COMPUTER SECURITY

PRINCIPLES AND PRACTICE

SECOND EDITION

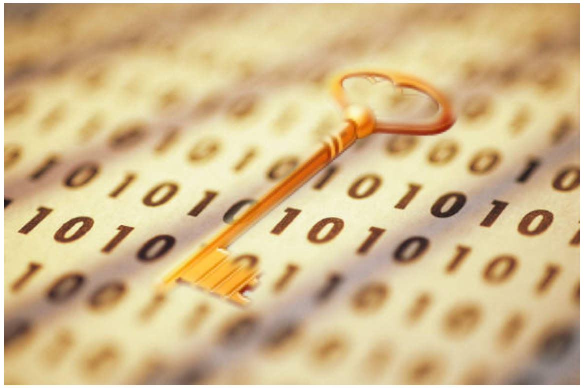
William Stallings | Lawrie Brown

Chapter 20

Symmetric Encryption and Message Confidentiality

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

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

Cryptanalysis

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

One Time Pads

- For confidentiality, One Time Pad provably secure.
  - Generate truly random key stream size of data to be encrypted.
  - Encrypt: Xor plaintext with the keystream.
  - Decrypt: Xor again with keystream.
- Weak for integrity
  - 1 bit changed in cipher text causes corresponding bit to flip in plaintext.
- Key size makes key management difficult
  - If key reused, the cipher is broken.
  - If key pseudorandom, no longer provably secure
  - Beware of claims of small keys but as secure as one time pad – such claims are wrong.

Feistel Cipher Structure

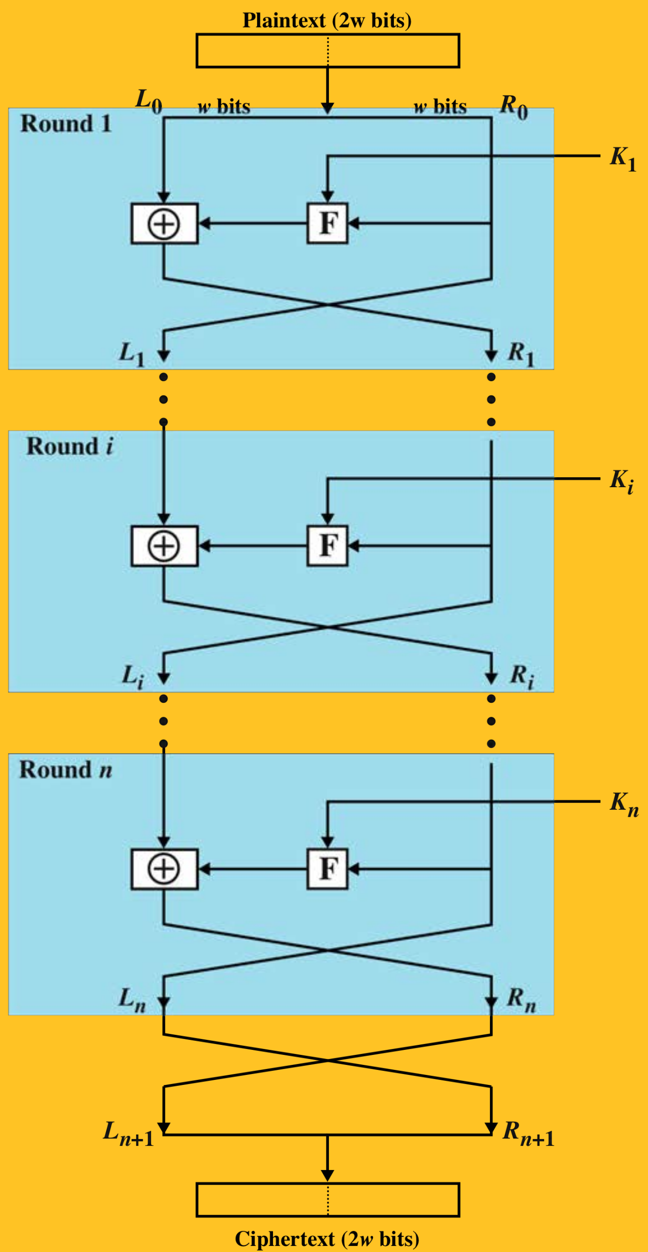


Figure 20.1 Classical Feistel Network

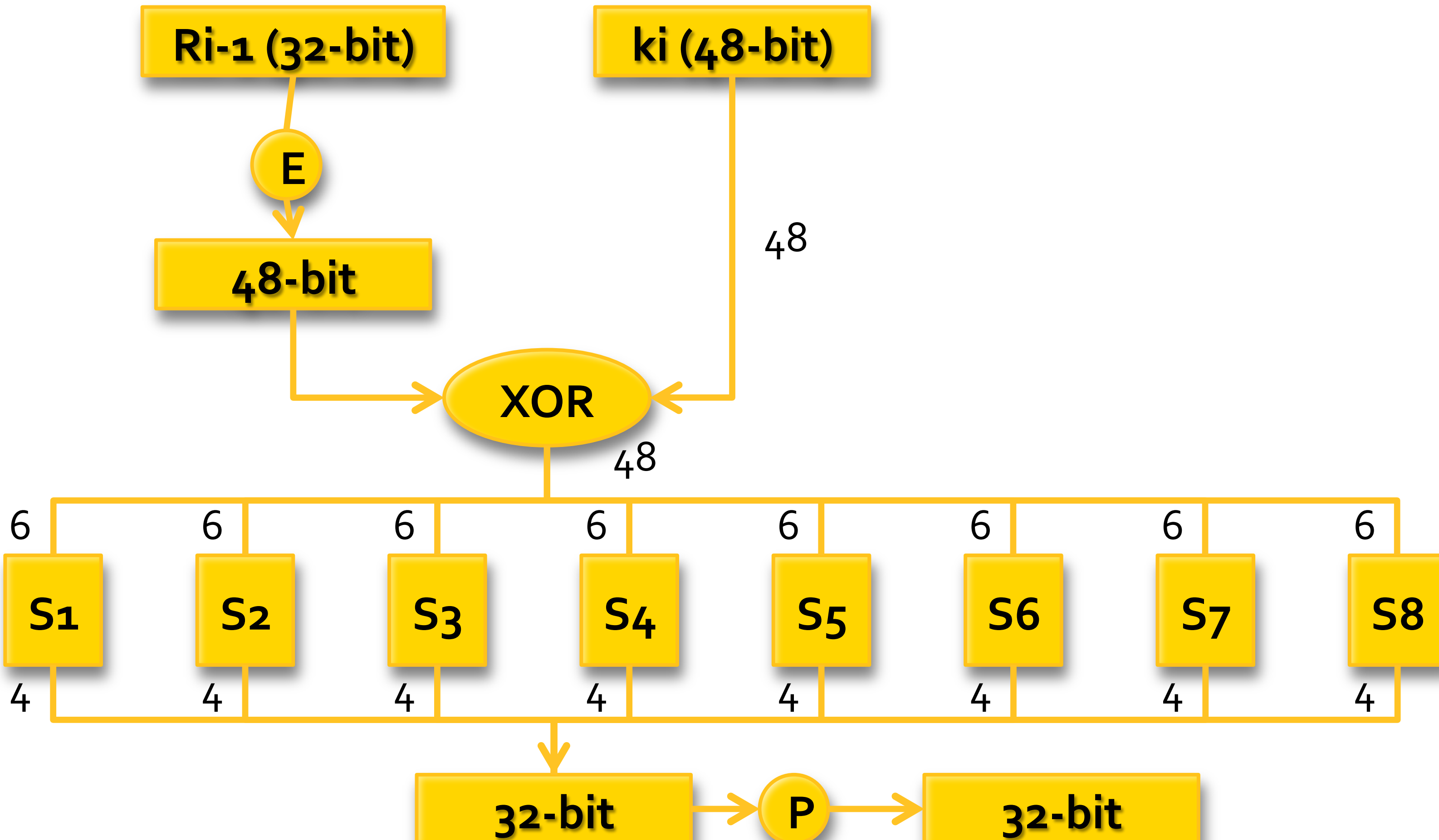
Data Encryption Standard (DES)

