Chapter 8

Encipherment Using Modern Symmetric-Key Ciphers

8-1 USE OF MODERN BLOCK CIPHERS

Symmetric-key encipherment can be done using modern block ciphers. Modes of operation have been devised to encipher text of any size employing either DES or AES.

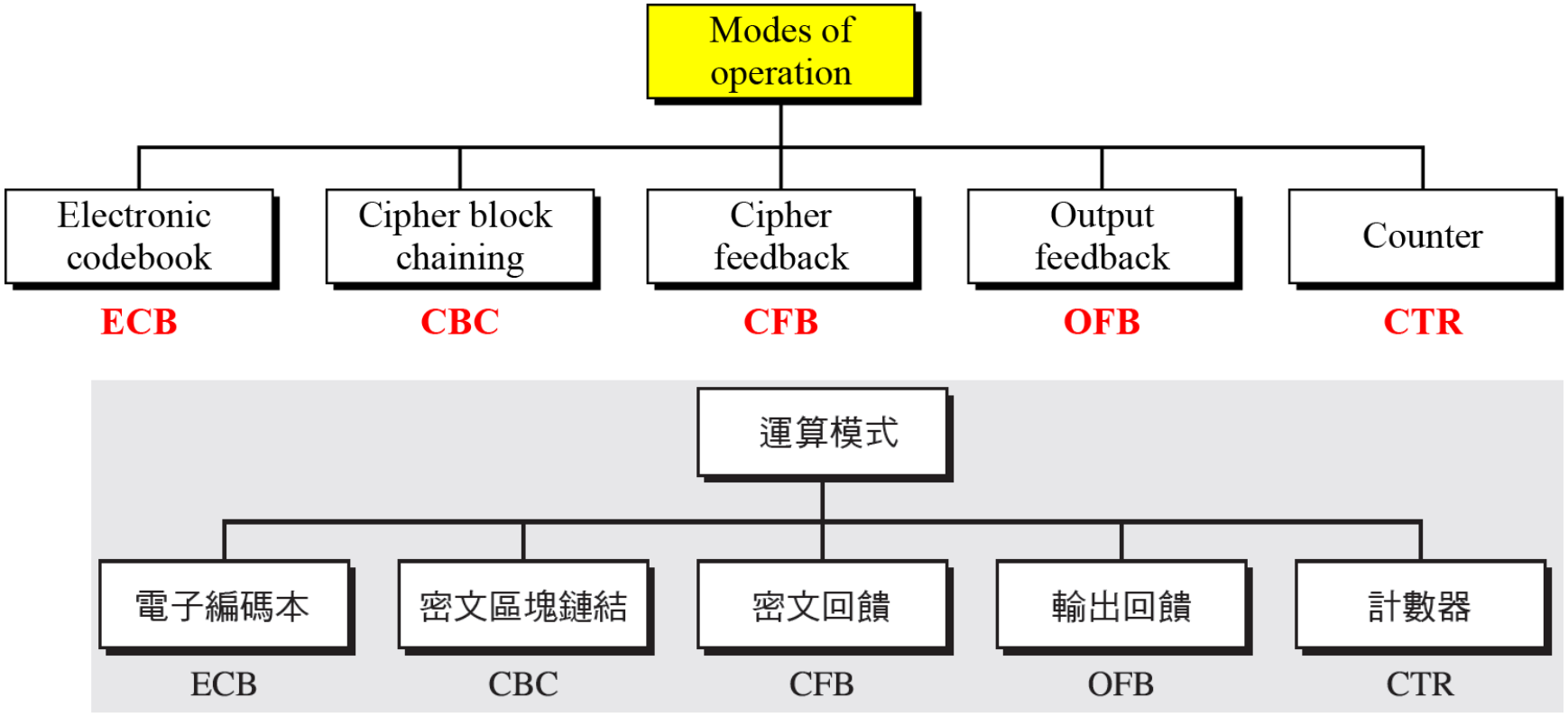
Topics discussed in this section:

Modes of Operation

- block ciphers encrypt fixed size blocks
- eg. DES encrypts 64-bit blocks, with 56-bit key
- AES encryots 128-bit block with 128-bit key
- need way to use in practise, given usually have arbitrary amount of information to encrypt
- four were defined for DES in ANSI standard ANSI X3.106-1983 Modes of Use
- subsequently now have 5 for DES and AES
- 2010, NIST added XTS-AES
- have block and stream modes

8-1 Continued

Figure 8.1 *Modes of operation*

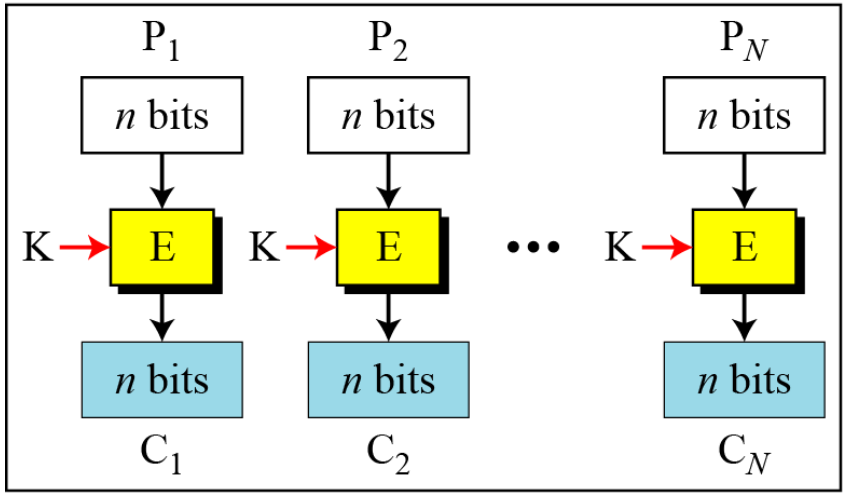


8.1.1 Electronic Codebook (ECB) Mode

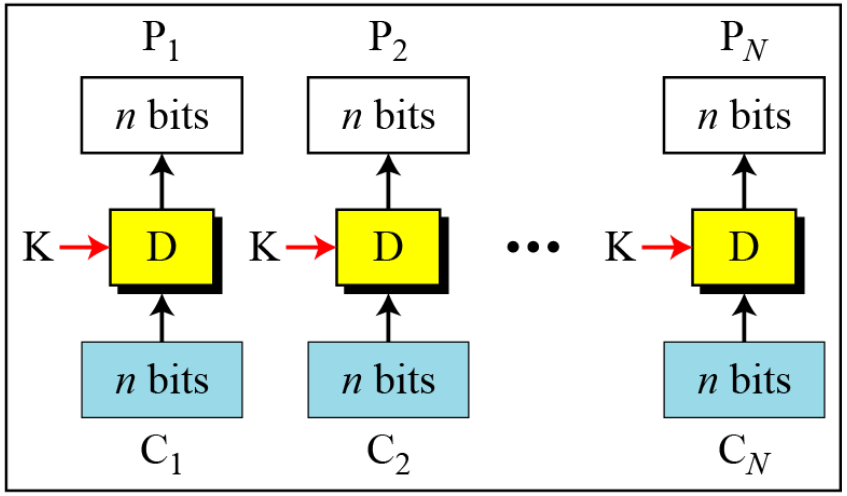
***The simplest mode of operation is called the electronic codebook (ECB) mode.*電子編碼本模式**

Encryption: $C_i = E_K(P_i)$ Decryption: $P_i = D_K(C_i)$

E: Encryption D: Decryption
P_i: Plaintext block i C_i: Ciphertext block i
K: Secret key



