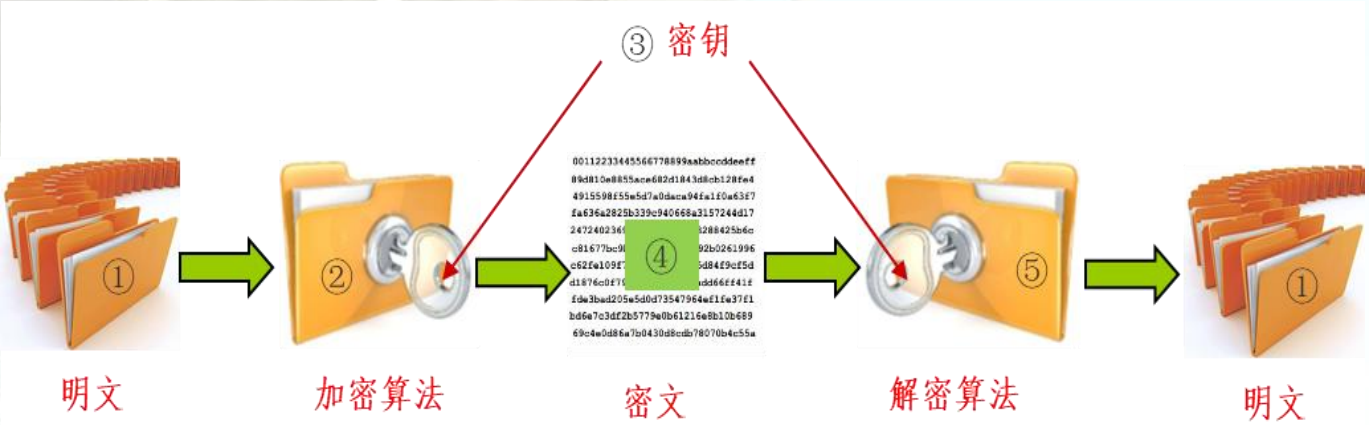
Symmetric Ciphers对称密码

（-）分组密码与加密标准

Block Ciphers and the Encryption Standard

对称加密算法（Symmetric Encryption）

- 对称密码算法：加密运算与解密运算使用同一把密钥，对称密码模型如图所示

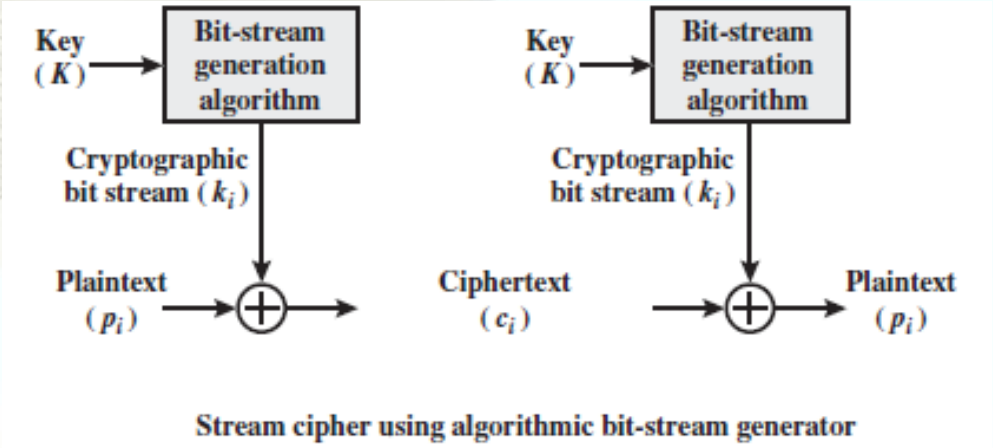


- ✓ 由5部分组成：①明文、②加密算法、③密钥、④密文、⑤解密算法
- ✓ 加密算法与解密算法采用同一算法，加密密钥与解密密钥为同一把密钥
- ✓ 常见的对称加密算法有AES、3DES、以及SM4

两类对称密码

序列（流）密码：

将明文消息按字符逐位加密



Stream cipher using algorithmic bit-stream generator

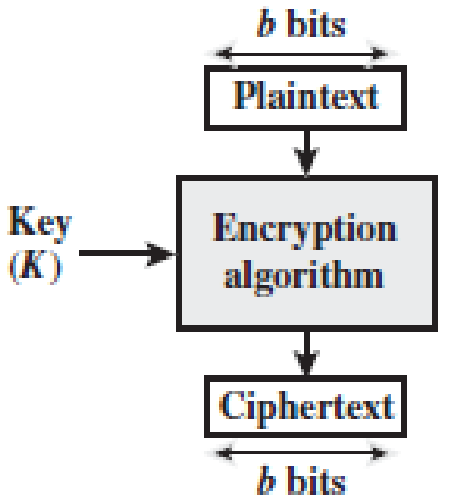
典型的算法代表: RC4

分组密码:

将明文消息分组，逐组的进行加密

- 典型的算法代表:

