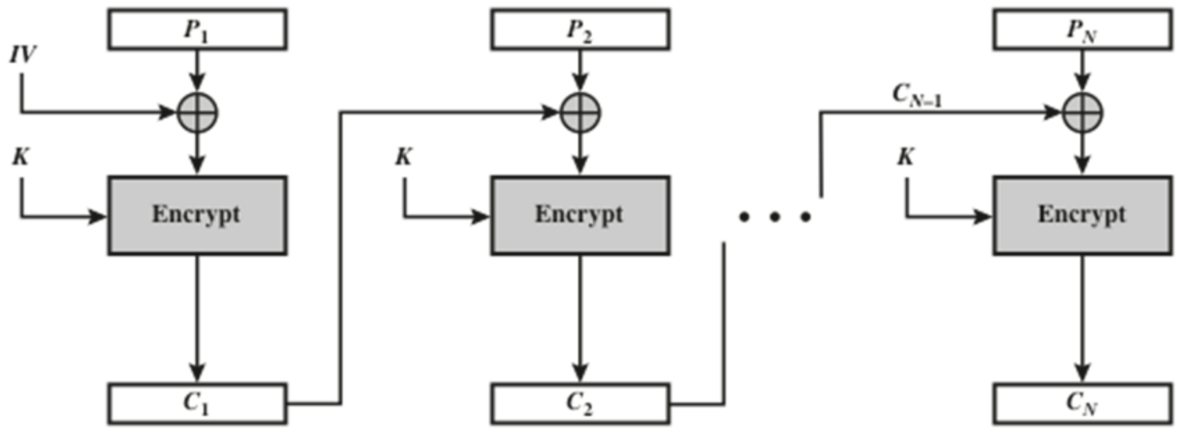
Cipher Block Modes of Operation

- CBC (Cipher Block Chaining)
  - Adds a feedback mechanism to the cipher
  - Plaintext patterns are concealed by XORing this block of P with the previous block of C :

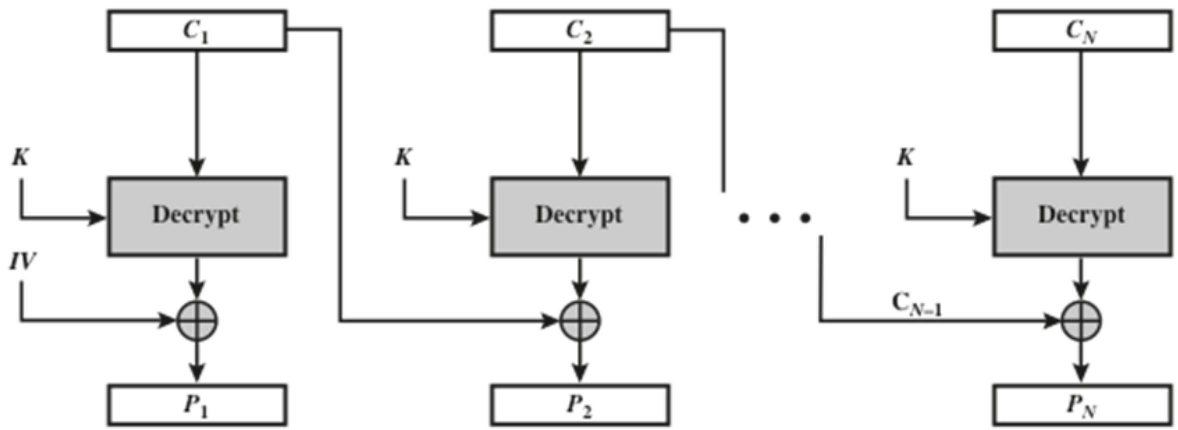
    $C_i = E_k(P_i \oplus C_{i-1}), \quad P_i = D_k(C_i) \oplus C_{i-1}$
  - Requires an IV (Initialization vector) : $C_1 = E_k(P_1 \oplus IV)$
  - Resistant against block replay attack

Cipher Block Modes of Operation

- CBC (Cipher Block Chaining)