Encryption



Decryption

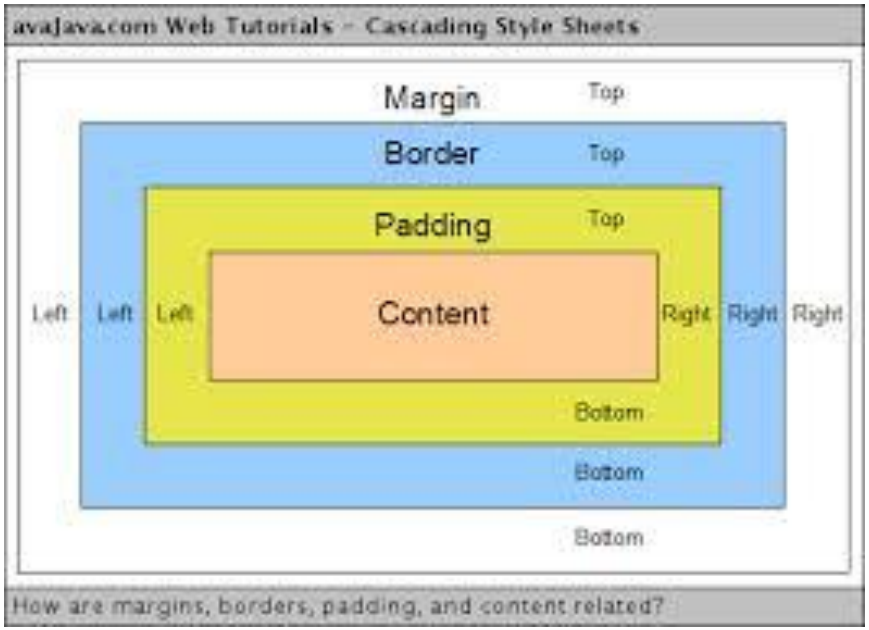
8.1.1 Error Propagation 誤差增值

A single bit error **in** ***transmission*** **can** *create errors in several bits in the corresponding decipher block.* ***However,*** *the error does not have any effect on the other blocks.*

Advantages and Limitations of ECB

- repetitions in message may show in ciphertext
  - if aligned with message block
  - particularly with data such graphics
  - or with messages that change very little, which become a code-book analysis problem
- weakness due to encrypted message blocks being independent
- main use is sending a few blocks of data

What is padding?

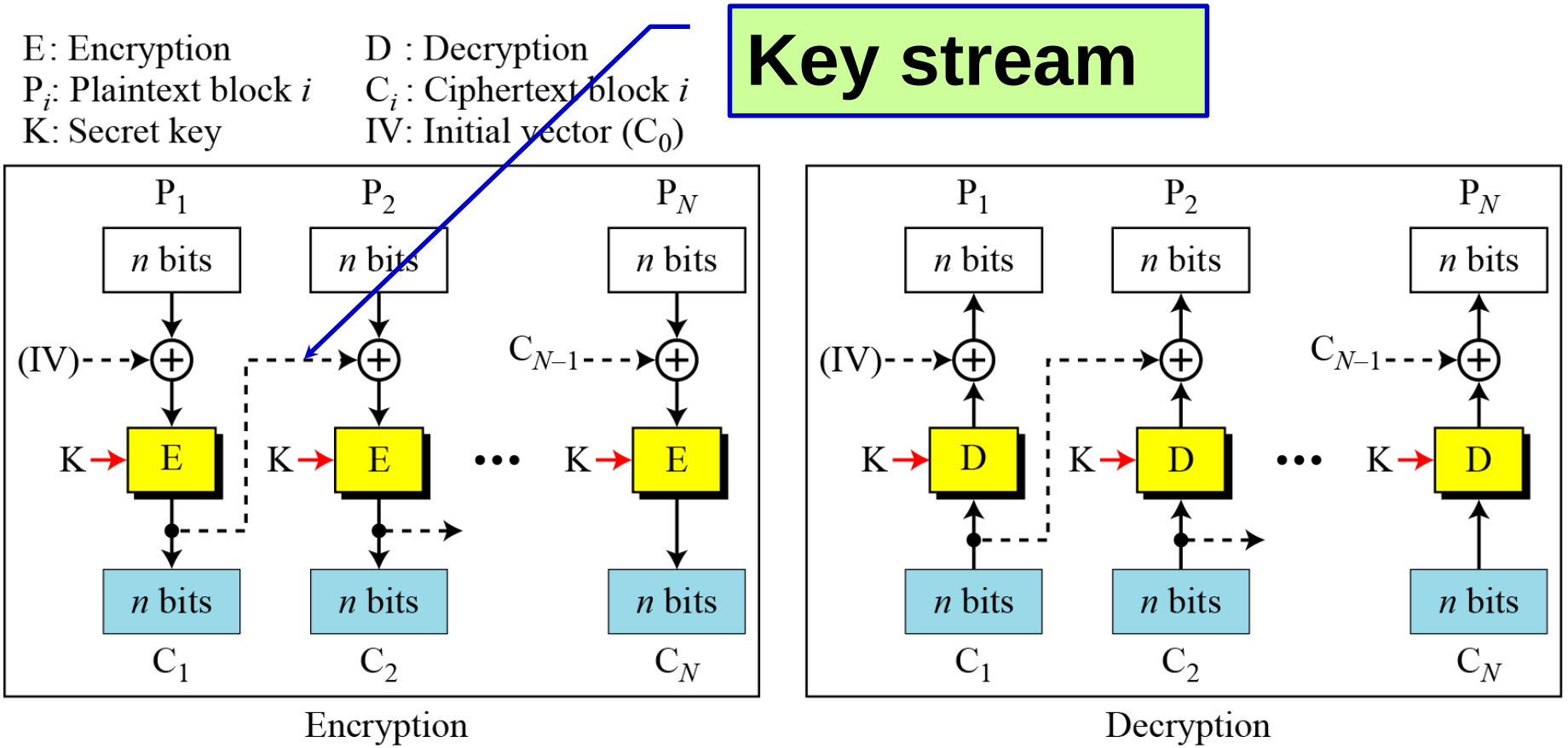


Class challenge: why block encryption need padding

8.1.2 Cipher Block Chaining (CBC) Mode

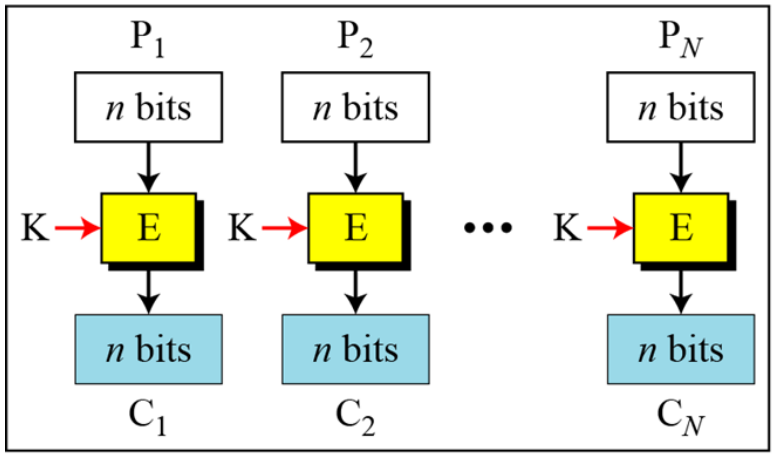
In CBC mode, each plaintext block is exclusive-ored with the previous ciphertext block before being encrypted.