  DES、3DES、 AES等



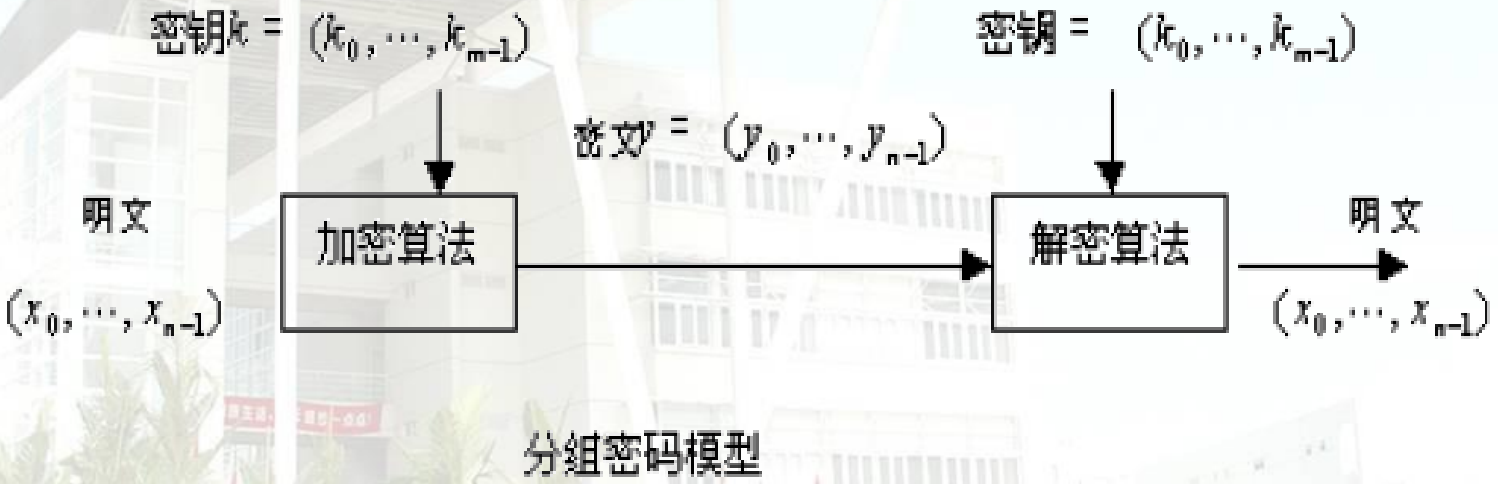
Block cipher

Modern Block Ciphers

- one of the most widely used types of cryptographic algorithms
- provide secrecy /authentication services

分组密码的一般设计原理

- 分组密码是将明文消息序列，划分成长度为*n*的组，
- 每组分别在密钥的控制下变换成等长的密文序列，



分组密码模型

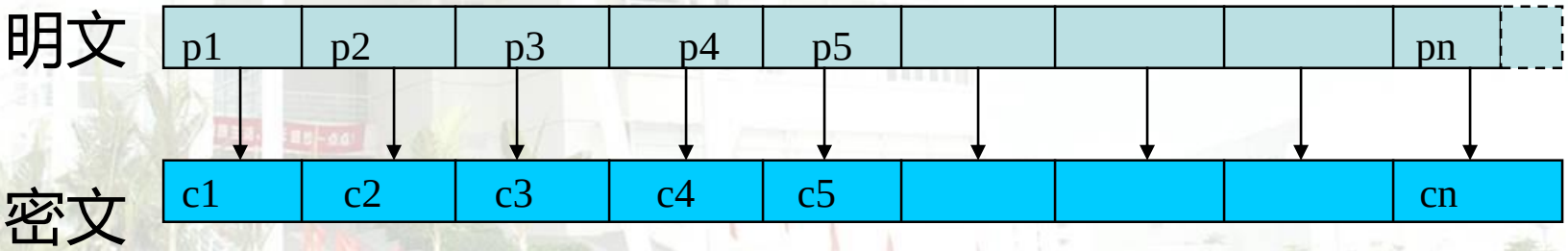
Modern Block Ciphers

对称分组密码算法

在明文分组和密文分组上进行运算

通常：分组长为64bits，或更长。

相同的明文和相同的密钥得到相同的密文。



设计准则

- 安全性准则
  设计安全算法
  分组长度
  密钥长度
- 实现性准则
  提高算法的执行速度

分组密码算法的安全性原则

基于Shannon理论(1945)

cipher needs to completely obscure statistical properties of original message

- **Diffusion(扩散)**

dissipates statistical structure of plaintext over bulk of ciphertext

  - **小扰动的影响波及到全局。**
  - **密文没有统计特征，明文一位影响密文的多位，增加密文与明文之间关系的复杂性**

- **Confusion(混乱)**

makes relationship between ciphertext and key as complex as possible

  - **强调密钥的作用**
  - **增加密钥与密文之间关系的复杂性**

设计准则

分组长度

必须足够大，阻止对分组密码进行统计分析

密钥长度

必须保证密钥长度尽可能大，要求至少128bits

实现原则

- **软件实现** 优点: 灵活性强、代价低

要求: * 使用子块和简单的运算

密码运算在子块上进行，如**16**、**32**比特等

* 密码运算尽量采用易于软件实现的运算

用标准处理器具有的基本指令: 如加法、乘法、移位等

- **硬件实现** 优点:可获得高速率

要求: * 加密和解密的相似性:

