BLM5102 Computer Systems and Network Security

Prof. Dr. Hasan Hüseyin BALIK

(9th Week)

Outline

- 3. Cryptographic Algorithms
  - 3.1. Cryptographic Tools
  - 3.2. Symmetric Encryption and Message Confidentiality
  - 3.3. Public-Key Cryptography and Message Authentication

3.2 Symmetric Encryption and Message Confidentiality

3.2. Outline

- Symmetric Encryption and Message Confidentiality
- Data Encryption Standard
- Advanced Encryption Standard
- Stream Ciphers and RC4
- Cipher Block Modes of Operation

Symmetric Encryption

- Also referred to as:
  - Conventional encryption
  - Secret-key or single-key encryption
- Only alternative before public-key encryption in 1970’s
  - Still most widely used alternative
- Has five ingredients:
  - Plaintext
  - Encryption algorithm
  - Secret key
  - Ciphertext
  - Decryption algorithm

Cryptography

Classified along three independent dimensions:

The type of operations used for transforming plaintext to ciphertext

- Substitution – each element in the plaintext is mapped into another element
- Transposition – elements in plaintext are rearranged

The number of keys used

- Sender and receiver use same key – symmetric
- Sender and receiver each use a different key - asymmetric

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

Table 20.1 Types of Attacks on Encrypted Messages

Type of Attack	Known to Cryptanalyst
Ciphertext only	•Encryption algorithm •Ciphertext to be decoded
Known plaintext	•Encryption algorithm •Ciphertext to be decoded •One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	•Encryption algorithm •Ciphertext to be decoded •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext 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
- Usually very difficult to estimate the amount of effort required to break
- Can estimate time/cost of a brute-force attack

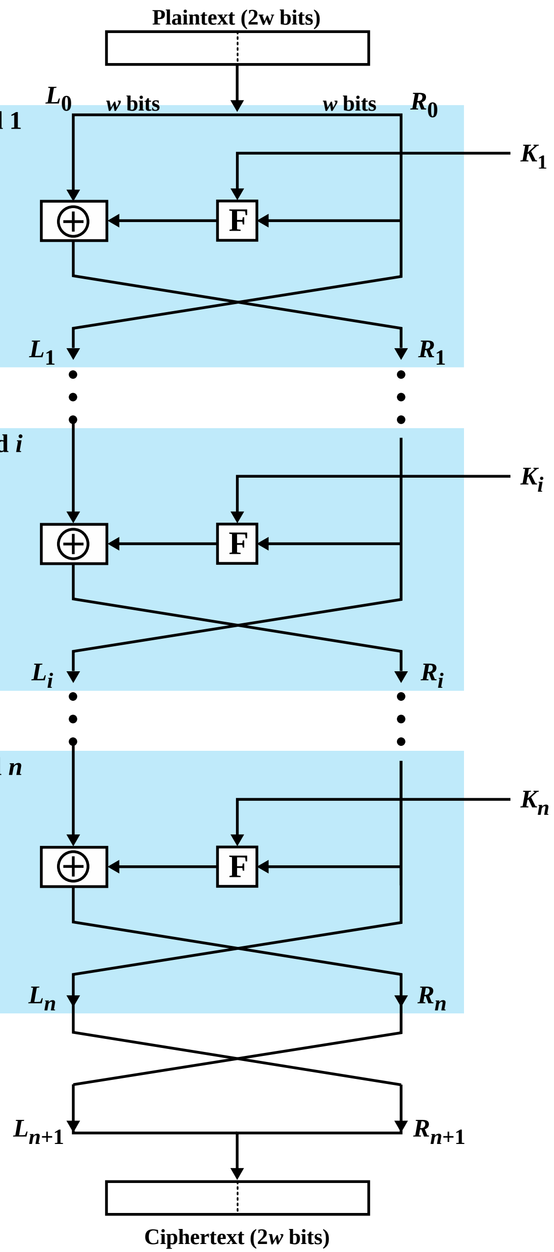
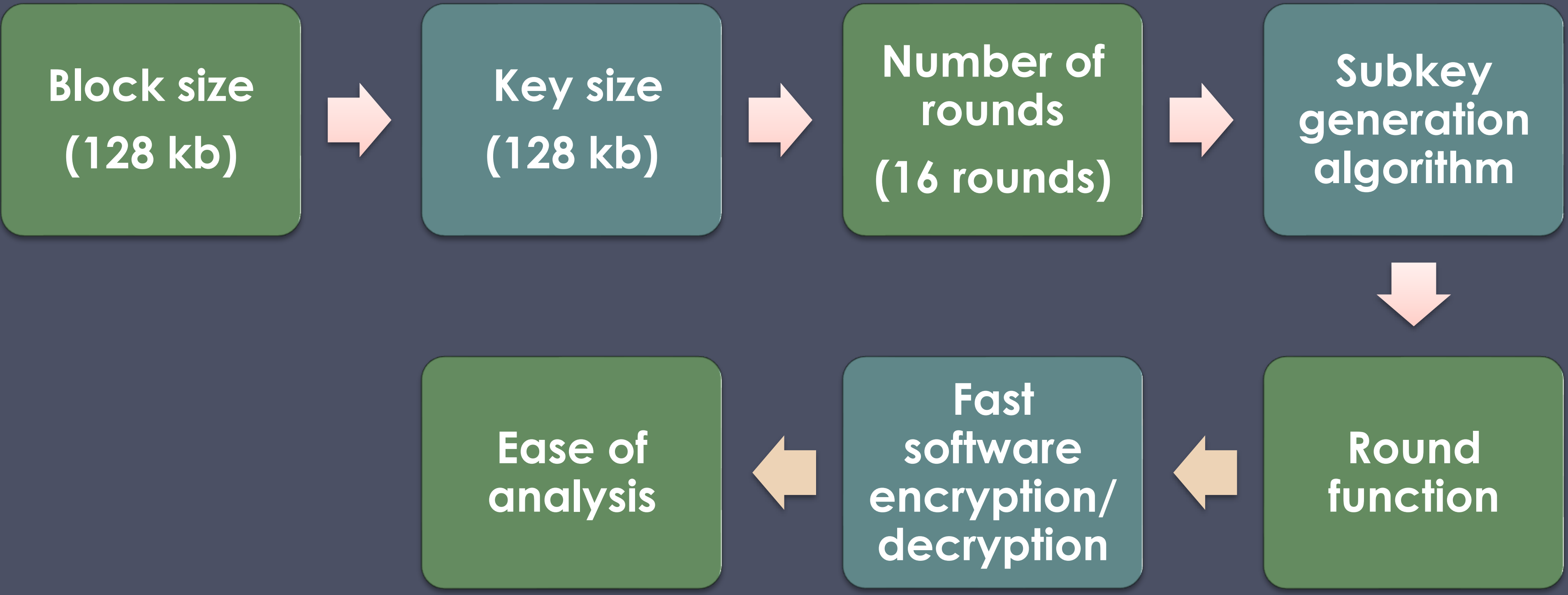