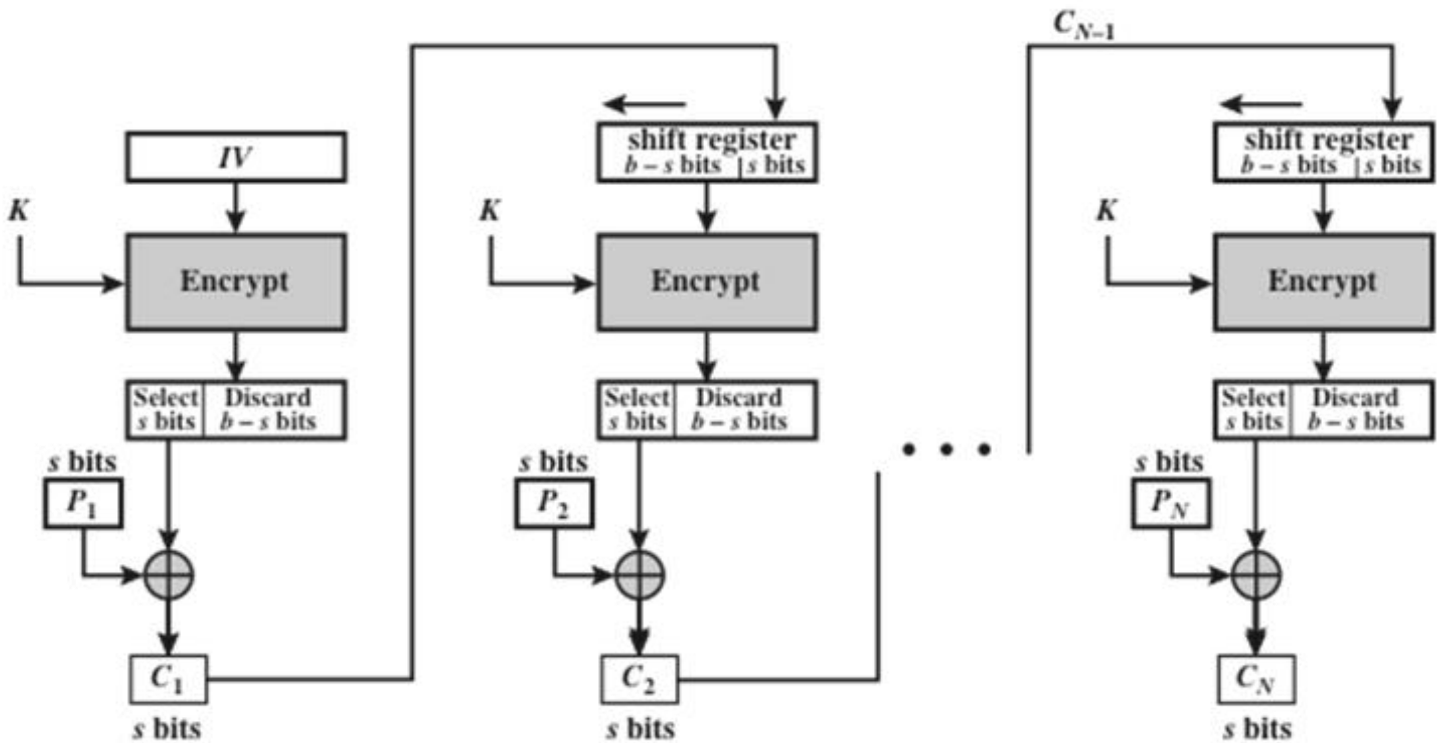
(a) Encryption



(b) Decryption

Cipher Block Modes of Operation

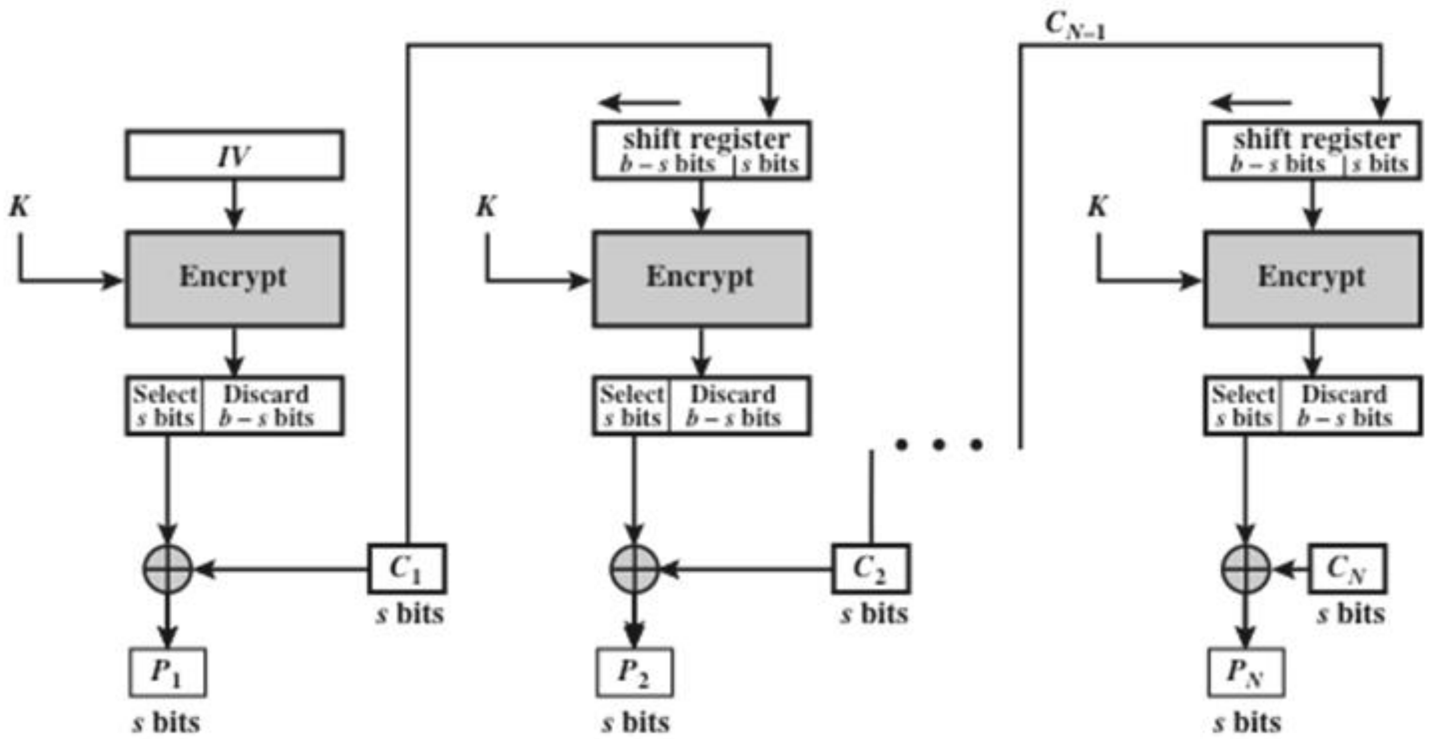