加密和解密过程的不同应仅仅在密钥使用方式上

-> 采用同样的器件来实现加密和解密，以节省费用和体积

* 尽量采用标准的组件结构

-> 适应于在VLSI IC 中实现

工作模式Mode

- 电子密码本（ECB）模式 (Electronic Codebook Book)
- 密码分组链接（CBC）模式 (Cipher Block Chaining)
- 密码反馈（CFB）模式 (Cipher FeedBack)
- 输出反馈（OFB）模式 (Output FeedBack)
- 计数器 (CTR) 模式 （Counter）

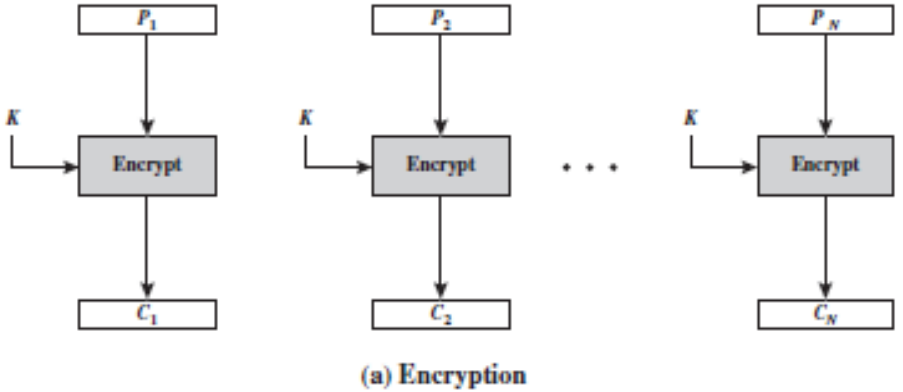
Block Cipher Modes of Operation

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 encryption output, and full blocks are used.	• 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

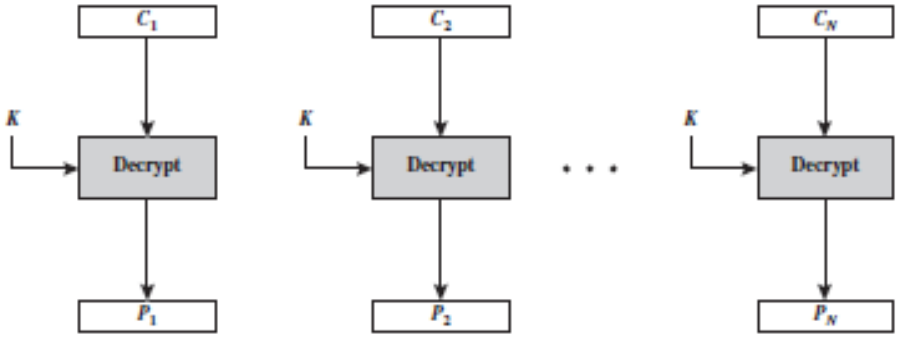
Electronic Code Book (ECB)电子密码本

ECB	$C_j = E(K, P_j)$	$j = 1, \ldots, N$	$P_j = D(K, C_j)$	$j = 1, \ldots, N$

- message is broken into independent blocks which are encrypted
- each block is encoded by using the same key
- Padding the last if necessary