Figure 8.3 *Cipher block chaining (CBC) mode*

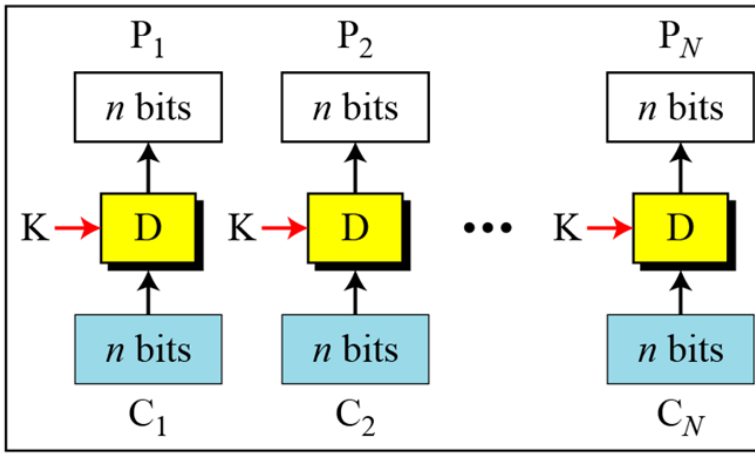


E: Encryption D: Decryption
P_i: Plaintext block i C_i: Ciphertext block i
K: Secret key

ECB



Encryption

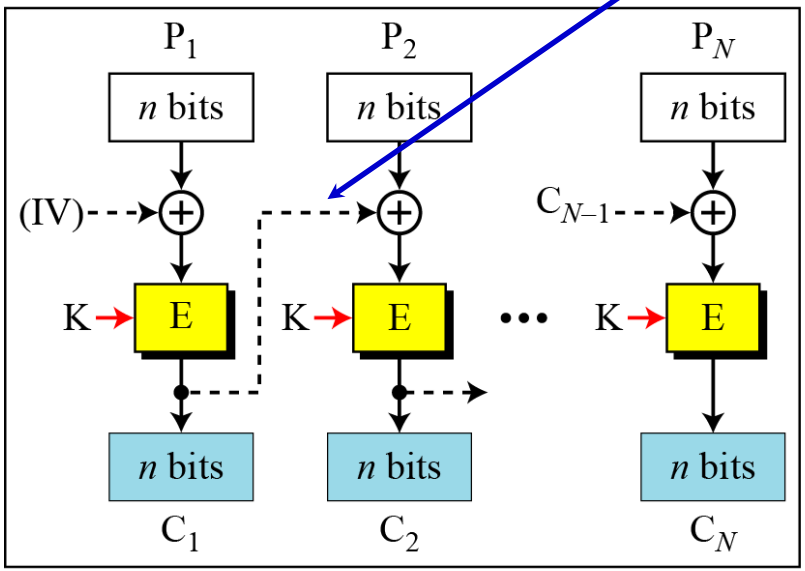


Decryption

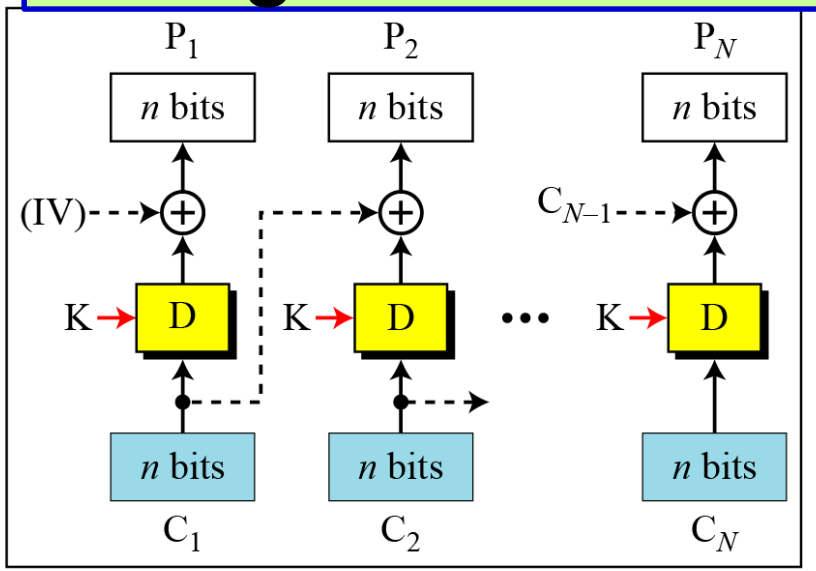
P_i: Plaintext block i C_i : Ciphertext block i
K: Secret key IV: Initial vector (C_0)

change the IVs

CBC



Encryption



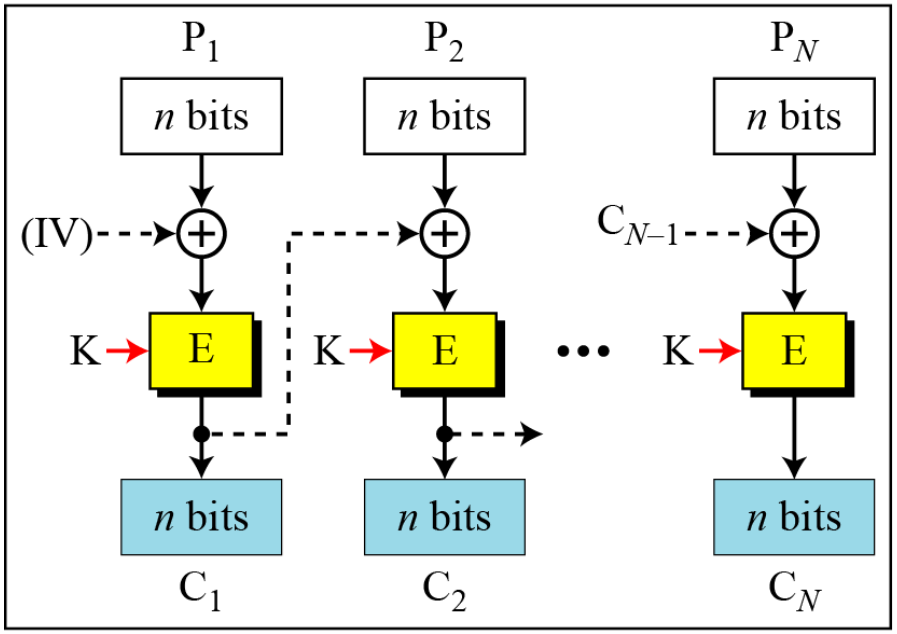
Decryption

8.1.2 Continued

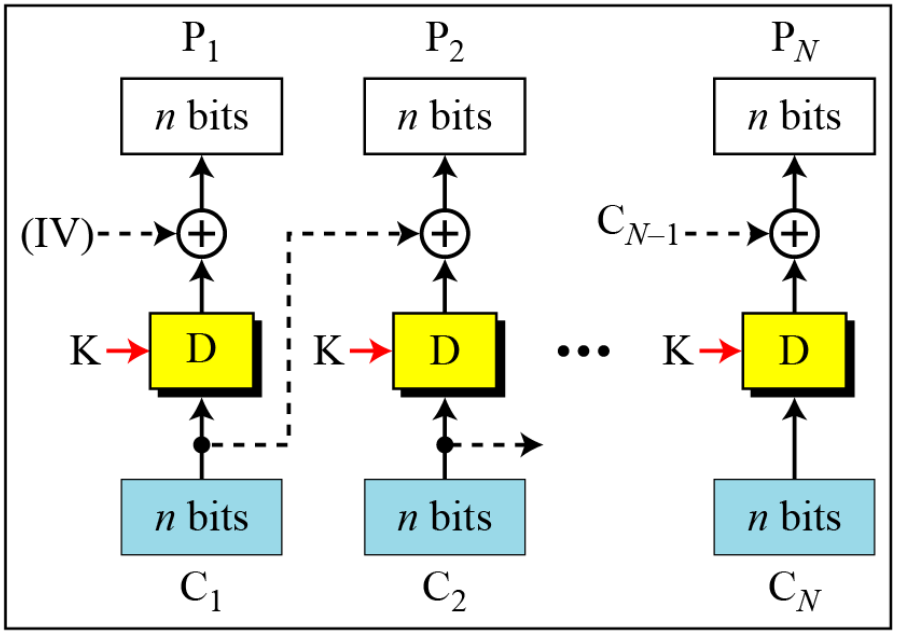
Figure 8.3 *Cipher block chaining (CBC) mode*