CFB (Cipher FeedBack)



(a) Encryption

Cipher Block Modes of Operation

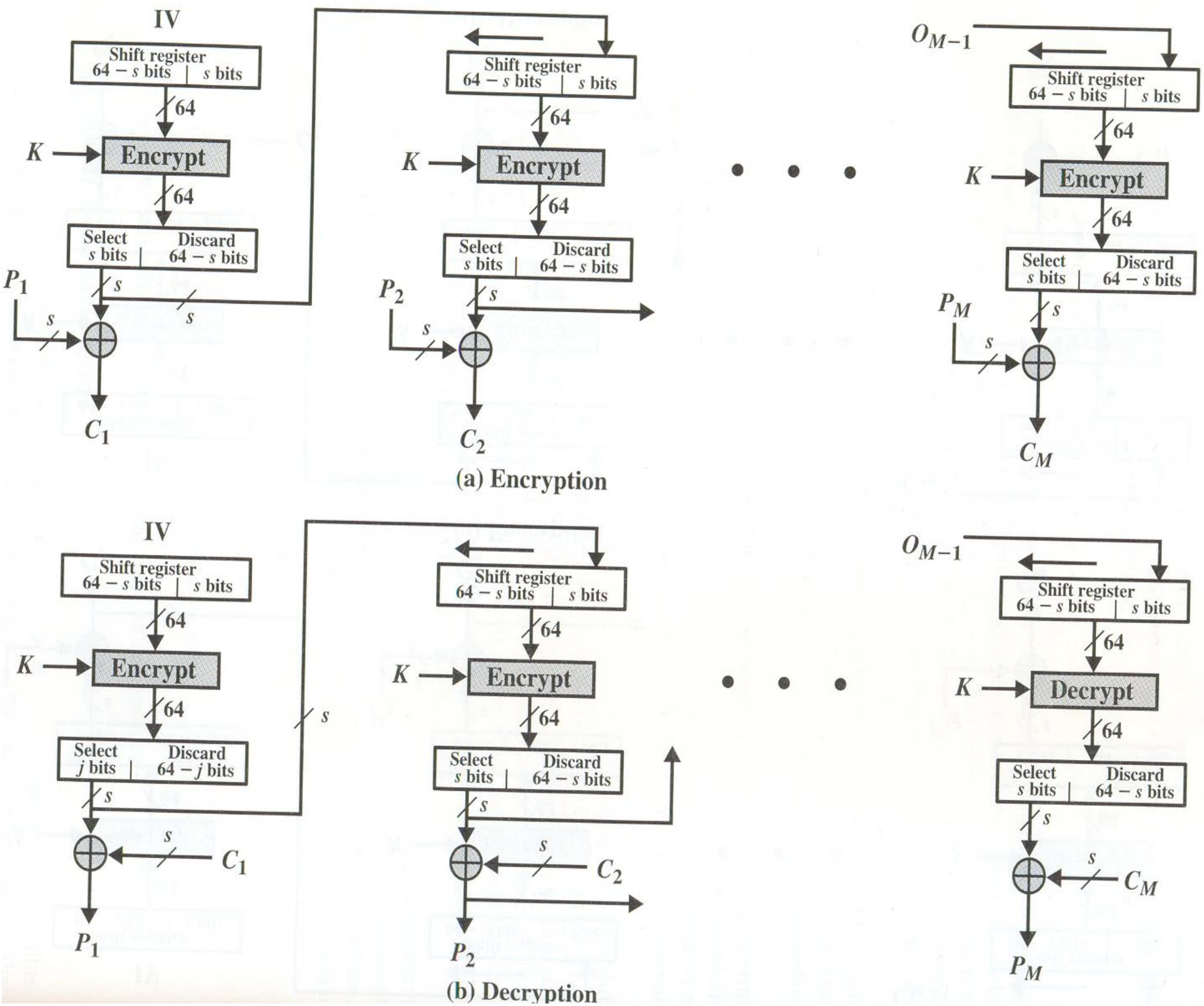
CFB (Cipher FeedBack)