(a) Encryption



(b) Decryption

Electronic Codebook (ECB) Mode

Electronic Codebook Book (ECB)电子密码本

- For a given key, a unique ciphertext for each block

  相同的明文永远被加密成相同的密文分组

  形成一个包含有明文及其对应的密文的密码本Codebook

  如果分组的大小为64位，那么密码本就有2^{64}项

- Simplest mode

  每个分组可以独立的进行加密，不必按次序进行

- No secure enough

  如果密码分析者有很多消息的明密文，就可以在不知道密钥的情况下编写密码本

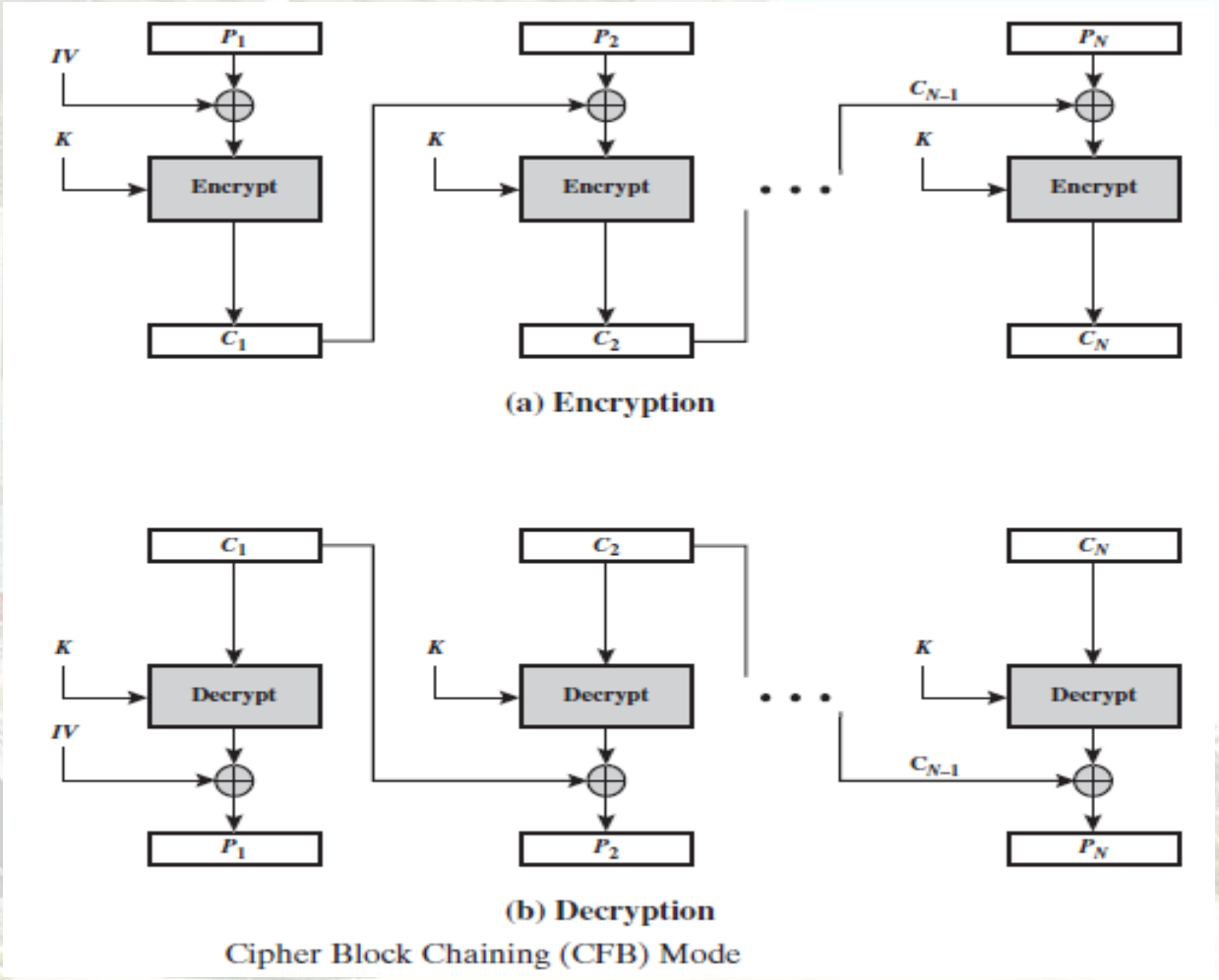
- Uses

  secure transmission of single values

  (sending a few blocks of data)

Cipher Block Chaining (CBC)密码分组链接

- message is broken into blocks
- blocks are linked together in the encryption operation



Cipher Block Chaining (CFB) Mode

Cipher Block Chaining (CBC)

each previous cipher blocks is chained with current plaintext block,

$$C_j = \mathrm{E}(K, [C_{j-1} \oplus P_j])$$

当前的明文与上一个密文的异或

- use Initial Vector (IV) **初始矢量** to start process

  $C_{-1} = \mathrm{IV}$

- uses: bulk data encryption, authentication
- Padding：

  pad last block with count of pad size

  eg. [b1 b2 b3 0 0 0 0 5] <- 3 bytes data, then 5 bytes pad+count

  对最后一分组的处理

Advantages and Limitations of CBC

- each ciphertext block depends on **all** message blocks
  a change in the message affects all ciphertext blocks
  密文与所有分组有关

- IV known to sender & receiver
  (**共享秘密**)