- most widely used encryption scheme
- adopted in 1977 by National Bureau of Standards
  - now NIST
- FIPS PUB 46
- algorithm is referred to as the Data Encryption Algorithm (DEA)
- minor variation of the Feistel network

DES

- $L_i = R_{i-1}$
  $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$
- where $f(R_{i-1}, k_i) = P(S(E(R_{i-1}) \oplus k_i))$
  - E is a fixed expansion permutation mapping R_{i-1} from 32 to 48 bits (all bits are used once, some used twice)
  - P is another fixed permutation on 32 bits
  - within each round, 8 fixed, carefully selected 6-to-4 bit substitution mapping (S-boxes) S_i are used

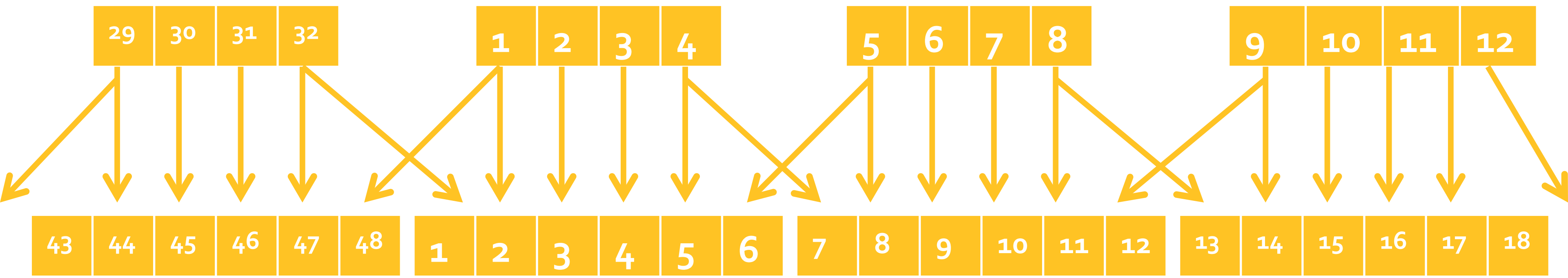
The Function f(Ri-1, ki)



ki

- Parity bits discarded from K (64 to 56 bits reduction).
- Initially, the 56-bit key is permuted.
- For each round:
  - ki is divided to two halves and rotated one or two positions each.
  - Result used as input to the next round and to select 48-bit key for the current round.

Expansion – E(Ri-1)



S-Box (S1)

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

Initial and Final Permutation

Input Position	1	2	3	4	5	…	60	61	62	63	64
Output Position	40	8	48	16	56	…	9	49	17	57	25

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

Triple DES (3DES)

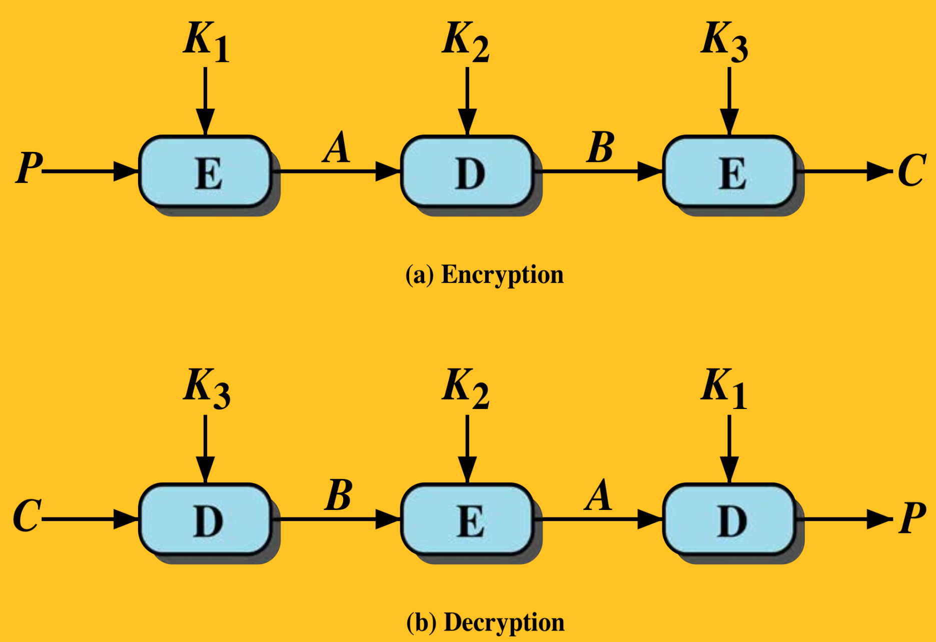


Figure 20.2 Triple DES

- first used in financial applications
- in DES FIPS PUB 46-3 standard of 1999
- uses three keys and three DES executions:

$$C = E(K_3, D(K_2, E(K_1, P)))$$

- decryption same with keys reversed
- use of decryption in second stage gives compatibility with original DES users
- effective 168-bit key length, slow, secure
- AES will eventually replace 3DES

Advanced Encryption Standard (AES)