Figure 20.1 Classical Feistel Network

Block Cipher Structure

- Symmetric block cipher consists of:
  - A sequence of rounds
  - With substitutions and permutations controlled by key
- Parameters and design features:



Data Encryption Standard (DES)

- Most widely used encryption scheme
- Adopted in 1977 by National Bureau of Standards (Now NIST)
- FIPS PUB 46 *(Data Encryption Standard*, January 1977).
- Algorithm is referred to as the Data Encryption Algorithm (DEA)
- The plaintext is 64 bits in length and the key is 56 bits in length
- Minor variation of the Feistel network

Triple DES (3DES) was first standardized for use in financial applications in ANSI standard X9.17 in 1985. 3DES was incorporated as part of the Data Encryption Standard in 1999, with the publication of FIPS PUB 46-3

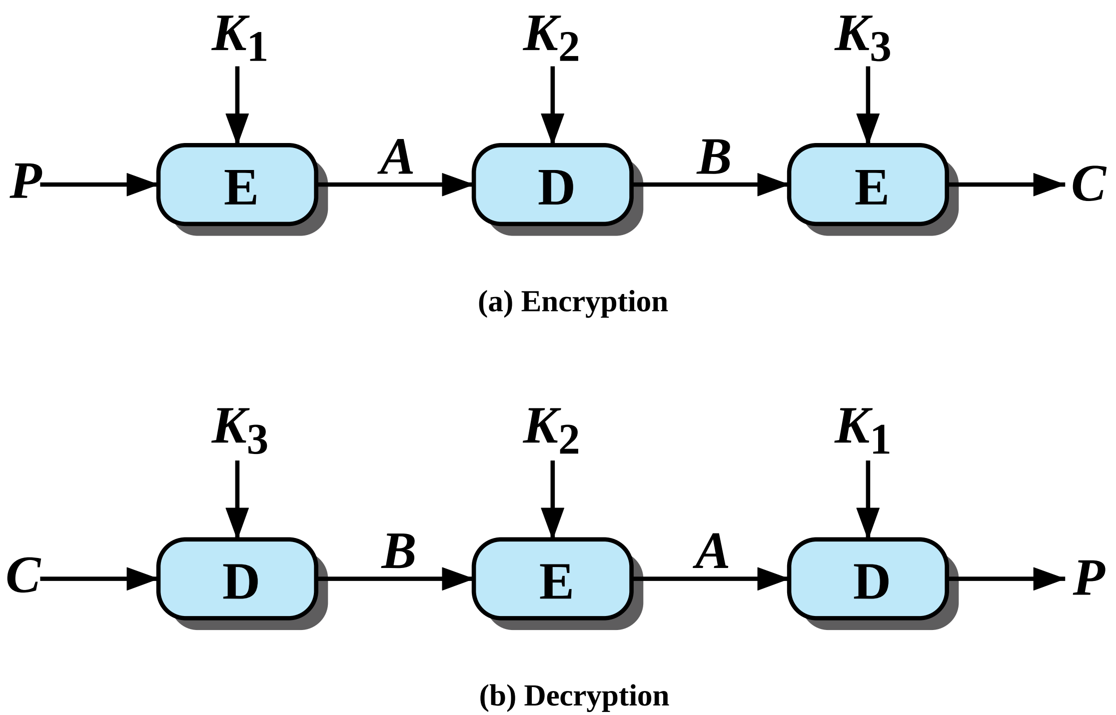


Figure 20.2 Triple DES

Advanced Encryption Standard (AES)

Needed a replacement for 3DES

- 3DES was not reasonable for long term use

NIST called for proposals for a new AES in 1997

- Should have a security strength equal to or better than 3DES
- Significantly improved efficiency
- Symmetric block cipher
- 128 bit data and 128/192/256 bit keys

Selected Rijndael in November 2001

- In a first round of evaluation, 15 proposed algorithms were accepted
- A second round narrowed the field to 5 algorithm
- Published as FIPS 197