CBC

Properties of XOR：

$$[A \oplus B] \oplus C = A \oplus [B \oplus C]$$

$$A \oplus A = 0$$

$$A \oplus 0 = A$$

$$C_i = E_K(P_i \oplus C_{i-1}) \Leftrightarrow P_i = D_K(C_i) \oplus C_{i-1}$$

Cipher FeedBack (CFB)密码反馈

- message is treated as a stream of bits
  处理为流密码

Cipher FeedBack (CFB)密码反馈

解密过程：

Cipher FeedBack (CFB)密码反馈

$$C_1 = P_1 \oplus S_s(E_k(IV))$$

$$where \quad 1 \le s \le 64$$

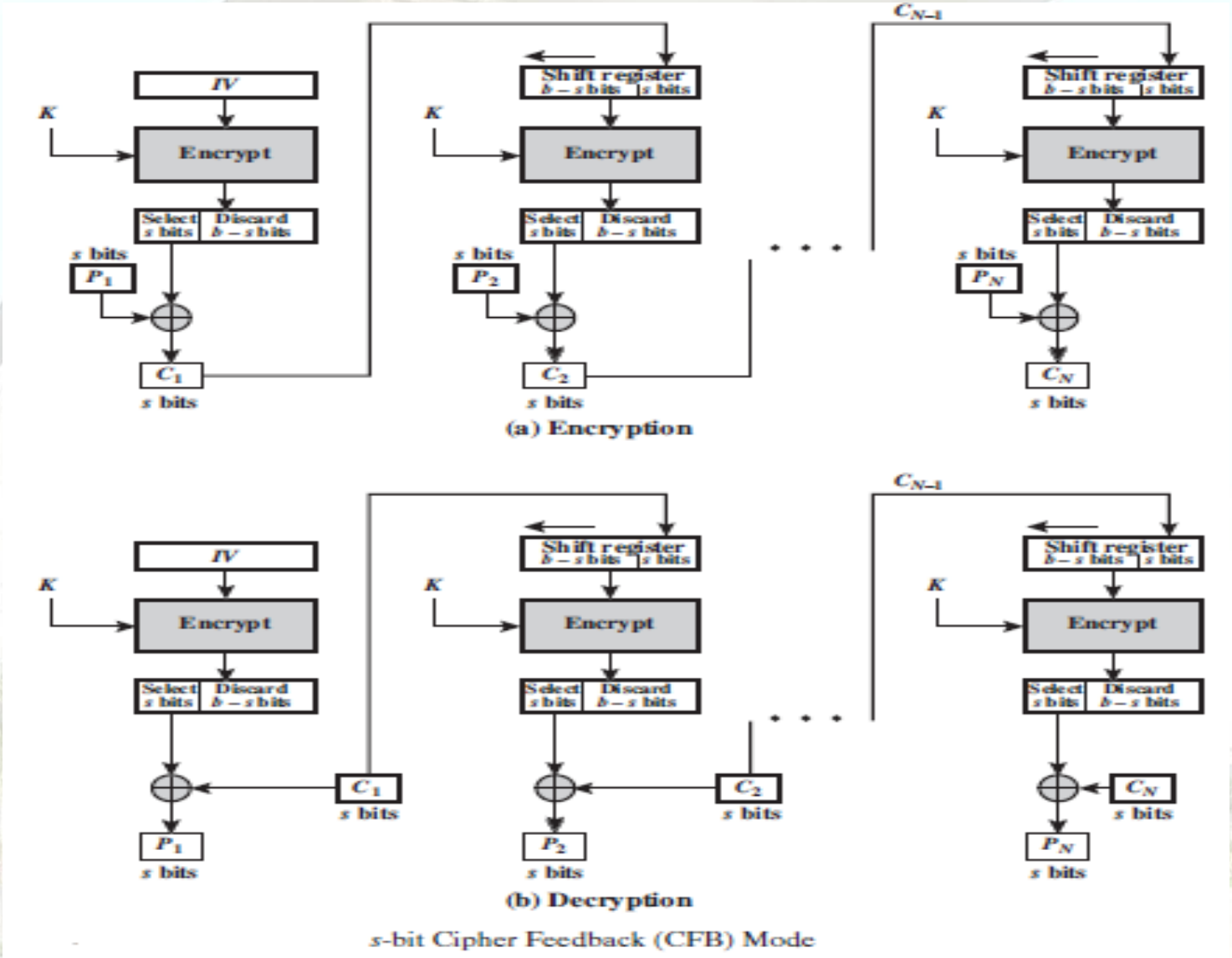
$$P_1 = C_1 \oplus S_s(E_k(IV))$$

- standard allows any number of bit (1,8 or 64 or whatever) to be feed back
  - denoted CFB-1, CFB-8, CFB-64 etc

CFB	$I_1 = IV$ $I_j = \text{LSB}_{b-s}(I_{j-1}) \,\|\, C_{j-1} \quad j = 2, \ldots, N$ $O_j = \text{E}(K, I_j) \quad j = 1, \ldots, N$ $C_j = P_j \oplus \text{MSB}_s(O_j) \quad j = 1, \ldots, N$	$I_1 = IV$ $I_j = \text{LSB}_{b-s}(I_{j-1}) \,\|\, C_{j-1} \quad j = 2, \ldots, N$ $O_j = \text{E}(K, I_j) \quad j = 1, \ldots, N$ $P_j = C_j \oplus \text{MSB}_s(O_j) \quad j = 1, \ldots, N$

- CFB-64 is most efficient to use all 64 bits

Cipher FeedBack (CFB)



s-bit Cipher Feedback (CFB) Mode

Advantages and Limitations of CFB

- 分组密码⇨流密码
- 隐藏了明文模式
- 需要共同的移位寄存器初始值IV
- 误差传递：一个单元损坏影响多个单元

Output FeedBack (OFB)输出反馈

- message is treated as a stream of bits
  处理为流密码

output of cipher is added to message
output is then feed back (hence name)

Output FeedBack (OFB)输出反馈

解密过程：

Output FeedBack (OFB)