E: Encryption
P_i: Plaintext block *i*
K: Secret key

D : Decryption
C_i : Ciphertext block *i*
IV: Initial vector (C_0)



Encryption



Decryption

Encryption:
$C_0 = IV$
$C_i = E_K (P_i \oplus C_{i-1})$

Decryption:
$C_0 = IV$
$P_i = D_K (C_i) \oplus C_{i-1}$

8.1.2 Continued

Example 8.4

Initialization Vector (IV)

The initialization vector (IV) should be known by the sender and the receiver.

IV can be sent by ECB mode

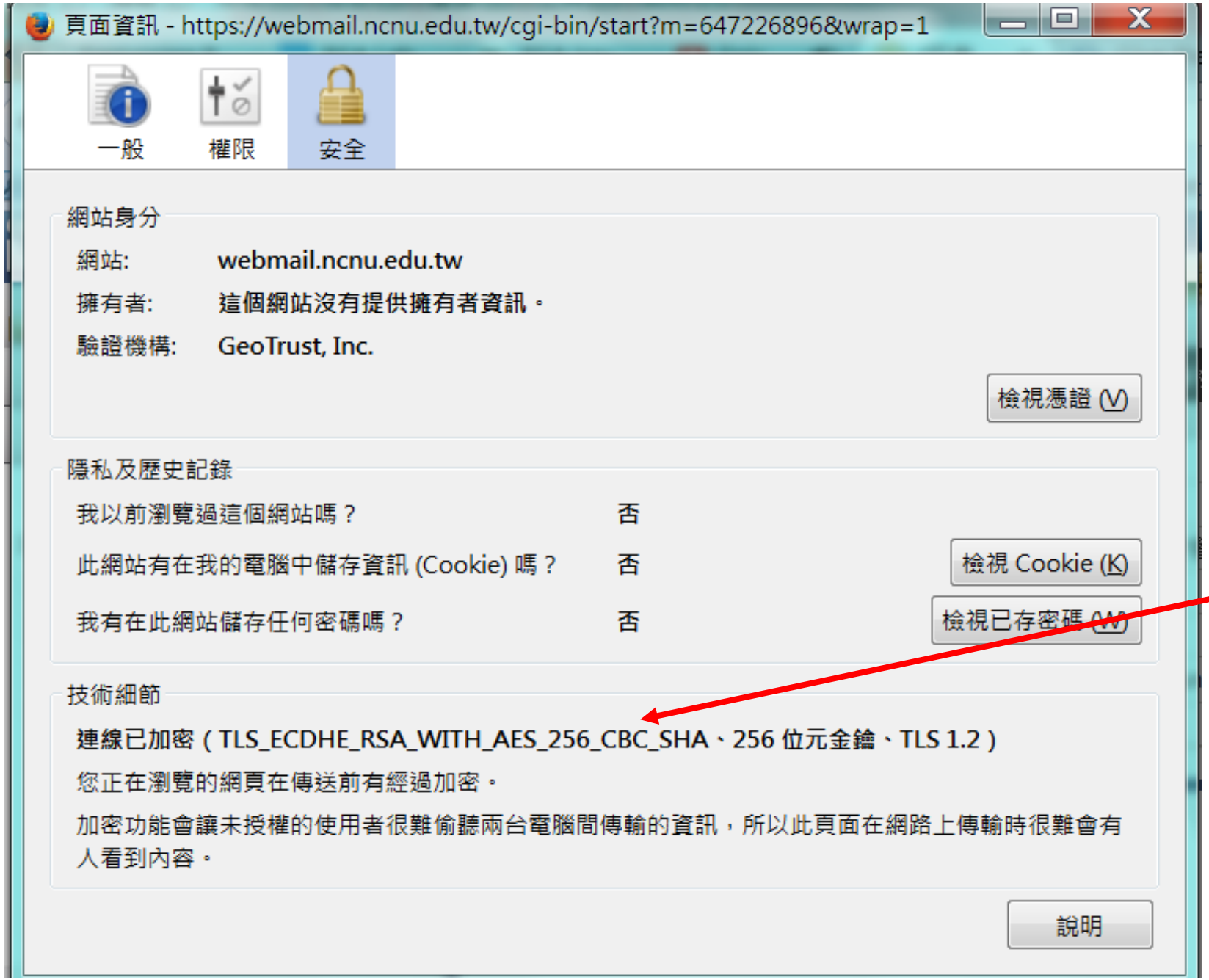
Error Propagation

In CBC mode, a single bit error in ciphertext block C_j during transmission may create error in most bits in plaintext block P_j & P_{j+1} during decryption.

Advantages and Limitations of CBC

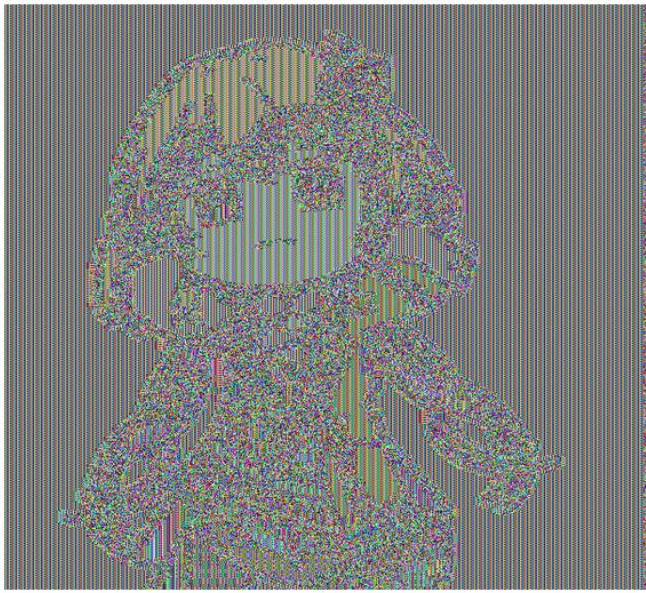
uses: bulk data encryption, authentation

- **each ciphertext block depends on all message blocks**
- **thus a change in the message affects all ciphertext blocks after the change as well as the original block**
- **need Initial Value (IV) known to sender & receiver**
  - **however if IV is sent in the clear, an attacker can change bits of the first block, and change IV to compensate**
  - **hence either IV must be a fixed value (as in EFTPOS) or it must be sent encrypted in ECB mode before rest of message**
- **at end of message, handle possible last short block**
  - **by padding either with known non-data value (eg nulls)**
  - **or pad last block with count of pad size**
    - **eg. [b1 b2 b3 0 0 0 0 5] <- 3 data bytes, then 5 bytes pad+count**
- **cannot parallel processing; one error in plain/cipher would affect other block encrypt/decrypt**