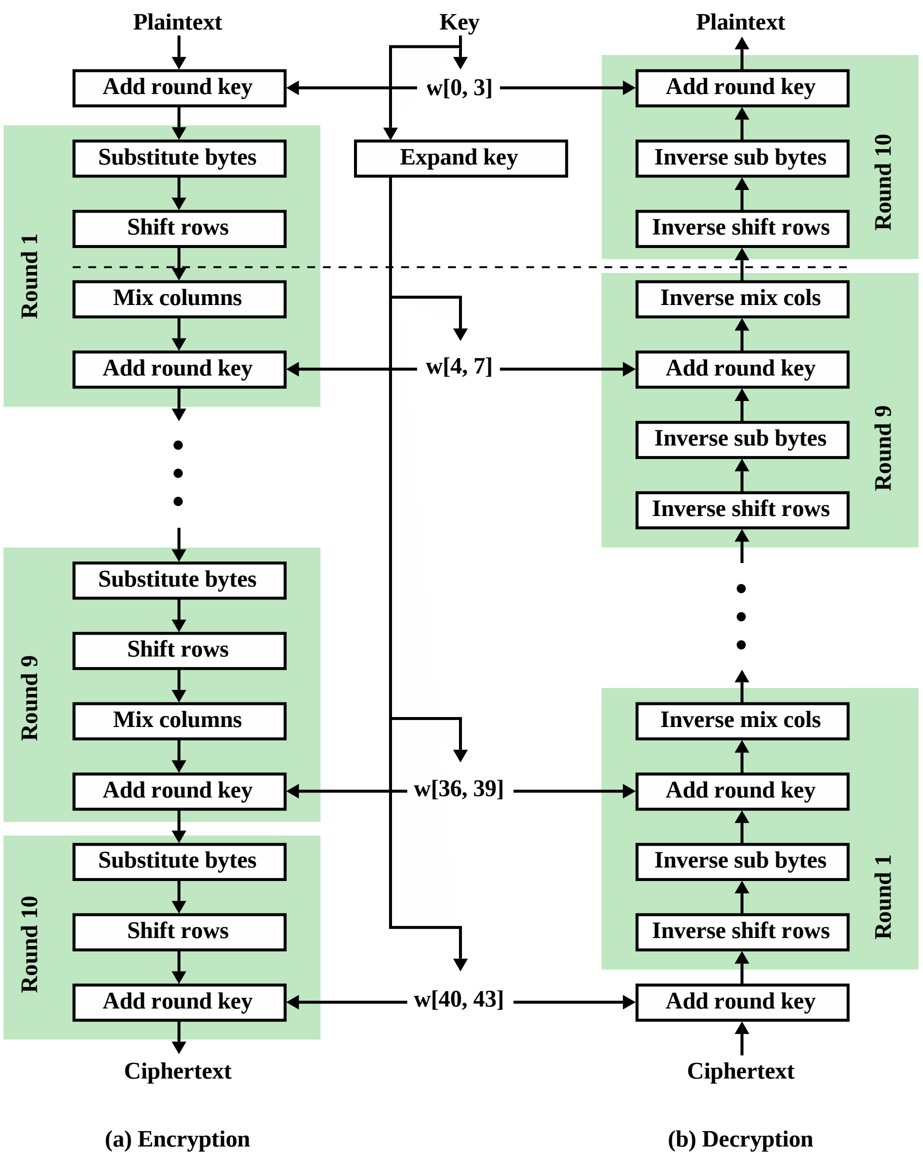


Figure 20.3 AES Encryption and Decryption

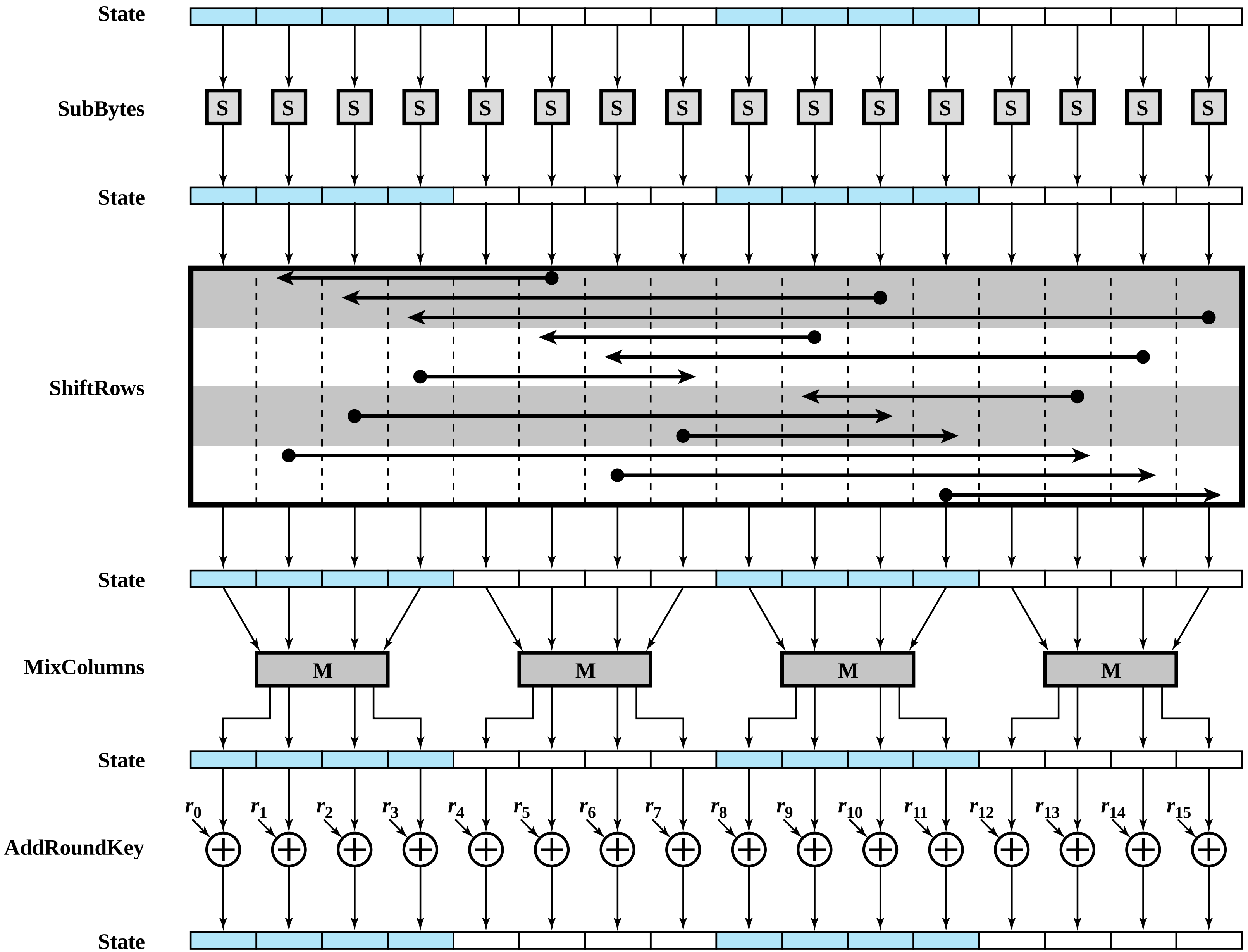


Figure 20.4 AES Encryption Round

Table 20.2 AES S-Boxes

(a) S-box

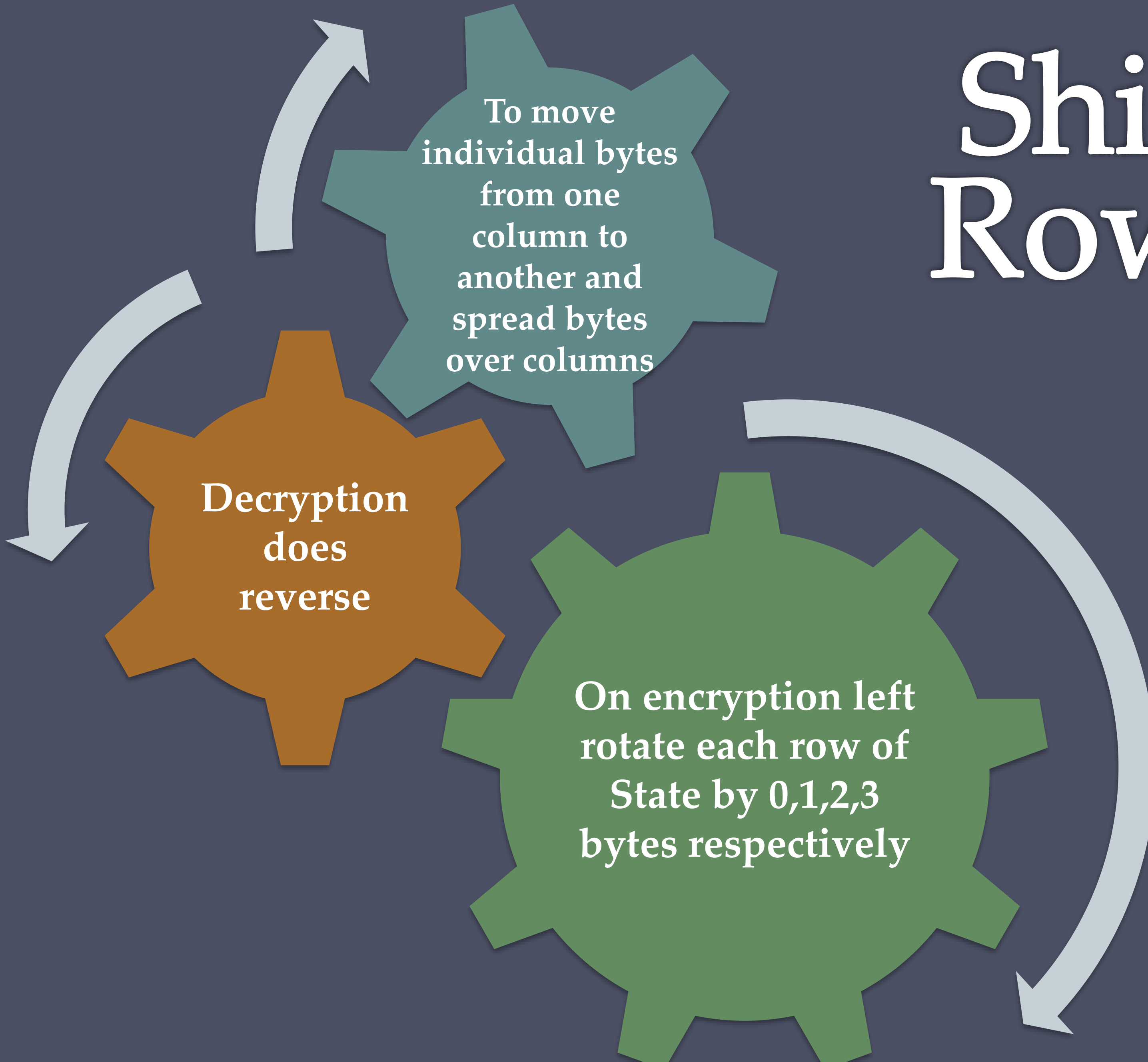
		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	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

Table 20.2 AES S-Boxes

(b) Inverse 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

Shift Rows


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

Mix Columns and Add Key

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

Stream Ciphers

Processes input elements continuously

Key input to a pseudorandom bit generator

- Produces stream of random like numbers
- Unpredictable without knowing input key
- XOR keystream output with plaintext bytes