(b) Decryption

Cipher Block Modes of Operation

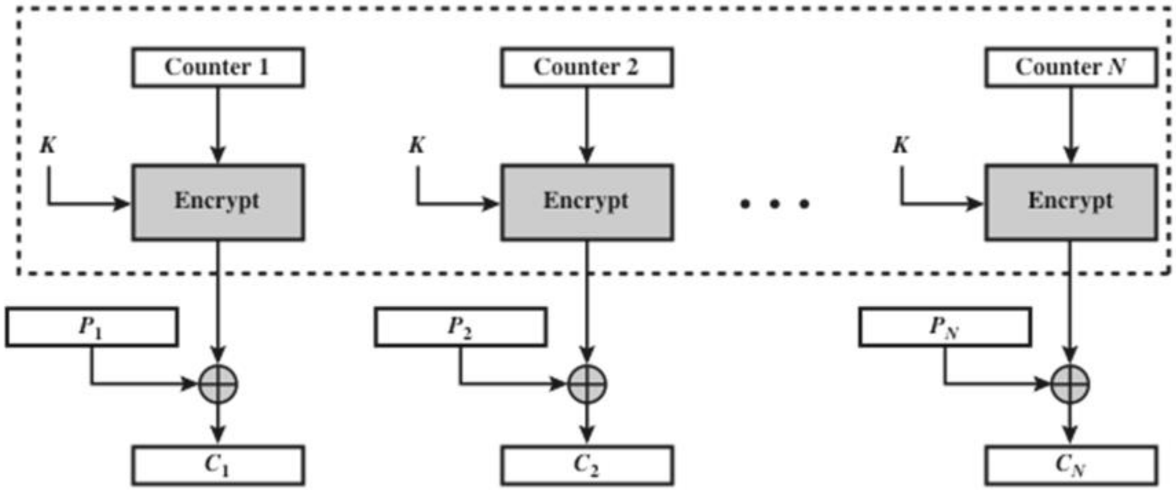
OFB (Output FeedBack)



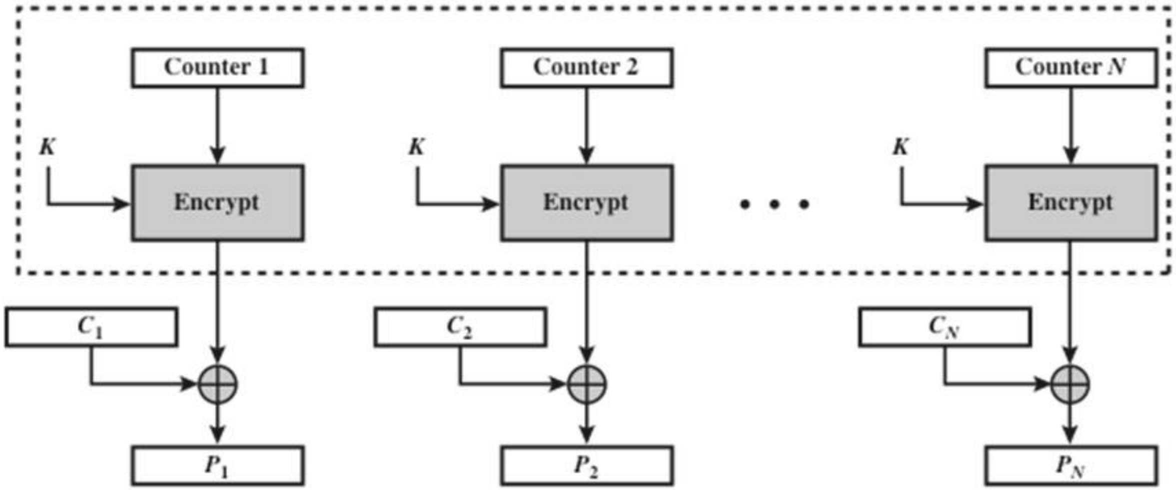
Cipher Block Modes of Operation

CTR (Counter) mode

- Different counter value is used to encrypt each plaintext
- Used in ATM and IPSec
- Advantages: efficient and ciphertext block can be processed in random-access pattern