頁面資訊 - https://webmail.ncnu.edu.tw/cgi-bin/start?m=647226896&wrap=1
一般
權限
安全
網站身分
網站: webmail.ncnu.edu.tw
擁有者: 這個網站沒有提供擁有者資訊。
驗證機構: GeoTrust, Inc.
檢視憑證 (V)
隱私及歷史記錄
我以前瀏覽過這個網站嗎？ 否
此網站有在我的電腦中儲存資訊 (Cookie) 嗎？ 否
檢視 Cookie (K)
我有在此網站儲存任何密碼嗎？ 否
檢視已存密碼 (W)
技術細節
連線已加密 (TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA、256 位元金鑰、TLS 1.2)
您正在瀏覽的網頁在傳送前有經過加密。
加密功能會讓未授權的使用者很難偷聽兩台電腦間傳輸的資訊，所以此頁面在網路上傳輸時很難會有人看到內容。
說明

ECB vs CBC image file :范植鈞

原圖



ECB加密

CBC加密

8.1.3 Cipher Feedback (CFB) Mode

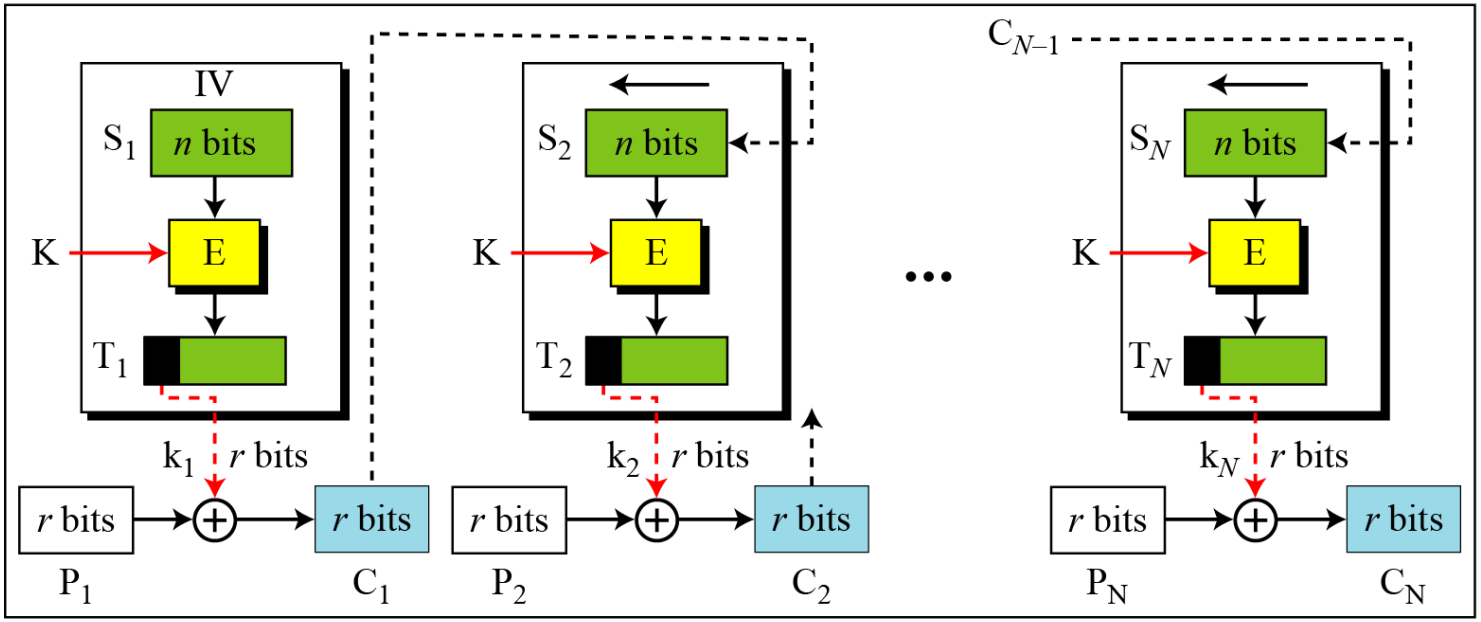
In some situations, we need to use DES or AES as secure ciphers, but the plaintext or ciphertext block sizes are to be smaller. *與(OFB) Mode比較的相對優點：若每次的IV值一樣時，加密區塊的Pi與上次的Pi 值不一樣，則Ci會不一樣，故 送到下一個區塊的register 的key stream不一樣，故不曾產生同樣的密文，故有confusion效果。*

Figure 8.4 *Encryption in cipher feedback (CFB) mode*

E : Encryption
P_i: Plaintext block *i*
K: Secret key

D : Decryption
C_i: Ciphertext block *i*
IV: Initial vector (S_1)