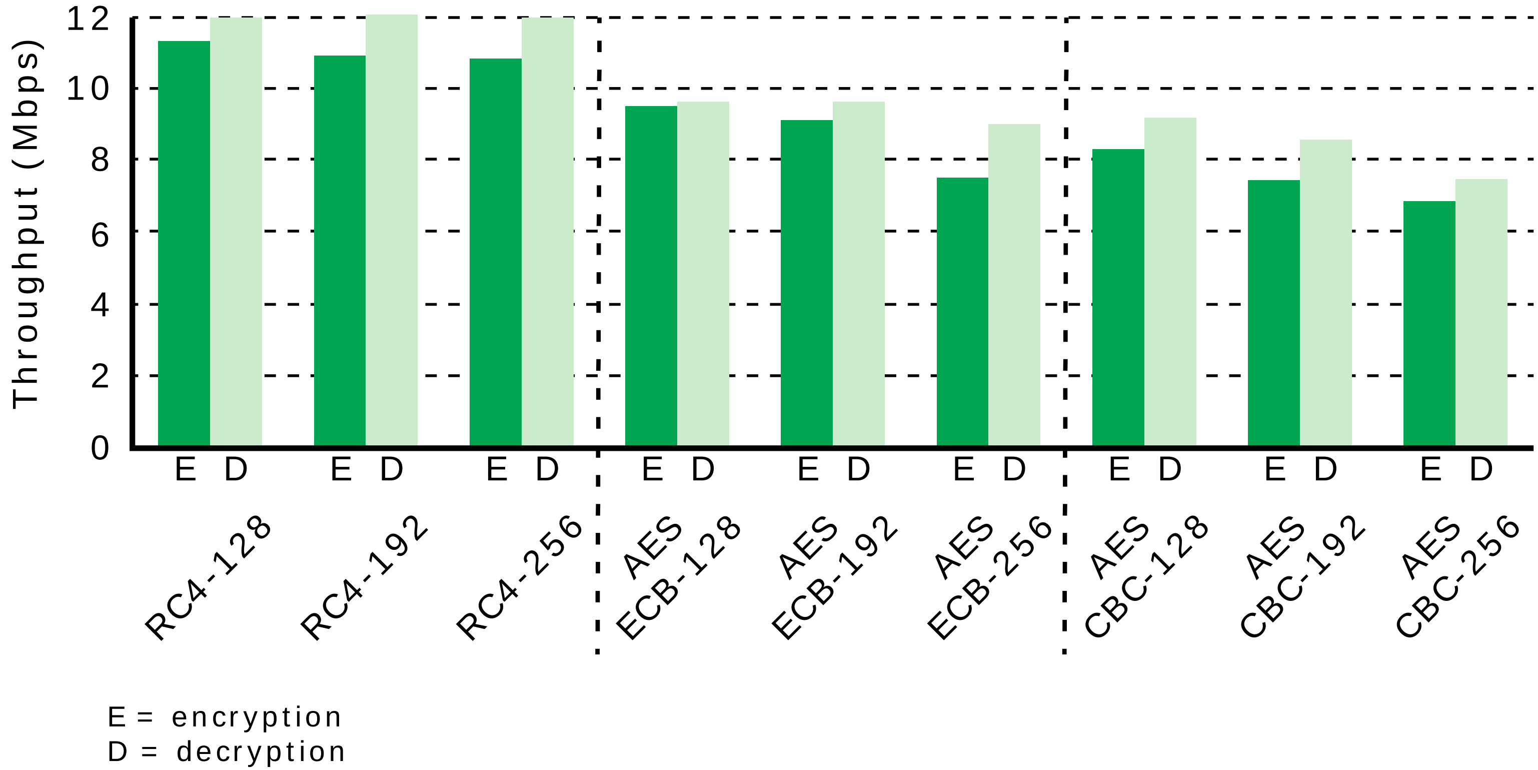


Figure 20.5 Performance Comparison of Symmetric Ciphers on a 3-GHz Processor

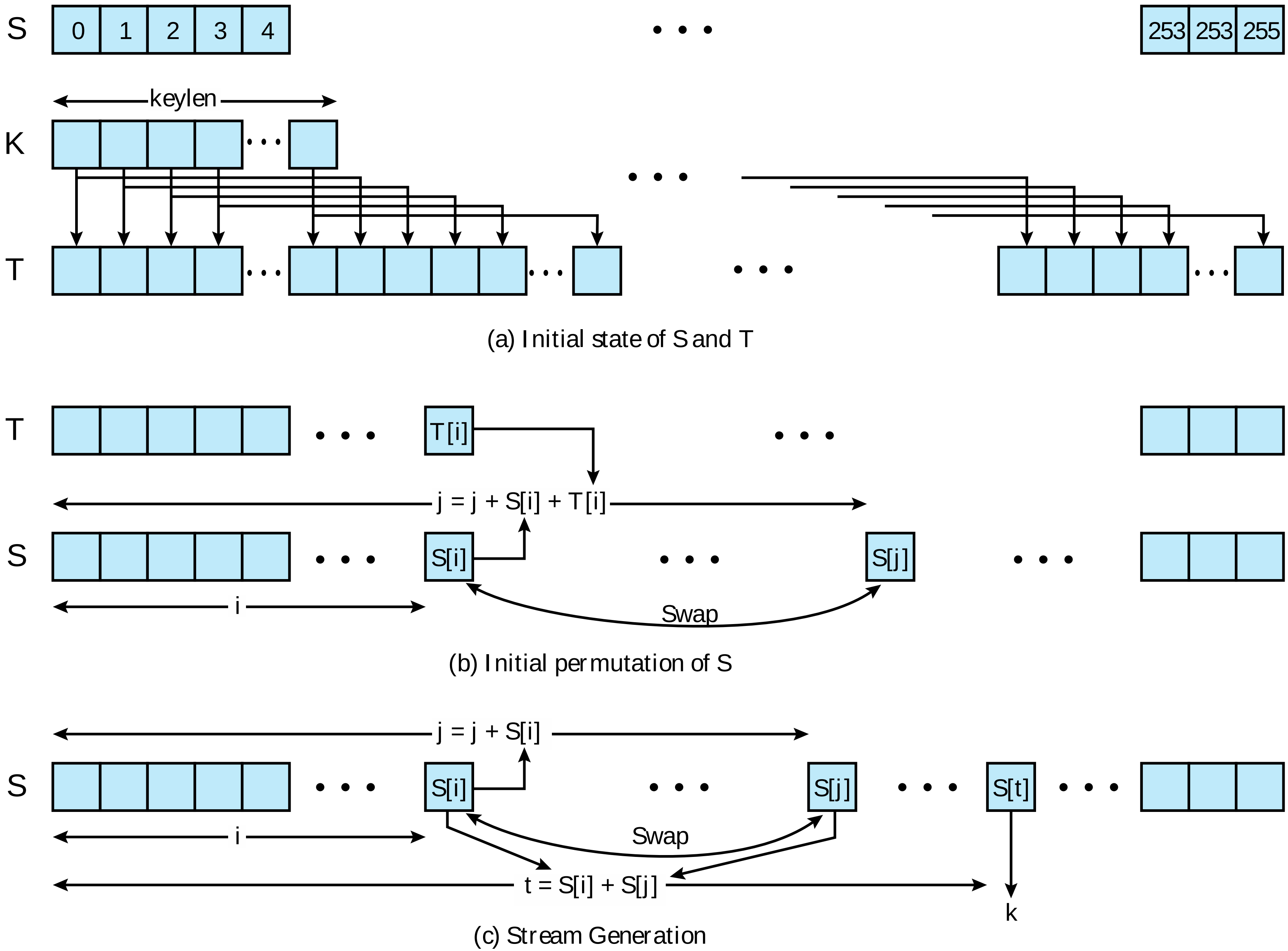


Figure 20.6 RC4

Block Cipher Modes of Operation

Mode	Description	Typical Application
Electronic Codebook (ECB)	Each block of 64 plaintext bits is encoded independently using the same key.	•Secure transmission of single values (e.g., an encryption key)
Cipher Block Chaining (CBC)	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
Cipher Feedback (CFB)	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
Output Feedback (OFB)	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 communication)
Counter (CTR)	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* bits 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