- message is treated as a stream of bits
- feedback is independent of message

  can be computed in advance

$C_i = P_i \text{ XOR } O_i$

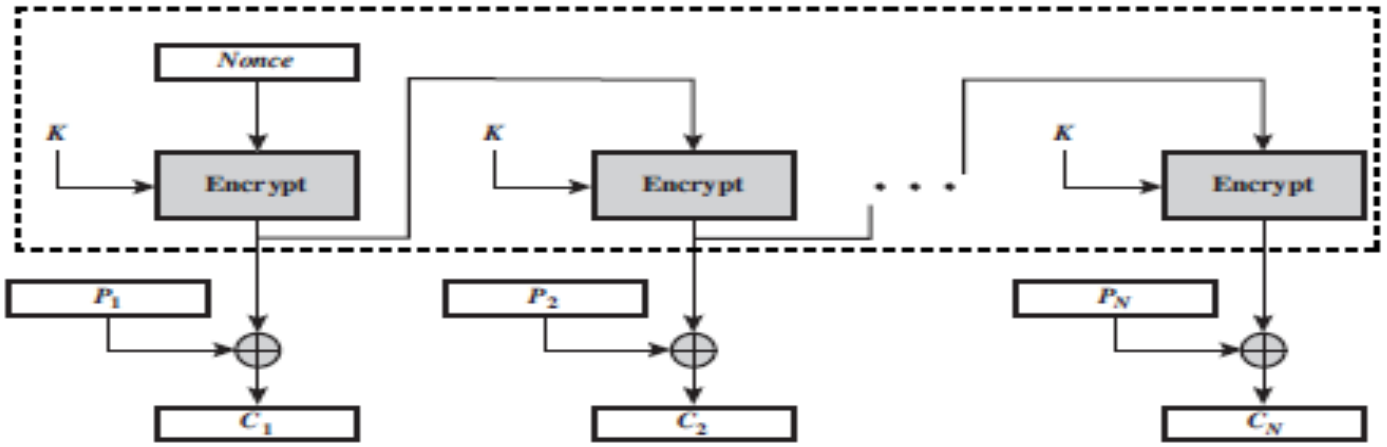
$O_i = S_s(E_K(O_{i-1}))$

$O_{-1} = IV$

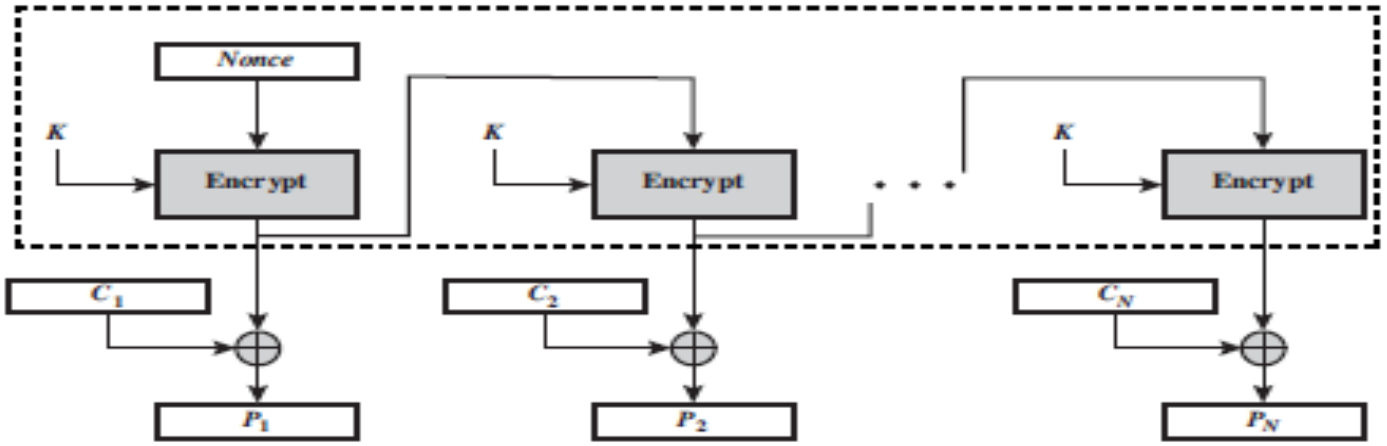
$$C_j = P_j \oplus \mathrm{E}(K, [C_{j-i} \oplus P_{j-1}])$$

$$P_j = C_j \oplus \mathrm{E}(K, [C_{j-1} \oplus P_{j-1}])$$

Output FeedBack (OFB)