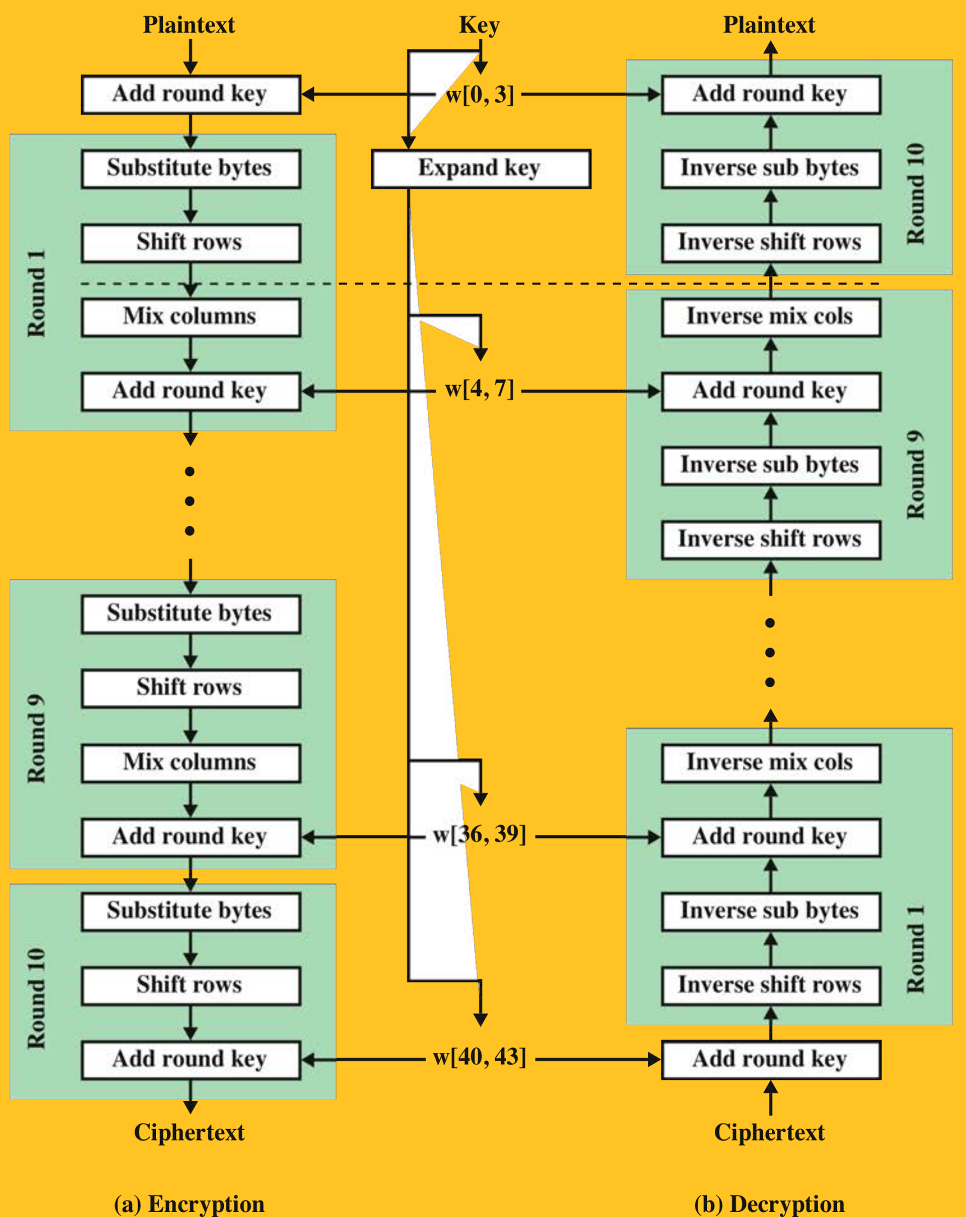


Figure 20.3 AES Encryption and Decryption

Certification of DES

- Had to be recertified every ~5 years
  - 1983: Recertified routinely
  - 1987: Recertified after NSA tried to promote secret replacement algorithms
    - Withdrawal would mean lack of protection
    - Lots of systems then using DES
  - 1993: Recertified after continued lack of alternative

Enter AES

- 1998: NIST finally refuses to recertify DES
  - 1997: Call for candidates for Advanced Encryption Standard (AES)
  - Fifteen candidates whittled down to five
  - Criteria: Security, but also efficiency
    - Compare Rijndael with Serpent
    - 9/11/13 rounds vs 32 (breakable at 7)
  - 2000: Rijndael selected as AES

Structure of Rijndael

- Unlike DES, operates on whole bytes for efficiency of software implementations
- Key sizes: 128/192/256 bits
- Variable rounds: 9/11/13 rounds
- More details on structure in the applied cryptography class.