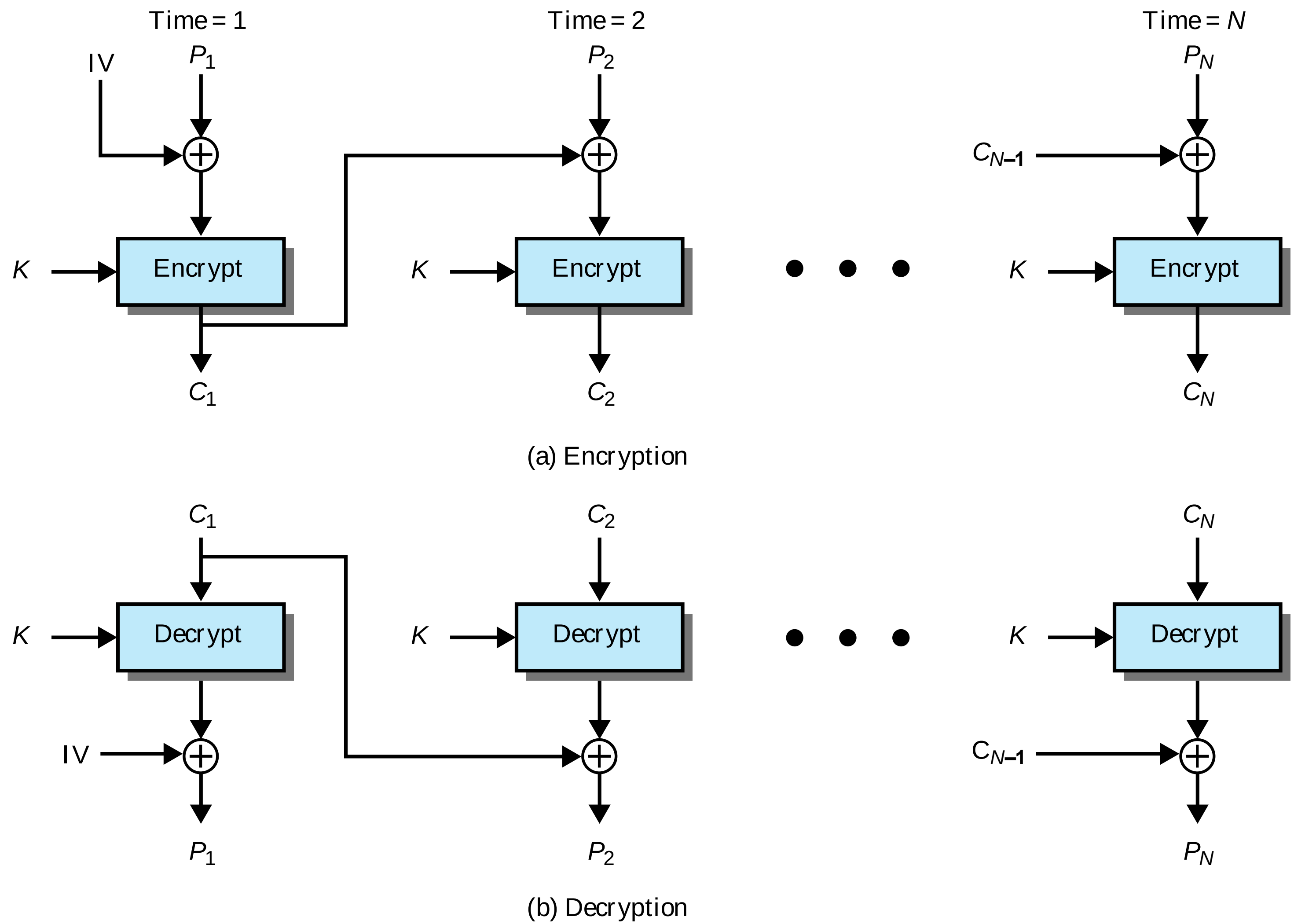


Figure 20.7 Cipher Block Chaining (CBC) Mode

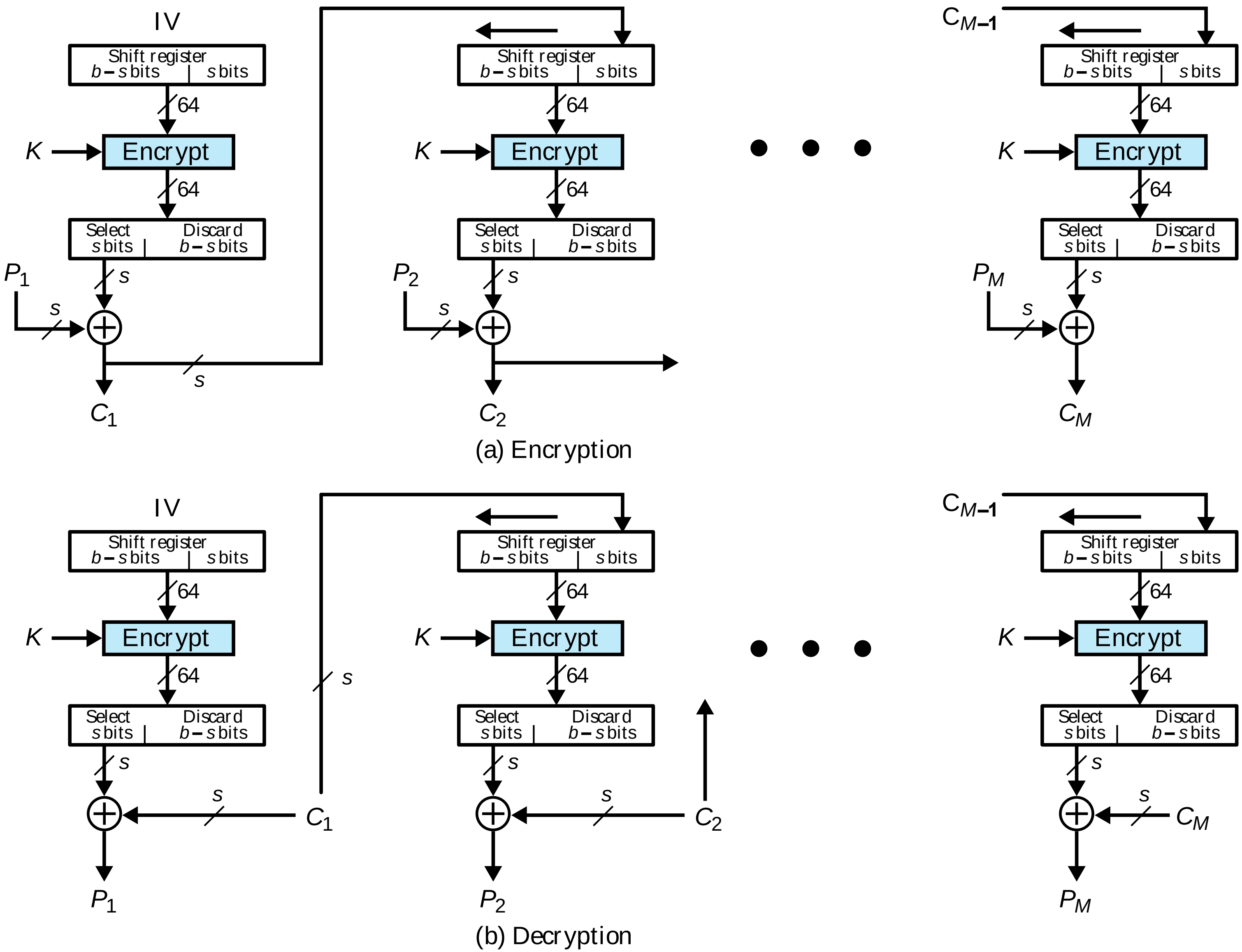