S_i: Shift register
T_i: Temporary register

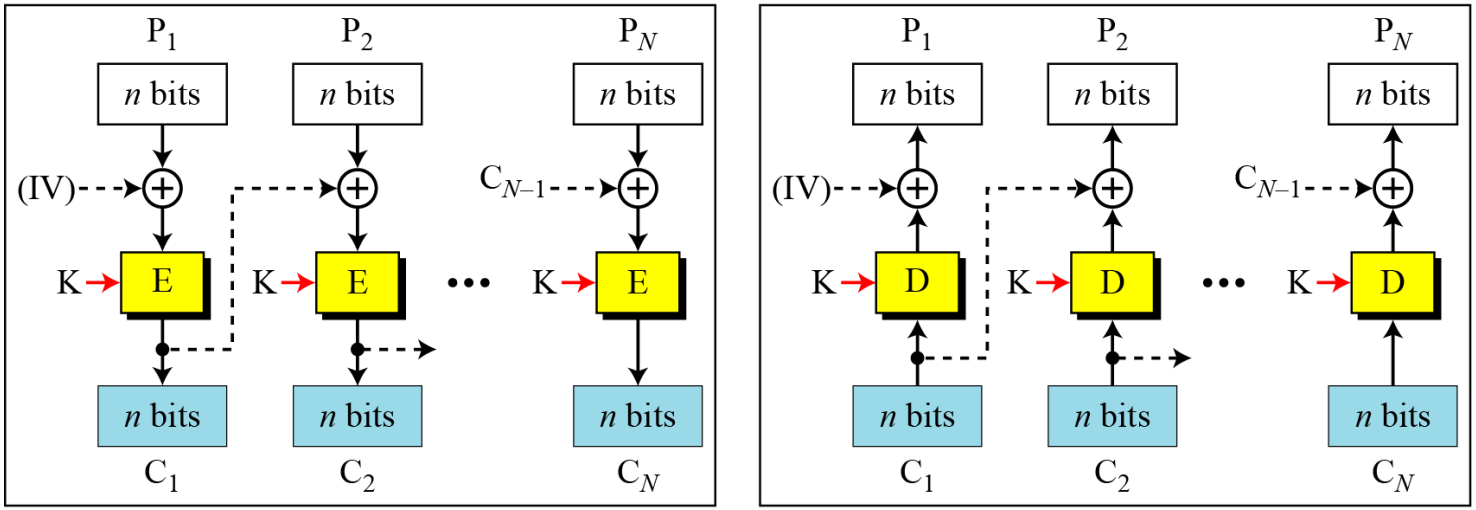


Encryption

8.1.3 Cipher Feedback (CFB) Mode

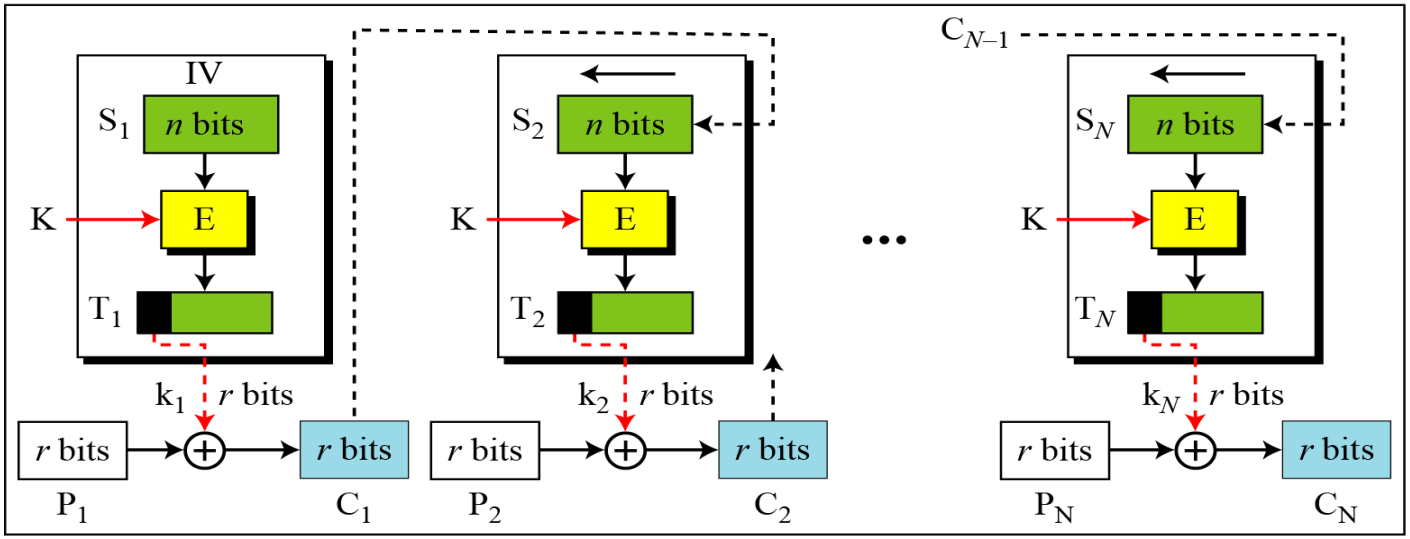
E: Encryption D : Decryption
P_i: Plaintext block i C_i : Ciphertext block i
K: Secret key IV: Initial vector (C_0)

CBC

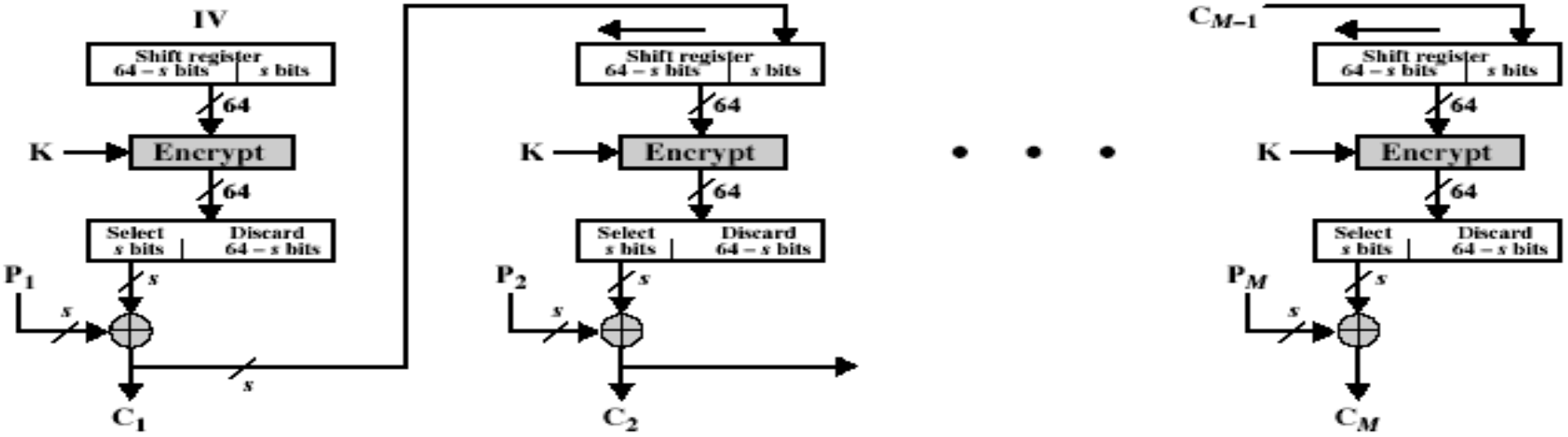


P_i: Plaintext block i C_i : Ciphertext block i T_i: Temporary register
K: Secret key IV: Initial vector (S_1)

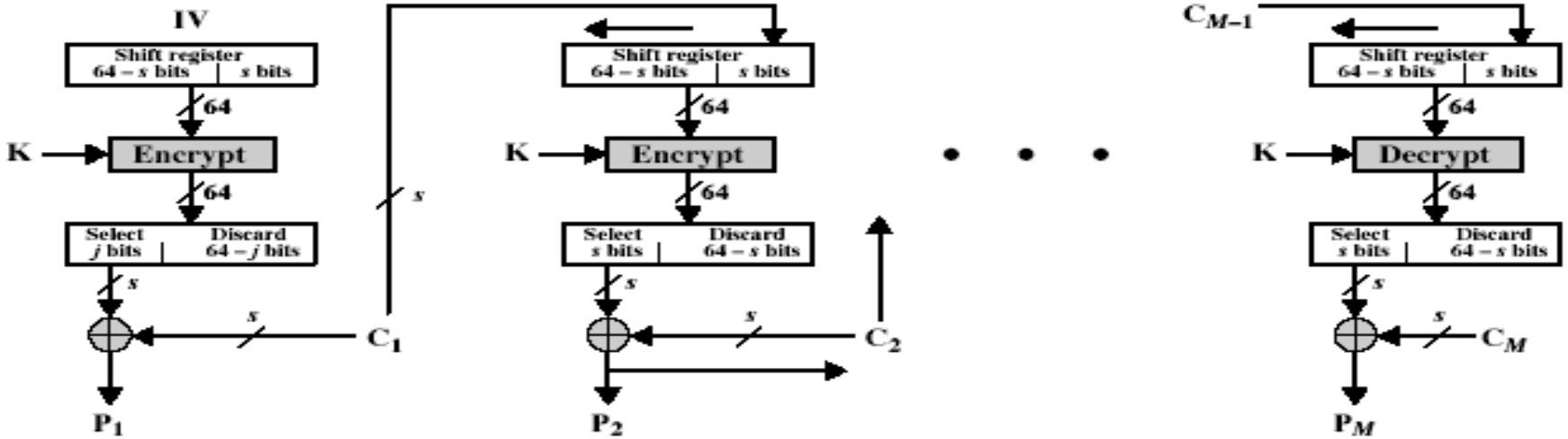
CFB



Cipher FeedBack (CFB- 以 DES 64為例)



(a) Encryption



(b) Decryption

Cipher FeedBack (CFB)