AES Round Structure

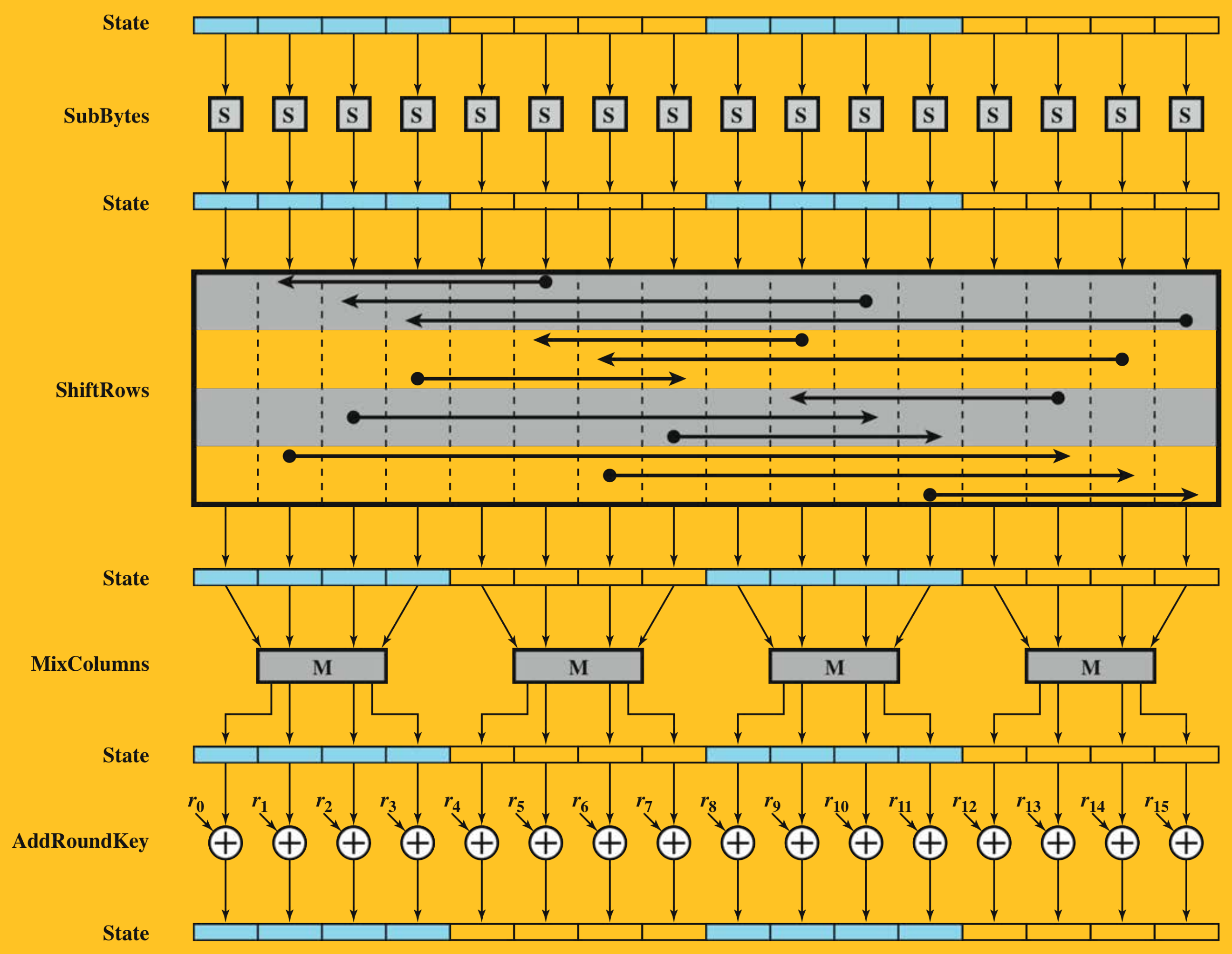


Figure 20.4 AES Encryption Round

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
- are faster and use far less code
- design considerations:
  - encryption sequence should have a large period
  - keystream approximates random number properties
  - uses a sufficiently long key

Table 20.3

Speed Comparisons of Symmetric Ciphers on a Pentium 4

Cipher	Key Length	Speed (Mbps)
DES	56	21
3DES	168	10
AES	128	61
RC4	Variable	113

Source: http://www.cryptopp.com/benchmarks.html

The RC4 Algorithm

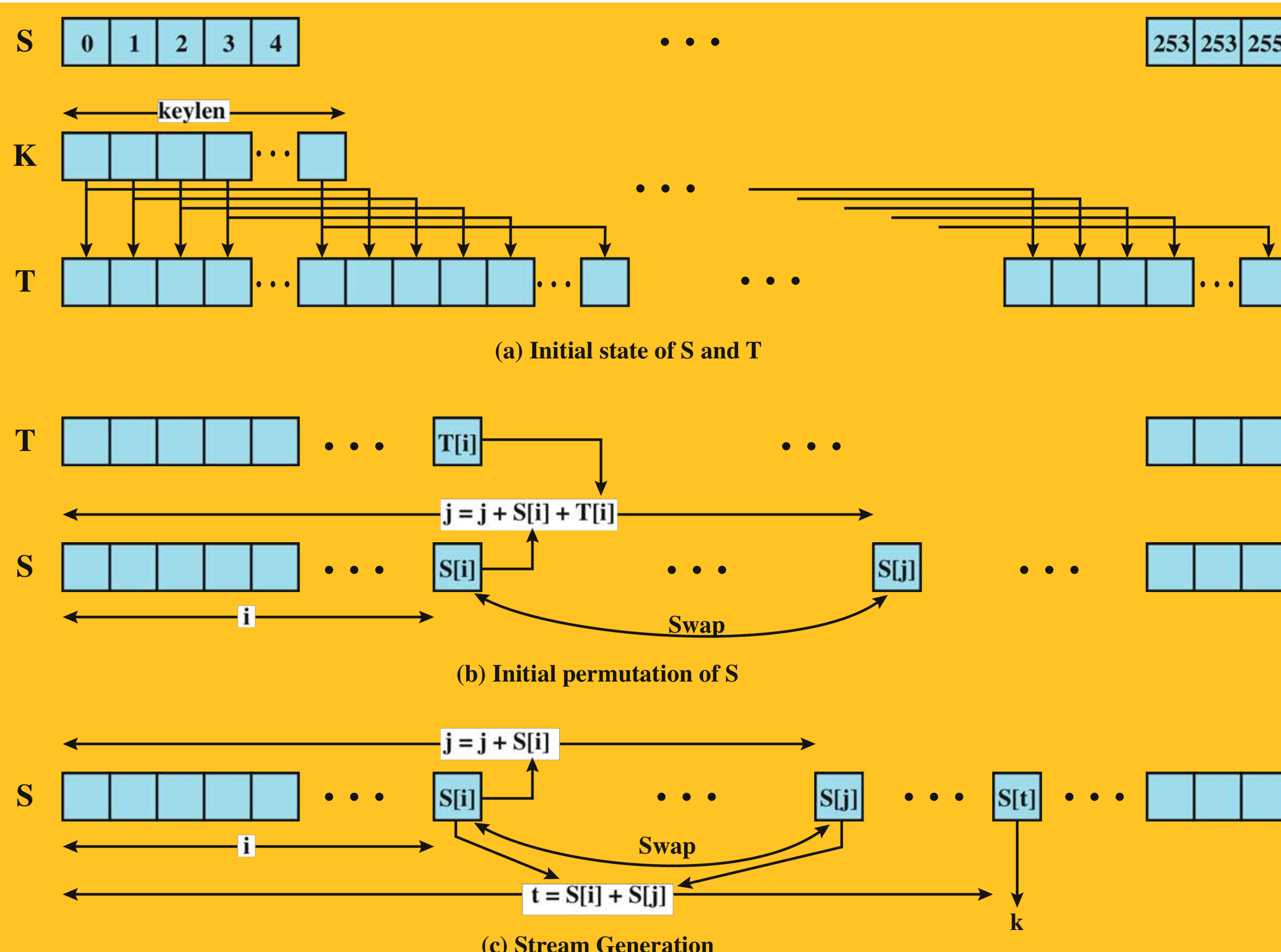


Figure 20.5 RC4

The RC4 Algorithm

- /* Initialization */

```
for i = 0 to 255 do
 S[i] = i;
T[i] = K[i mod keylen];
```