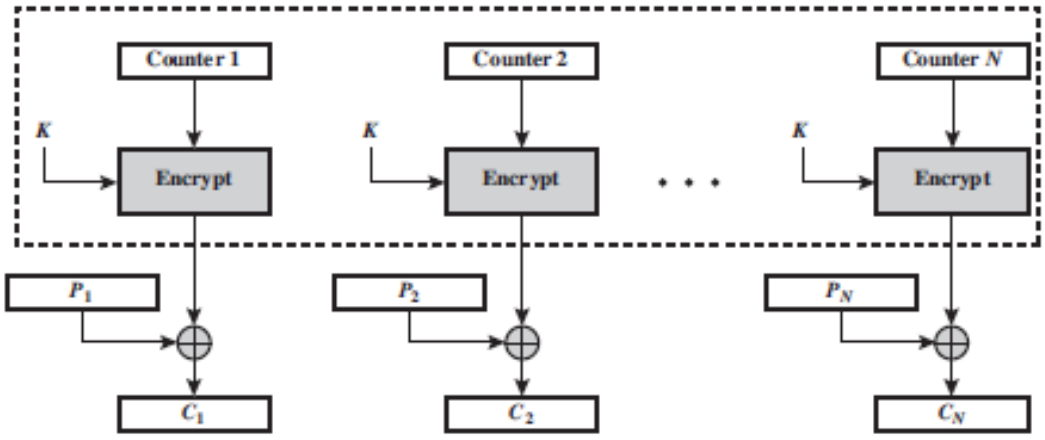
(a) Encryption



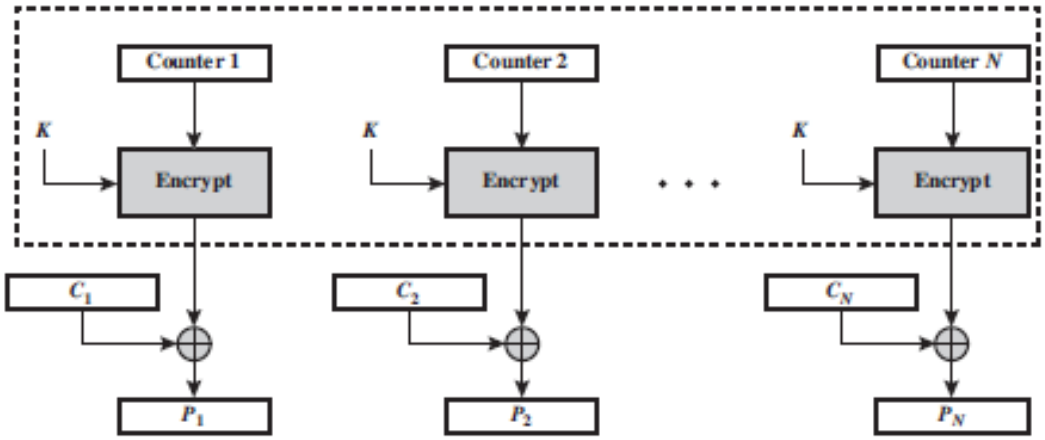
(b) Decryption

Output Feedback (OFB) Mode

Counter (CTR)计数器



(a) Encryption



(b) Decryption

Counter (CTR) Mode

Counter (CTR)计数器

- encrypts counter value rather than any feedback value
- must have a different key & counter value for every plaintext block (never reused)

$$C_i = P_i \text{ XOR } O_i$$

$$O_i = E_K(i)$$

CTR	$C_j = P_j \oplus \mathrm{E}(K, T_j) \quad j = 1, \ldots, N-1$ $C_N^* = P_N^* \oplus \mathrm{MSB}_u[\mathrm{E}(K, T_N)]$	$P_j = C_j \oplus \mathrm{E}(K, T_j) \quad j = 1, \ldots, N-1$ $P_N^* = C_N^* \oplus \mathrm{MSB}_u[\mathrm{E}(K, T_N)]$

- uses: high-speed network encryptions

Advantages and Limitations of CTR

- efficiency in both Hardware and software
  - can do parallel processing **并行处理**
  - good for high speed links

    e.g wireless -- 802.11i
- random access to encrypted data blocks
- but must ensure never reuse key/counter values

Feistel Cipher Structure

- most symmetric block ciphers are based on
  Feistel Cipher Structure

利用不断更新和替换的密码表

Shannon理论：

diffusion(扩散):小扰动的影响波及到全局
消除密文统计特征
confusion(混乱):通过密钥增加密钥与密文之间关系的复杂性

Feistel Cipher Structure

partitions input block into two halves

process through multiple rounds：

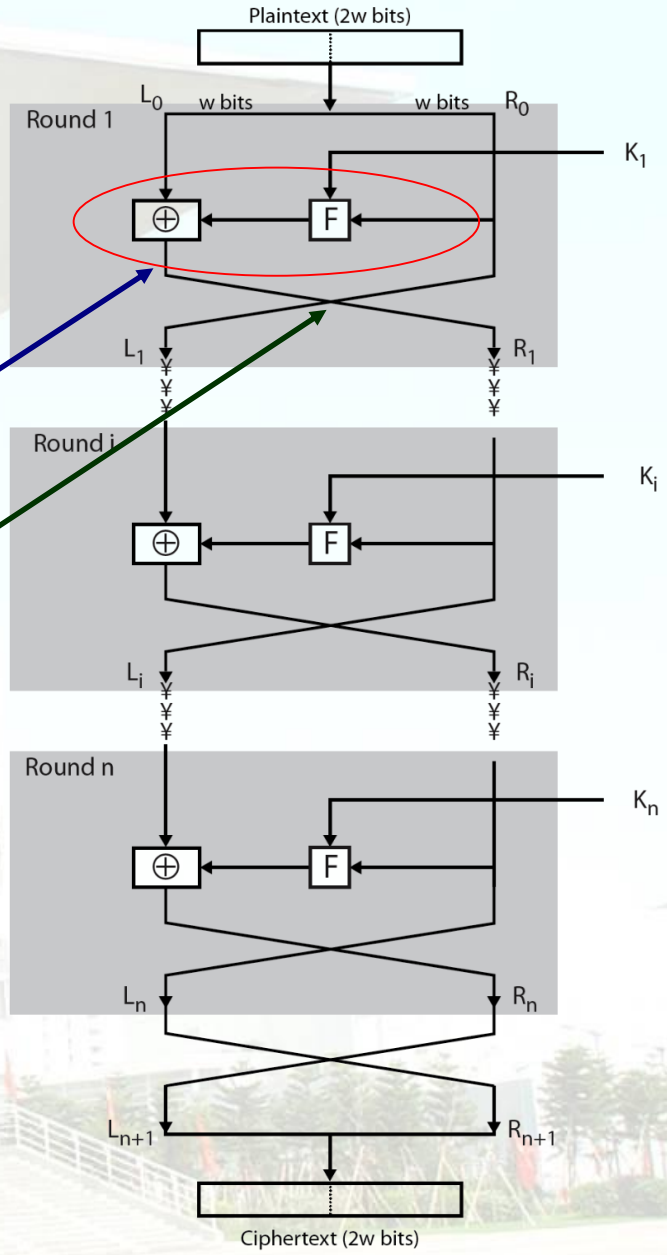
perform a substitution（代换） on left data half