(a) Encryption



(b) Decryption

Random Number Generation

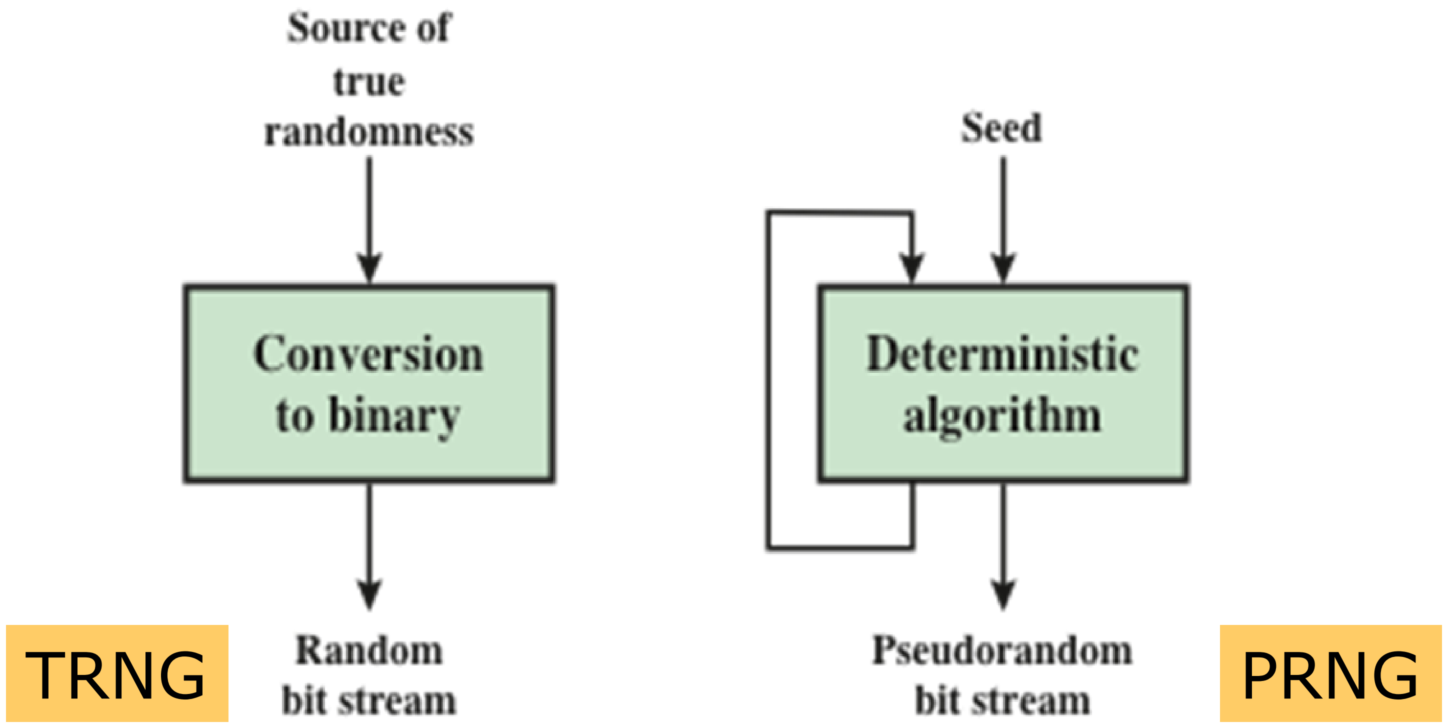
- Many security algorithms make use of random numbers (nonces)
  - Generation of keys in public-key encryption algorithms like RSA and DH algorithms
  - OTP (One-time password)
  - Generation of a symmetric key for use as a temporary session key; used in a number of networking applications such as TLS, Wi-Fi, e-mail security, and IPsec
  - In key distribution scenarios, random numbers are used for handshaking to prevent replay attacks: Kerberos, SSL

Random Number Generation

- Requirements
  - Randomness
    - The distribution of bits in the sequence should be uniform
    - Frequency of occurrence of ones and zeros should be approximately the same
  - Unpredictability
    - No one subsequence in the sequence can be inferred from the others
    - an opponent should not be able to predict future elements of the sequence based on earlier elements