Figure 20.8 s-bit Cipher Feedback (CFB) Mode

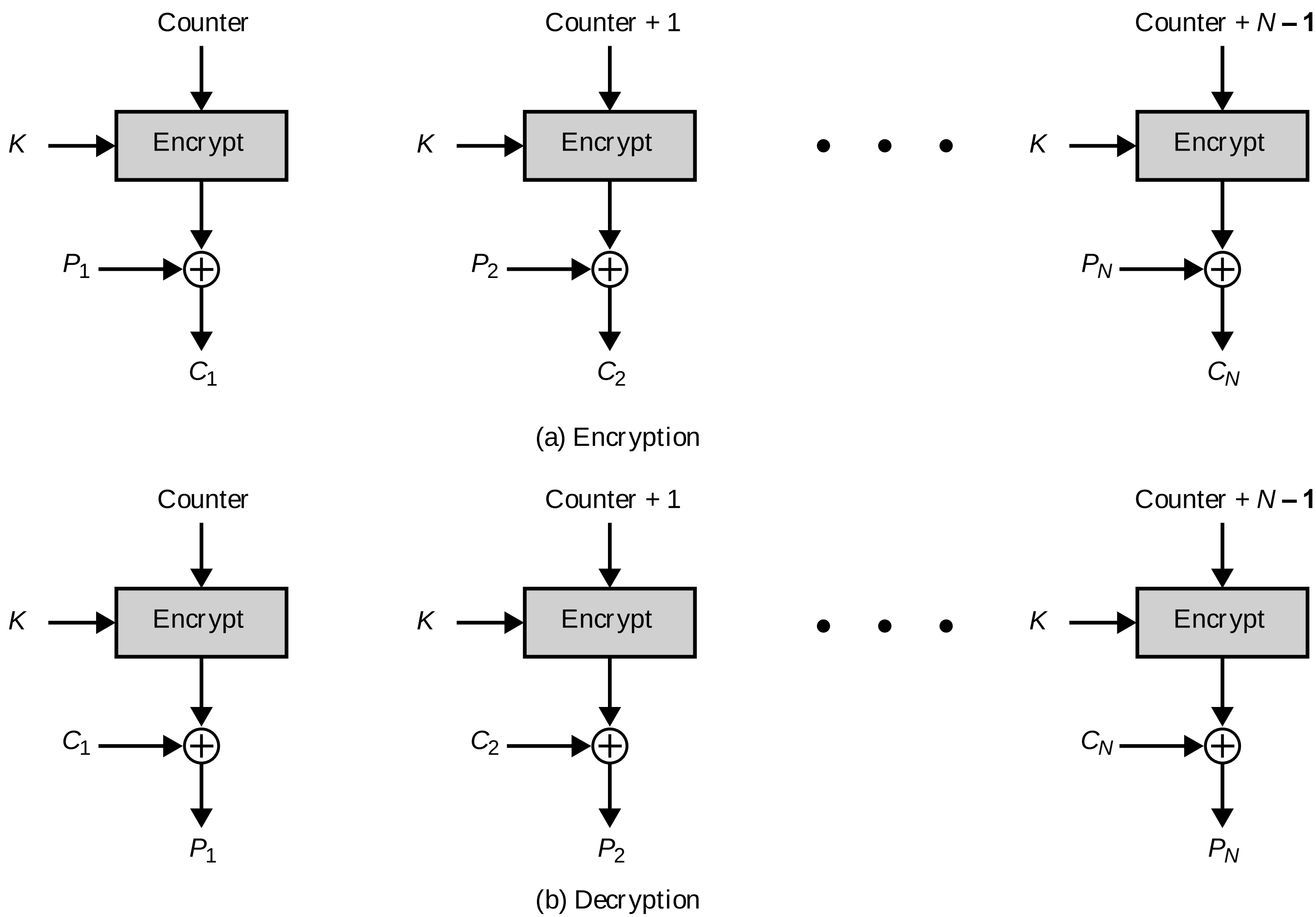


Figure 20.9 Counter (CTR) Mode

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