- F 轮函数（右半数据，子密钥）
- 与左半数据异或

have permutation（置换）swapping

implements Shannon's SPN concept
(Substitution permutation Network)

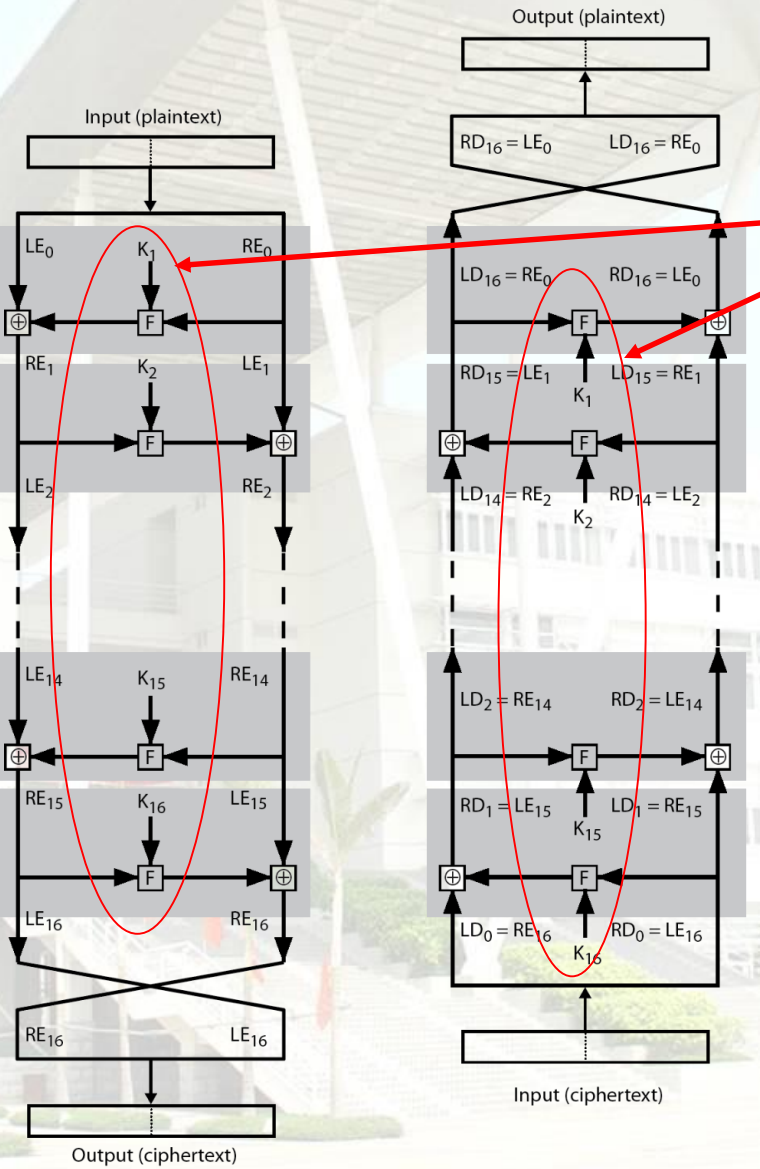
substitution (S-box)
permutation (P-box)



Cipher Design

- block size:
  larger block size -> greater security
  but reduce en/decryption speed
  ≥64 bits （DES）, AES:128 bits,
- key size:
  larger key size -> greater security
  greater resistance to brute-force attacks
  greater confusion
  but reduce e/d speed
  ≥64 bits （DES）, AES:128 bits,
- number of rounds: multiple rounds offer increasing security. Typical: 16
- subkey generation algorithm: greater complexity -> greater difficulty cryptanalysis
- round function: greater complexity -> greater resistance to cryptanalysis
- fast software en/decryption
- algorithm: ease to analyze

Feistel Cipher Decryption



encryption

Subkeys k_i in reverse order

Don't need two difference algorithms

Decryption