Random Number Generation

- True-random (TRNG) and Pseudo-random(PRNG) number generators



Placement of Encryption Function

- Networks are vulnerable to eavesdropping
- Encryption is the effective way to protect from eavesdropping
  - Link level encryption
  - End-to-end encryption

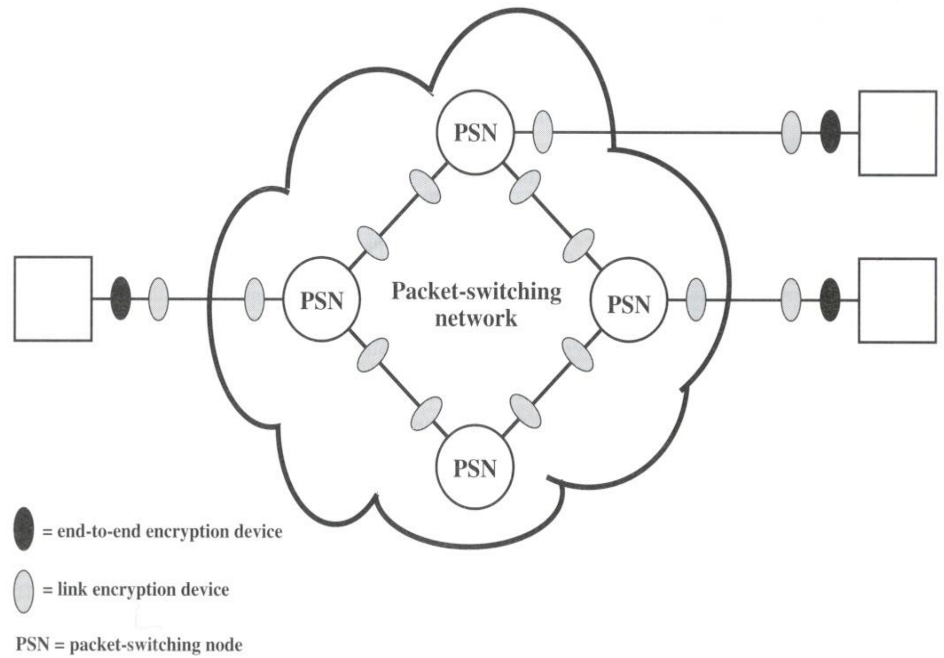
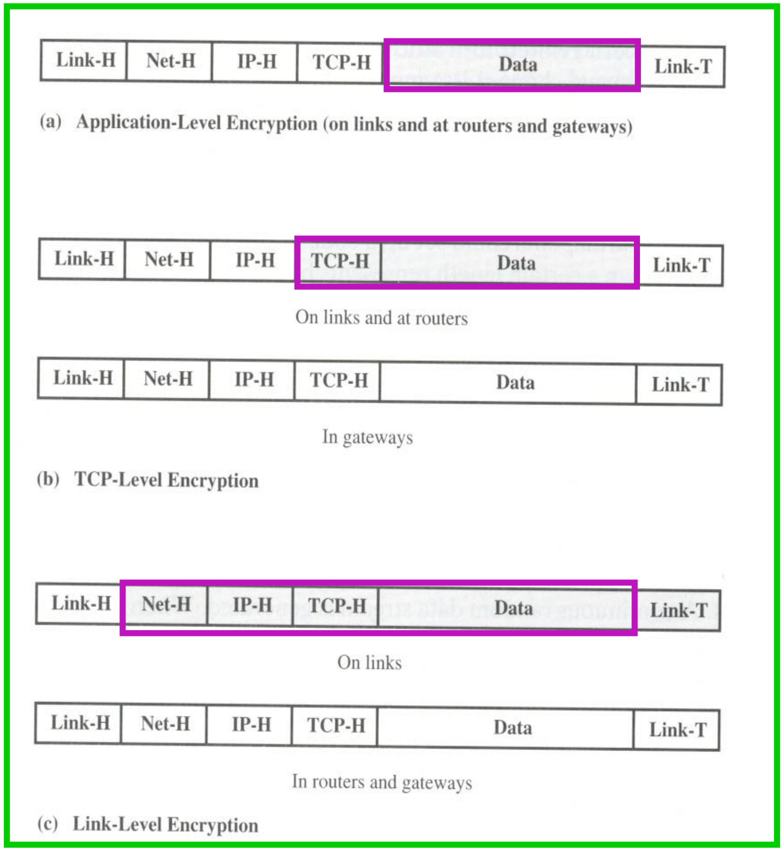


Figure 5.2 Encryption Across a Packet-Switching Network.