- /* Initial Permutation of S */

```
j = 0;
for i = 0 to 255 do
j = (j + S[i] + T[i]) mod 256;
Swap (S[i], S[j]);
```

- /* Stream Generation */

```
i, j = 0;
while (true)
i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
Swap (S[i], S[j]);
t = (S[i] + S[j]) mod 256;
k = S[t];
```

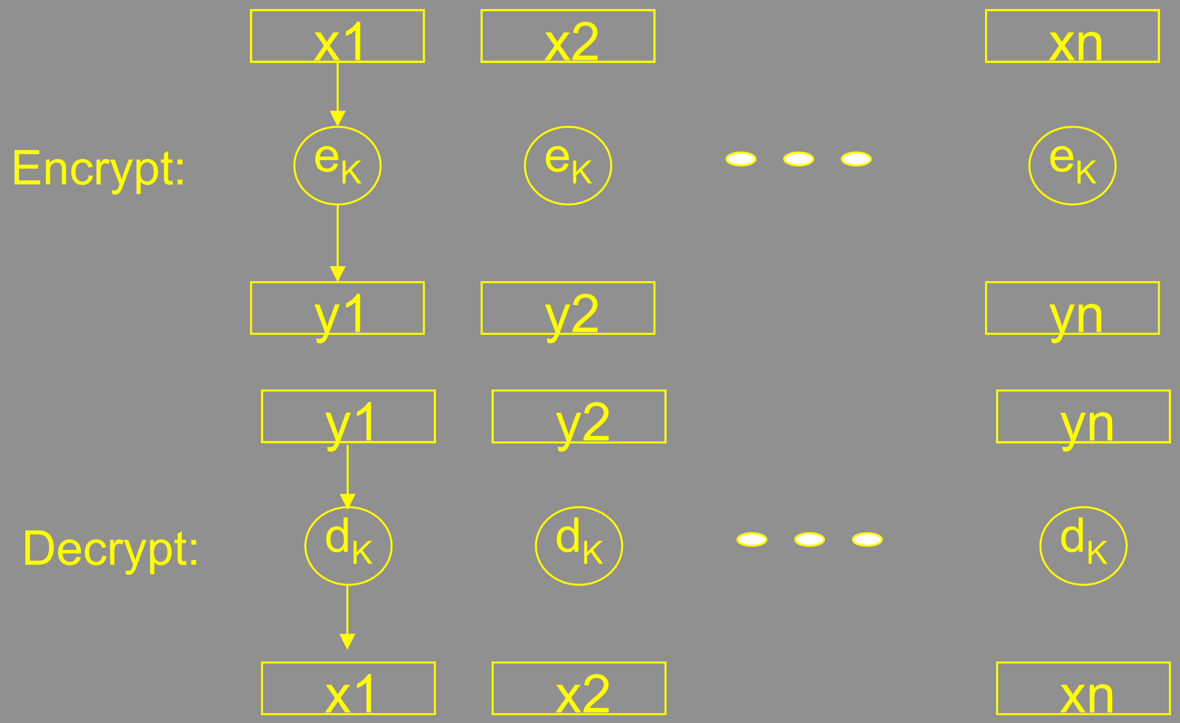
Modes of Operation

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)

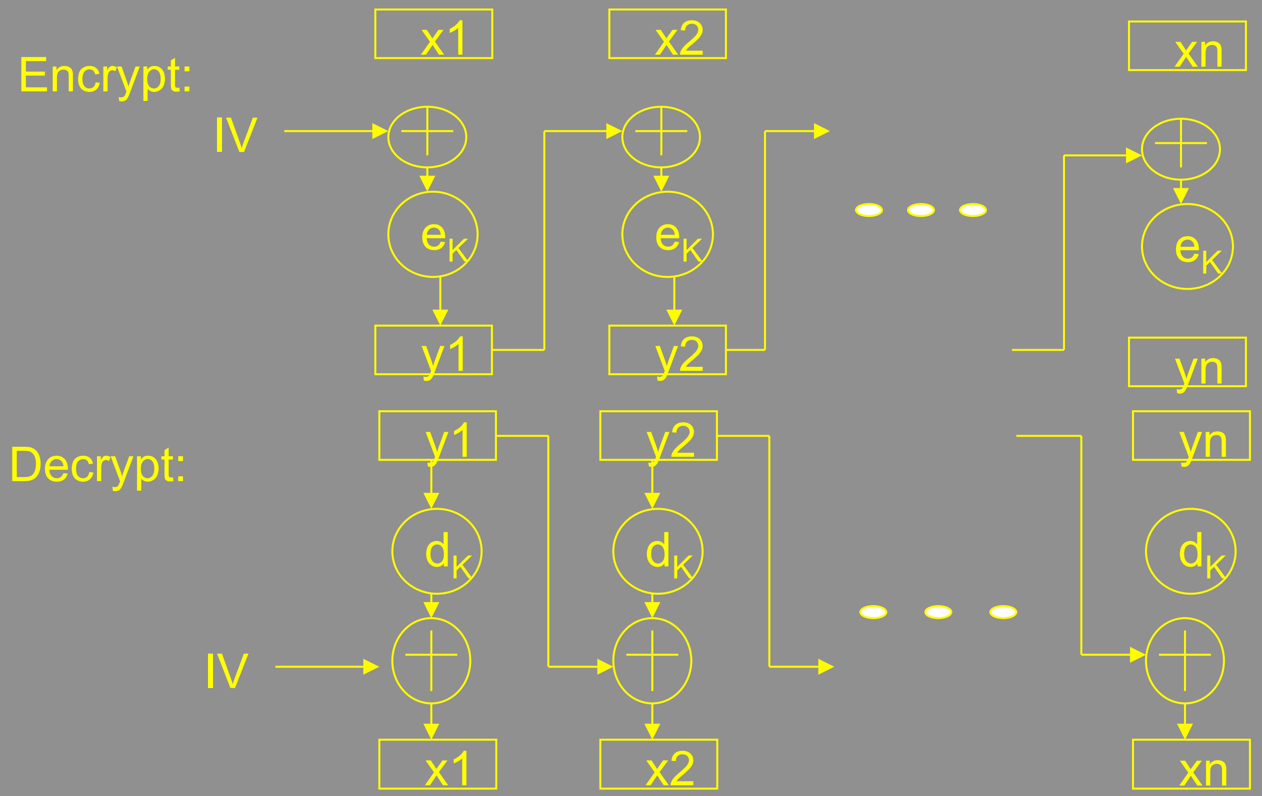
- **simplest mode**
- **plaintext is handled *b* bits at a time and each block is encrypted using the same key**
- **“codebook” because have unique ciphertext value for each plaintext block**
  - **not secure for long messages since repeated plaintext is seen in repeated ciphertext**
- **to overcome security deficiencies you need a technique where the same plaintext block, if repeated, produces different ciphertext blocks**