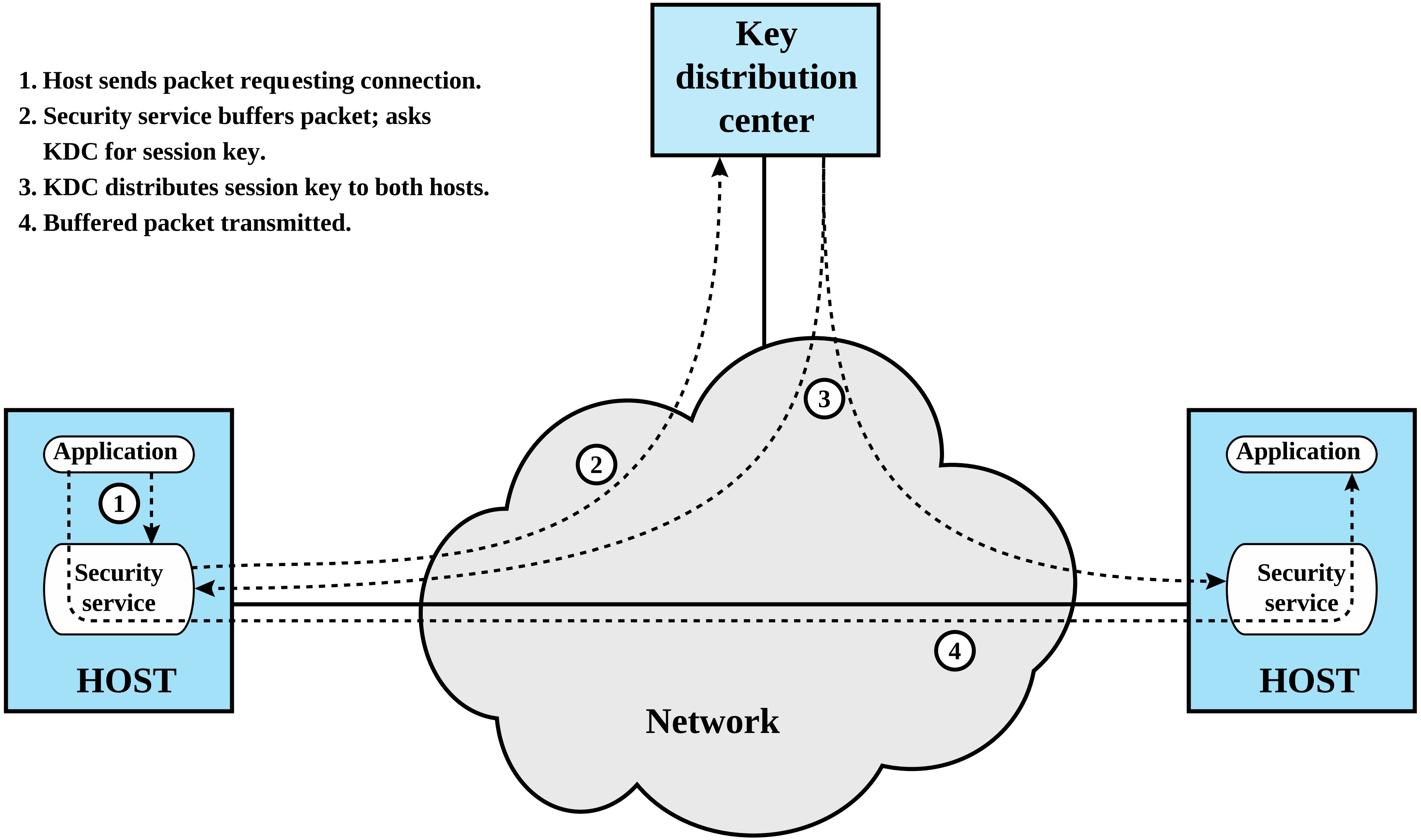


Figure 20.10 Automatic Key Distribution for Connection-Oriented Protocol