- message is treated as a stream of bits
- added to the output of the block cipher
- result is feed back for next stage (hence name)
- standard allows any number of bit (1,8 or 64 or whatever) to be feed back
  - denoted CFB-1, CFB-8, CFB-64 etc
- is most efficient to use all 64 bits (CFB-64)

$$C_i = P_i \text{ XOR } DES_{K1}(C_{i-1})$$

$$C_{-1} = IV$$

- uses: stream data encryption, authentication

Advantages and Limitations of CFB

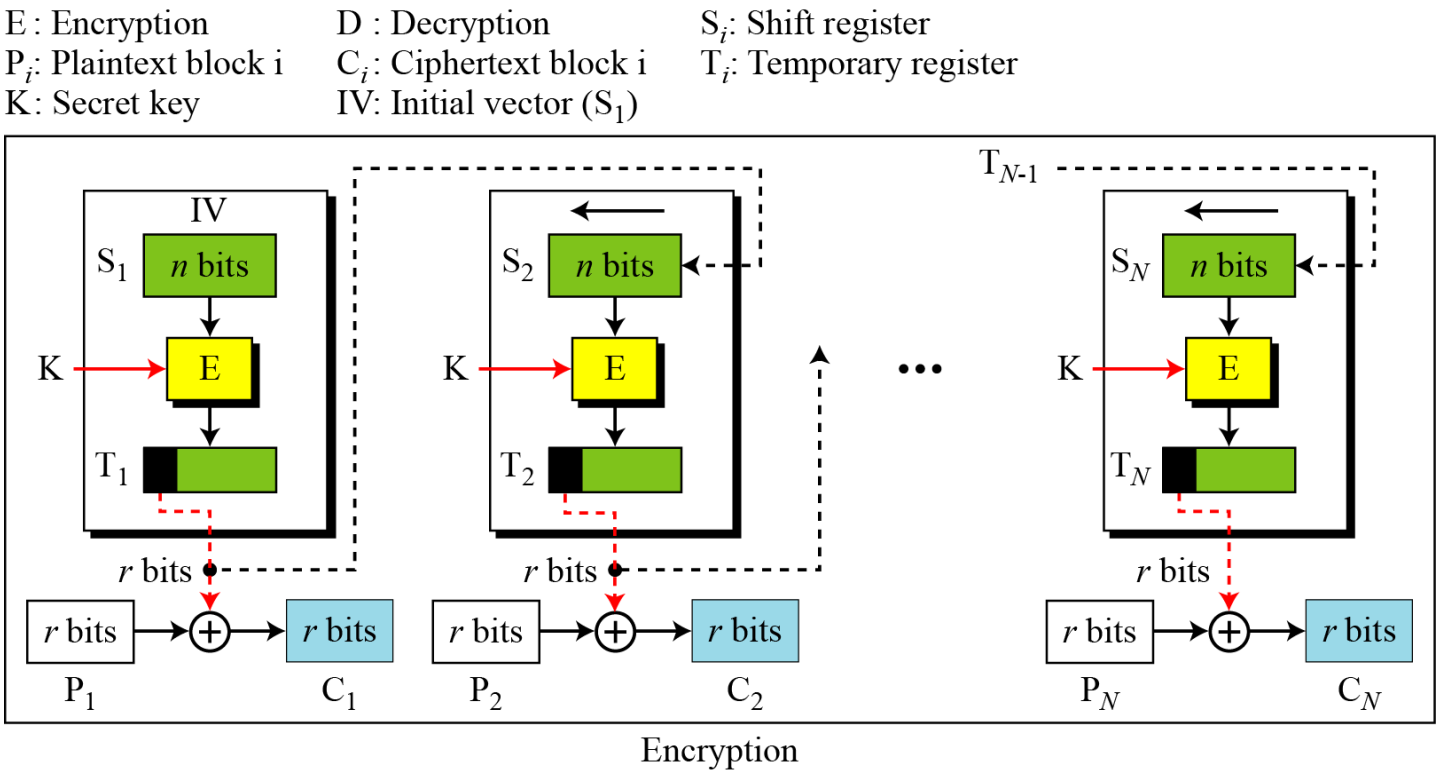
- appropriate when data arrives in bits/bytes
- most common stream mode
- limitation is need to stall while do block encryption after every n-bits
- note that the block cipher is used in encryption mode at both ends
- errors propogate for several blocks after the error (指 tx error)
- cannot parallel processing; one error in plain/cipher would affect other block encrypt/decrypt

18.1.4 Output Feedback (OFB) Mode

In this mode each bit in the ciphertext is independent of the previous bit or bits. This avoids error propagation.

與(CFB) Mode的相對 缺點：若每次的IV值一樣時，產生的key stream皆一樣，即使加密區塊的Pi與上次的Pi 值不一樣，但送到下一個區塊的register 的key stream 皆相同。故沒有confusion效果。

Figure 8.6 *Encryption in output feedback (OFB) mode*



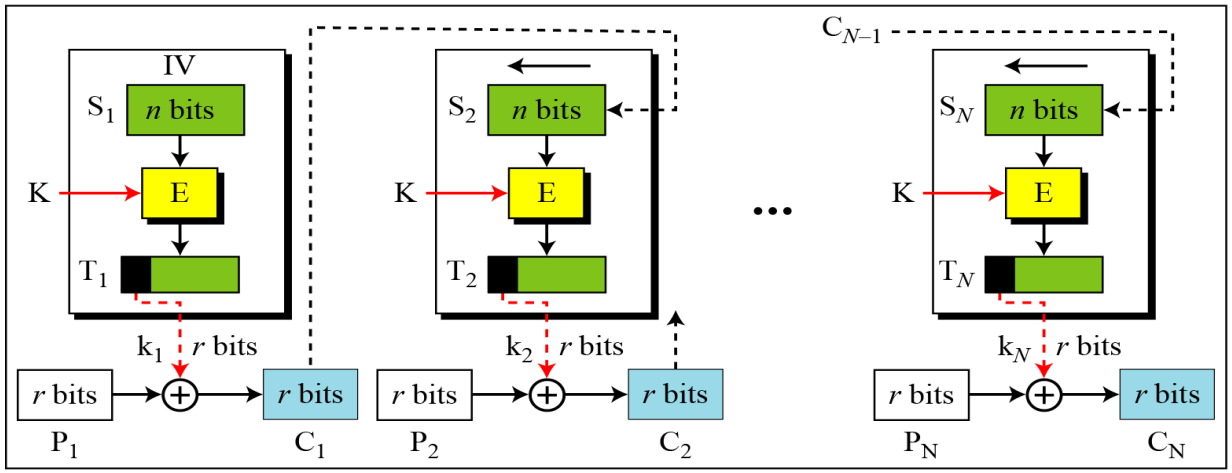
18.1.4 Output Feedback (OFB) Mode

CFB

E : Encryption
P_i: Plaintext block i
K: Secret key

D : Decryption
C_i: Ciphertext block i
IV: Initial vector (S_1)