Electronic Code Book (ECB)



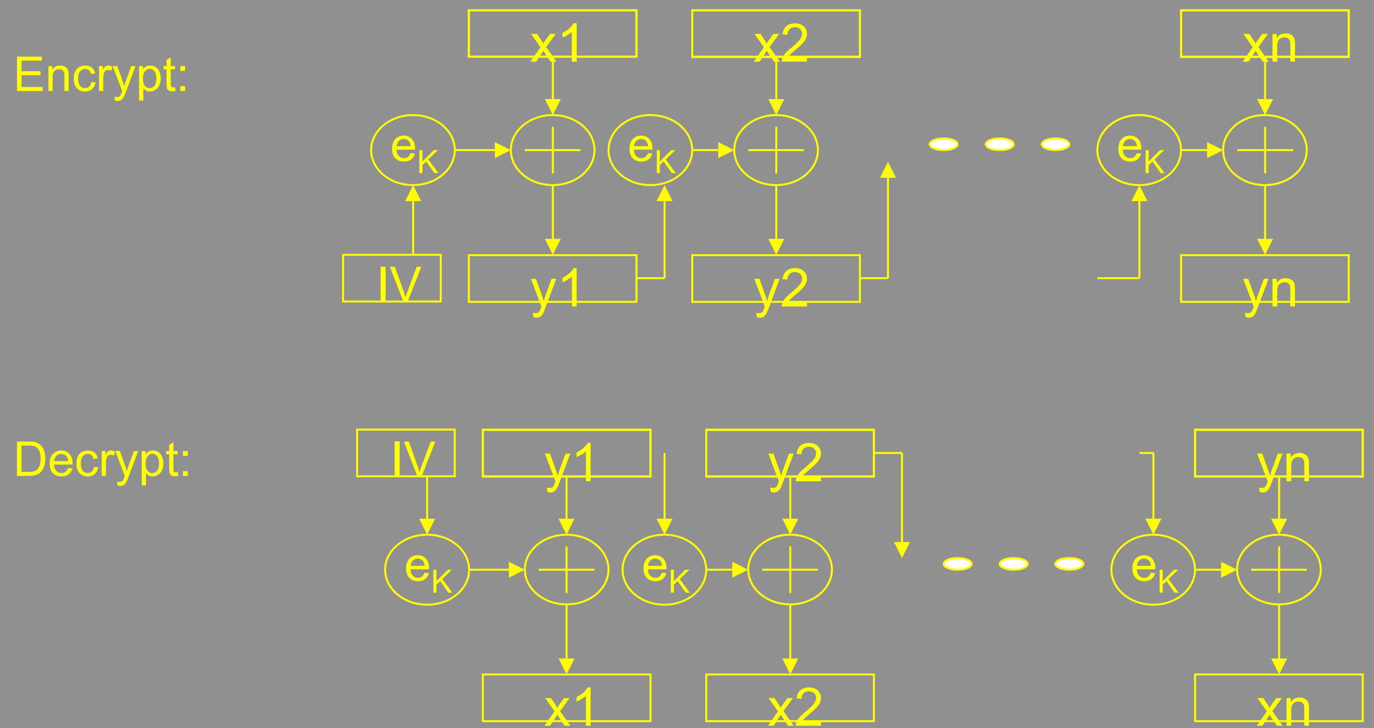
- **Each block encrypted in isolation**
- **Vulnerable to block replay**

Cipher Block Chaining (CBC)



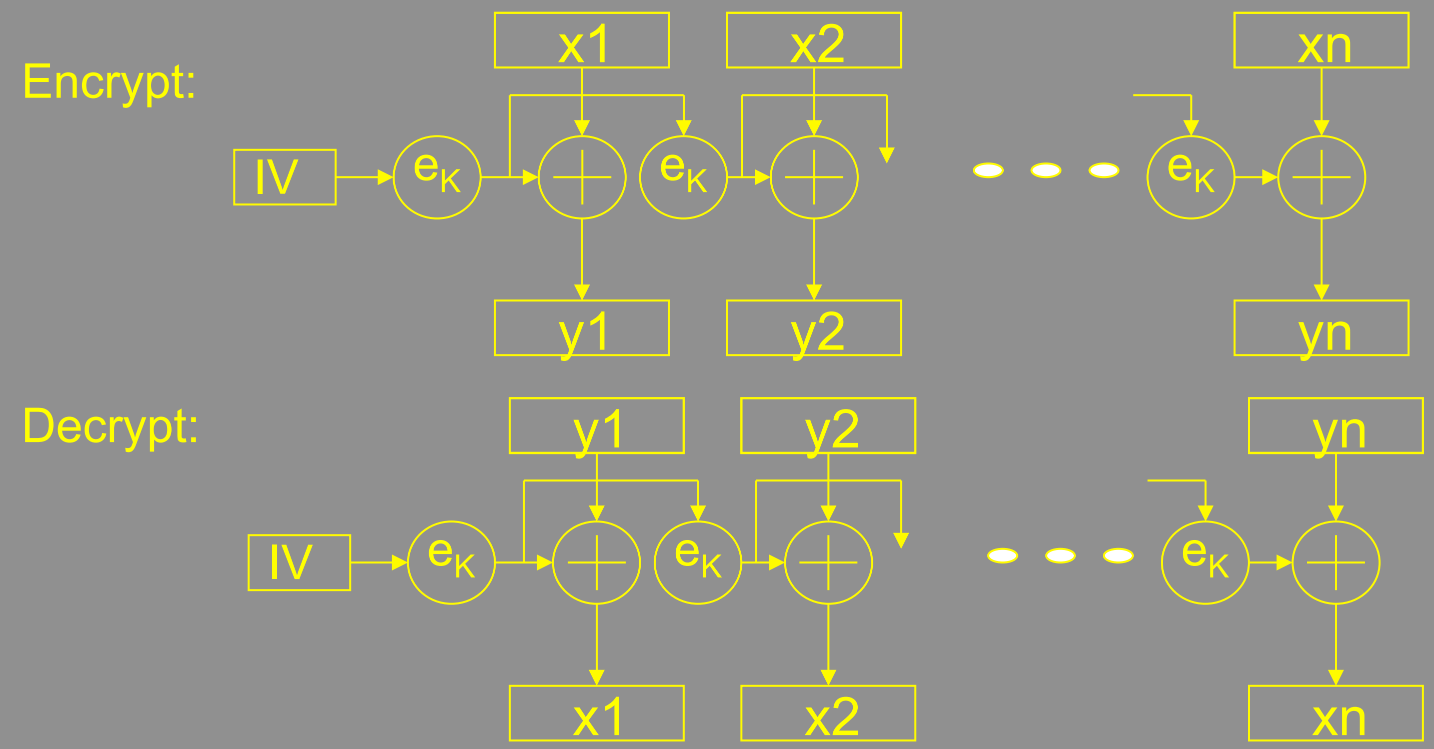
– **Each plaintext block XOR'd with previous ciphertext**
– **Easily incorporated into decryption**
– **What if prefix is always the same? IV!**

Cipher Feedback Mode (CFB)



- For encrypting character-at-a-time (or less)
- Chains as in CBC
- Also needs an IV – Must be Unique – Why?