Placement of Encryption Function

- Link level encryption
  - Each pair of nodes must share a unique key
  - The packet must be decrypted at each node for routing
- End-to-end encryption
  - User data is encrypted, but packet header is delivered in the clear
  - Provides a degree of authentication



Traffic Analysis

- Traffic analysis attack
  - Message patterns, message quantity
  - Identifiers of partners
  - Frequency of communications
  - Etc.
- Counter measure
  - Traffic padding
  - Tunneling : end-point concealing

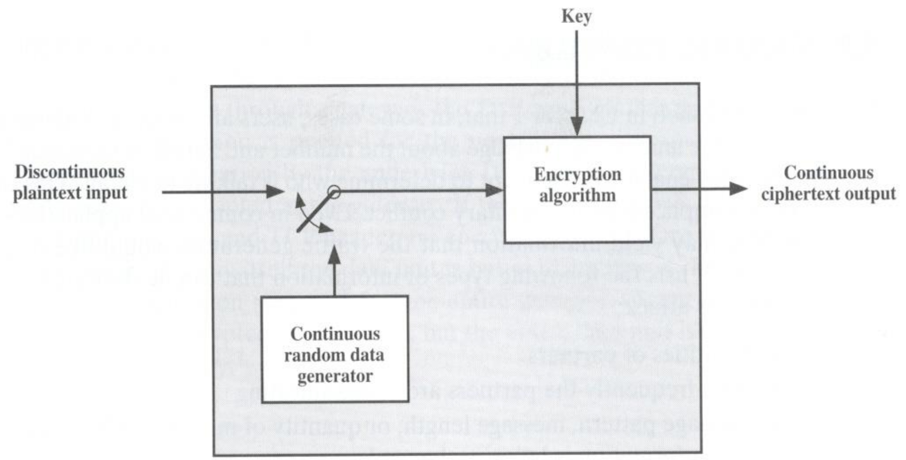
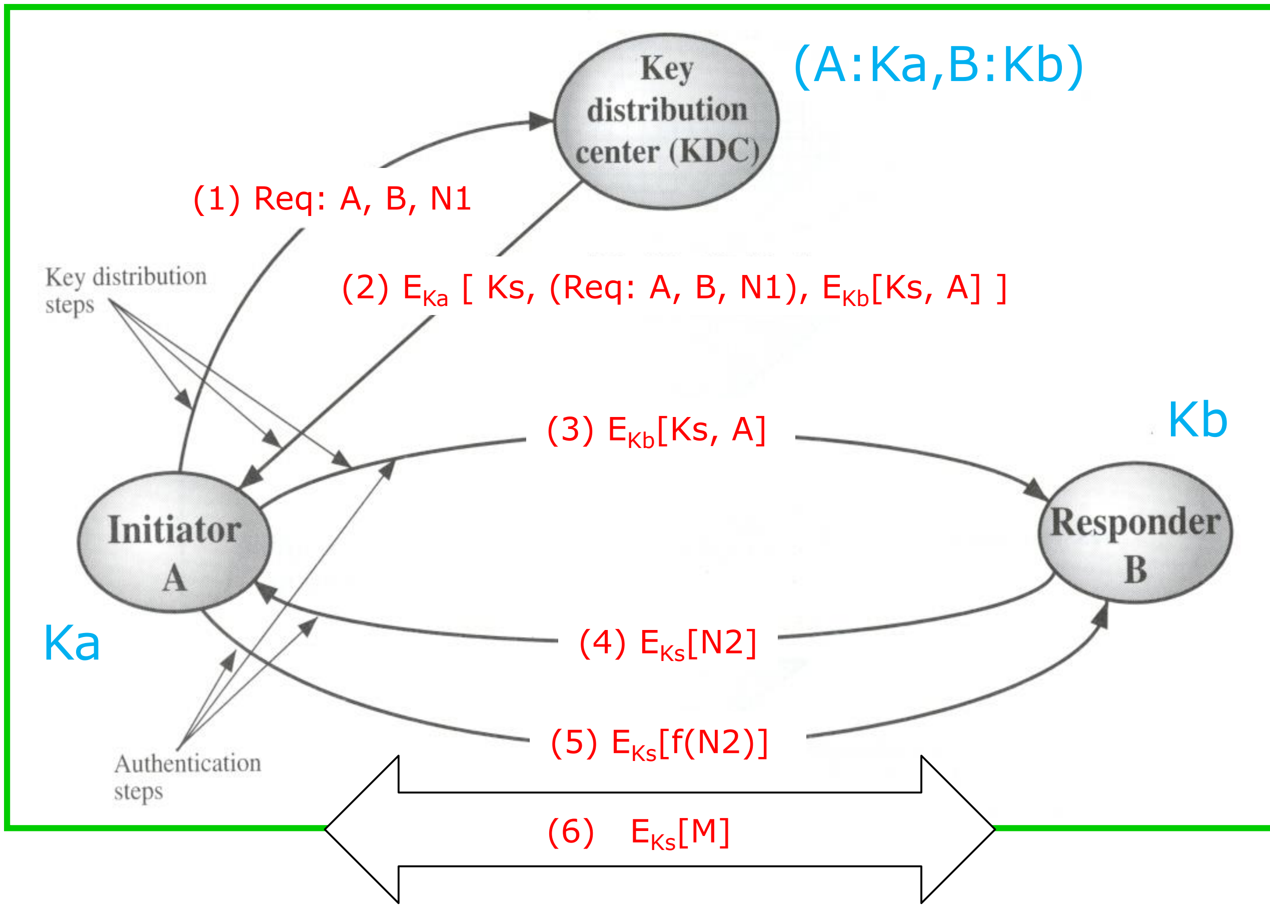