Output Feedback Mode (OFB)



–Like CFB, but some bits of output fed back into input stream

Counter (CTR)

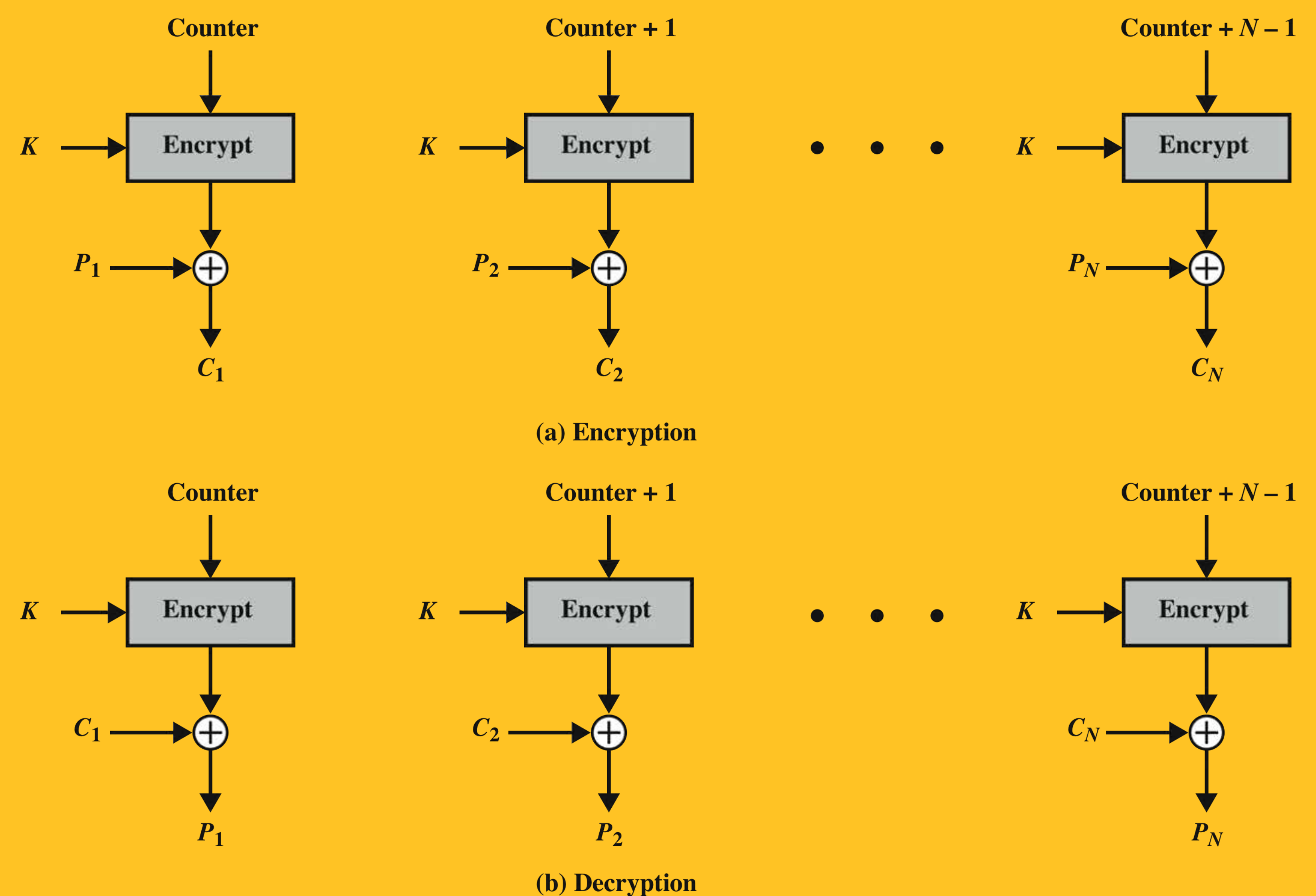


Figure 20.8 Counter (CTR) Mode

Location of Encryption

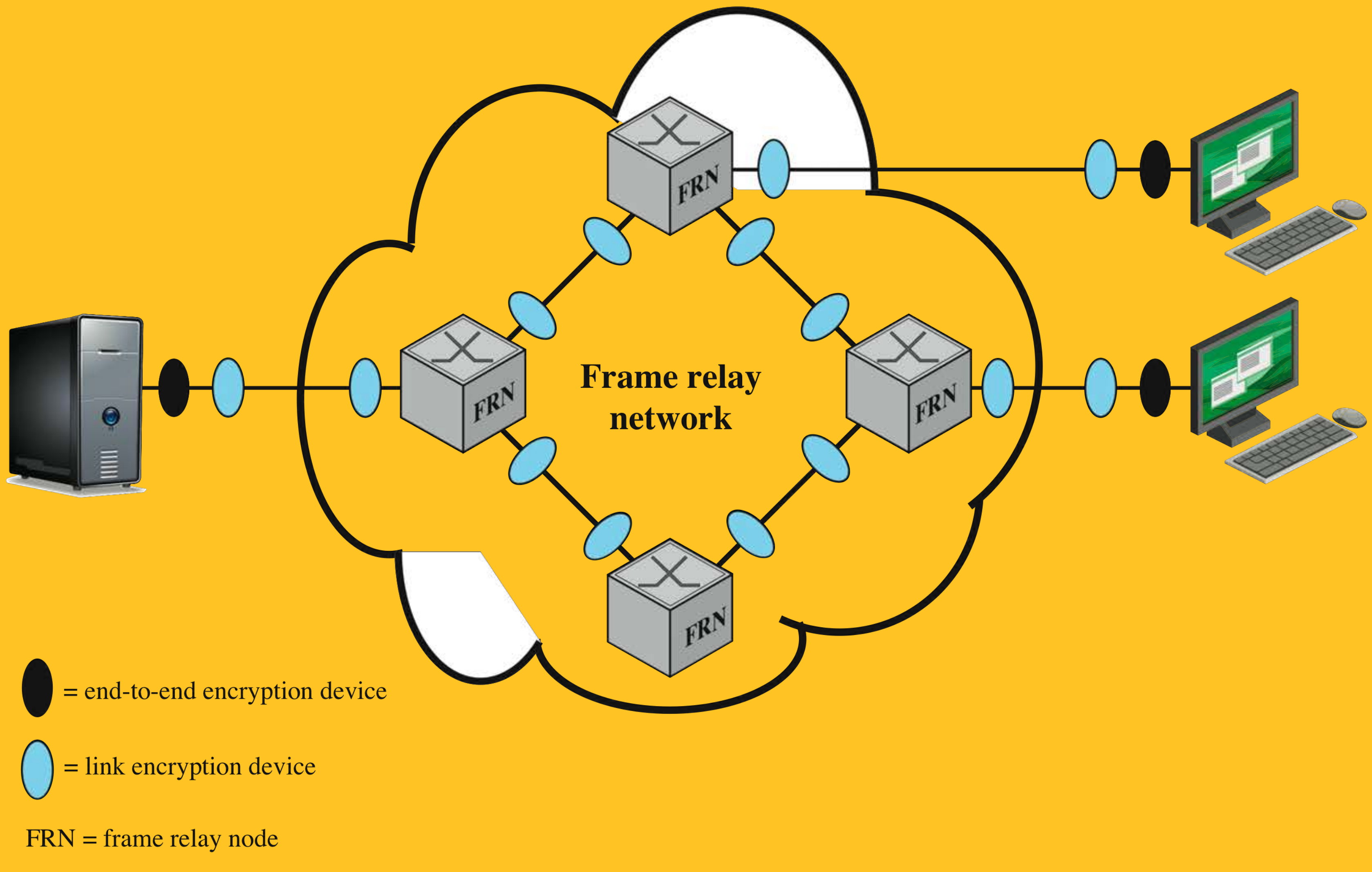


Figure 20.9 Encryption Across a Frame Relay Network

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

Key Distribution

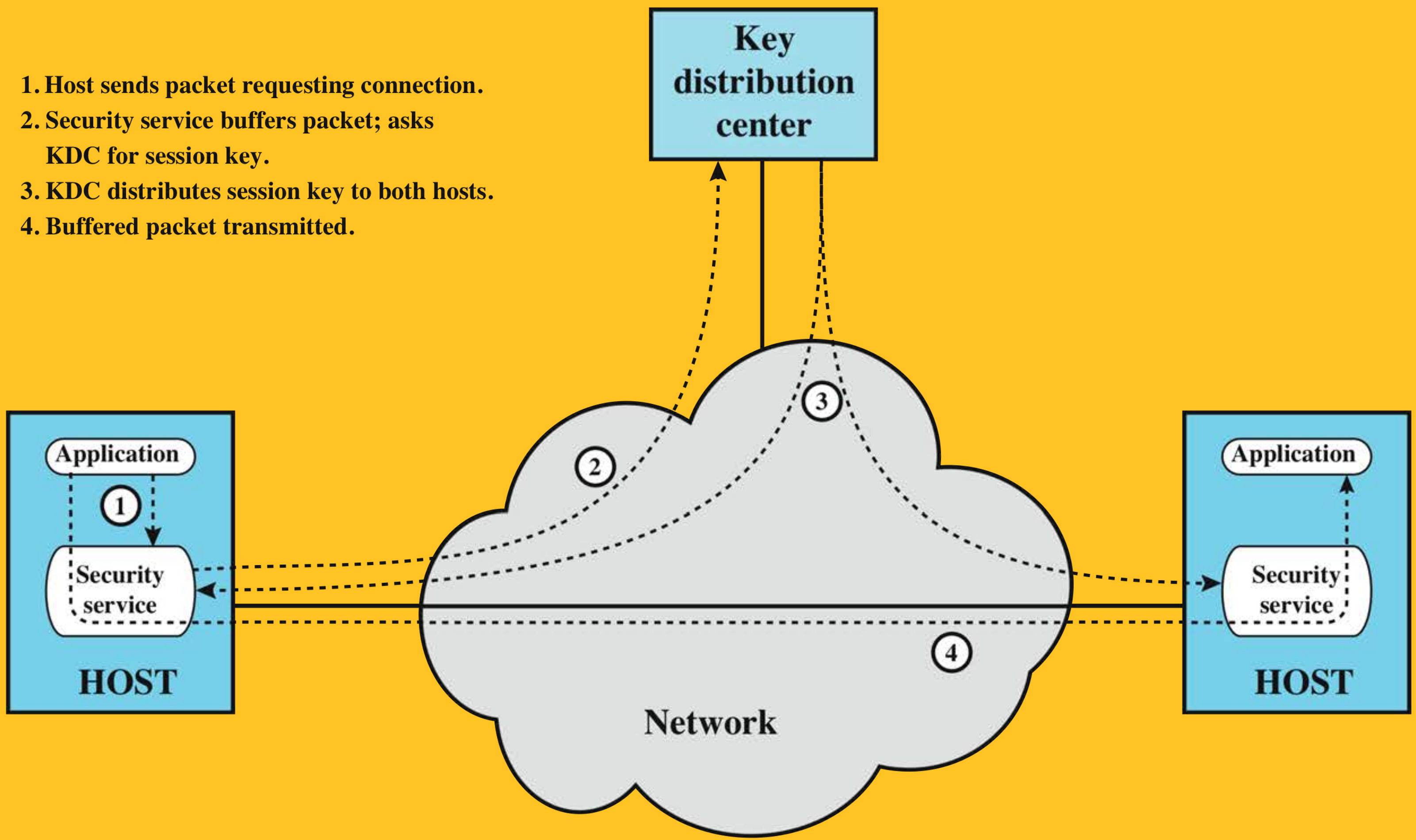


Figure 20.10 Automatic Key Distribution for Connection-Oriented Protocol

Summary

- symmetric encryption principles
  - cryptography
  - cryptanalysis
  - Feistel cipher structure
- data encryption standard
  - triple DES
- advanced encryption standard
  - algorithm details
- key distribution
- stream ciphers and RC4
  - stream cipher structure
  - RC4 algorithm
- cipher block modes of operation
  - electronic codebook mode
  - cipher block chaining mode
  - cipher feedback mode
  - counter mode
- location of symmetric encryption devices