Figure 5.6 Traffic-Padding Encryption Device.

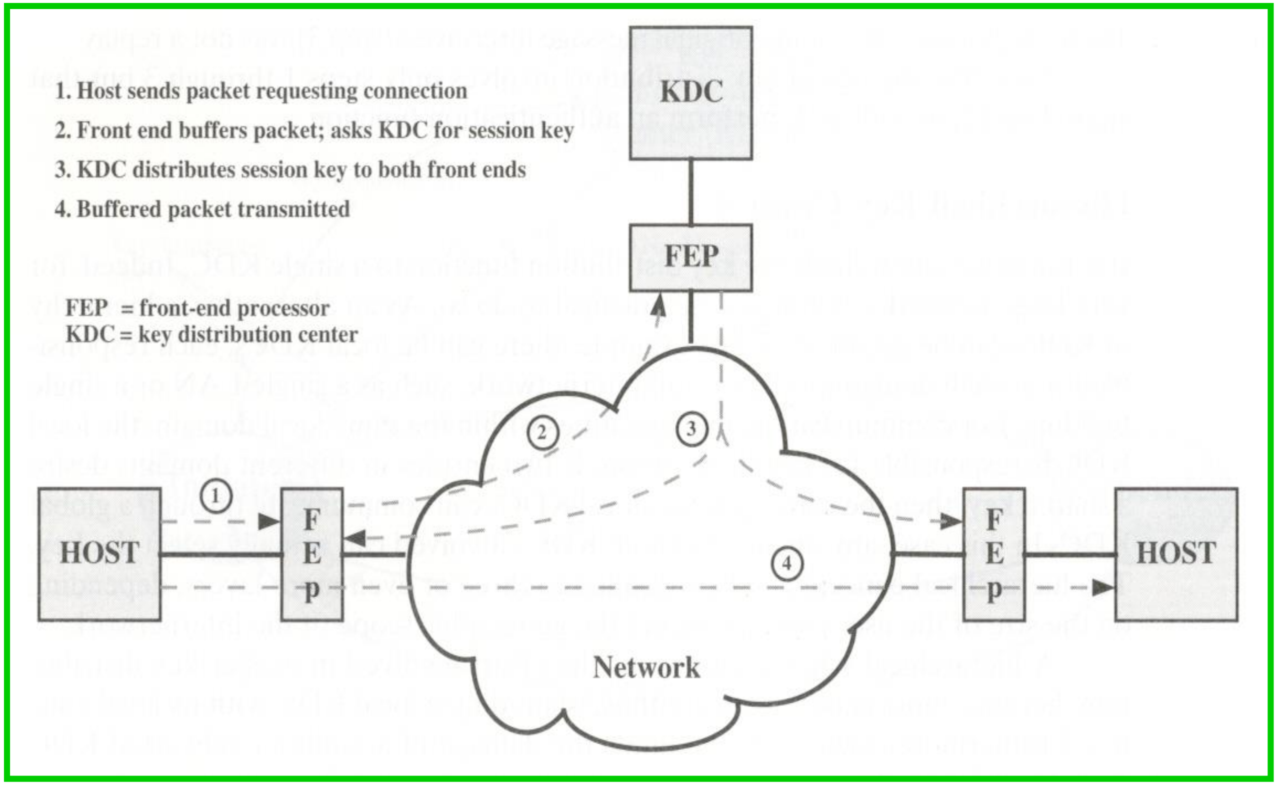
Key Distribution

- Key distribution using key distribution center (KDC)
- For large networks, a hierarchy of KDCs may be used



Key Distribution

- Transparent Key Distribution
  - In a end-to-end encryption using a connection-oriented protocol



Key Distribution

- Decentralized Key Distribution
  - Shared master secret b/w peers
  - Decentralized key distribution requires n(n-1)/2 master keys for a configuration with n end systems