S_i: Shift register
T_i: Temporary register



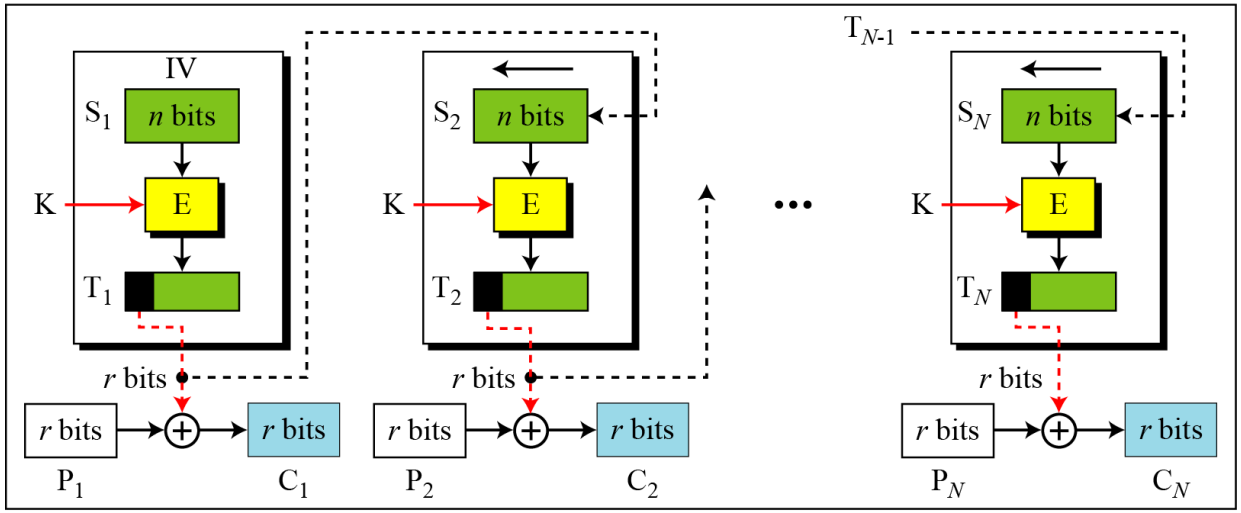
Encryption

OFB

E : Encryption
P_i: Plaintext block i
K: Secret key

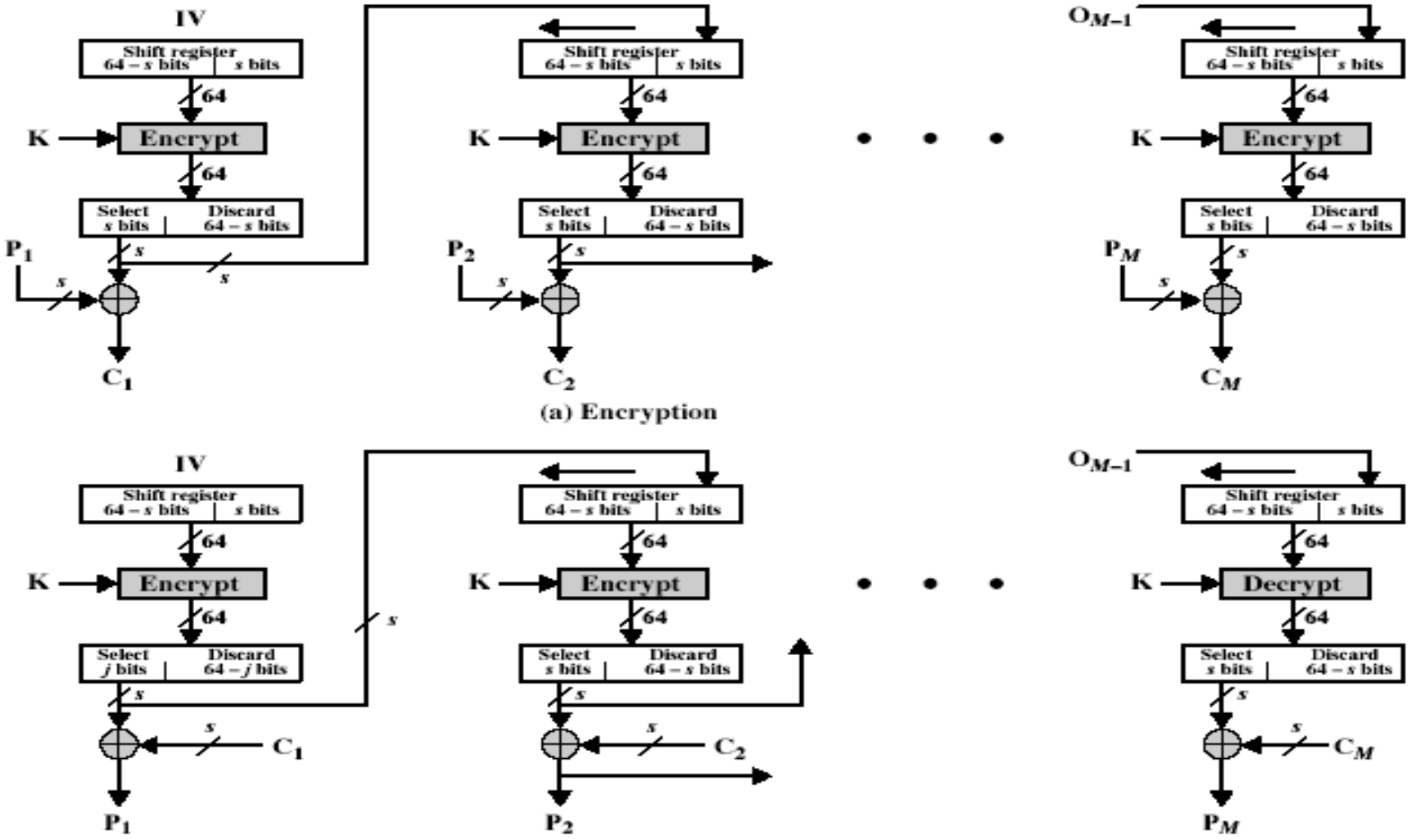
D : Decryption
C_i: Ciphertext block i
IV: Initial vector (S_1)

S_i: Shift register
T_i: Temporary register



Encryption

Output FeedBack (OFB)



Output FeedBack (OFB)

- message is treated as a stream of bits
- output of cipher is added to message
- output is then feed back (hence name)
- feedback is independent of message
- can be computed in advance

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

$$O_i = DES_{K1}(O_{i-1})$$

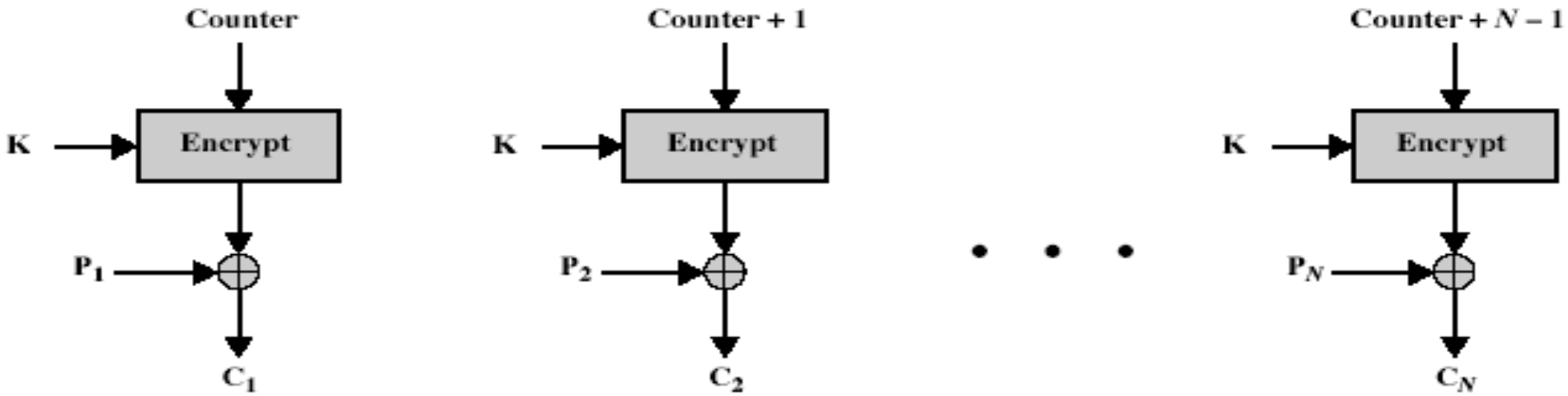
$$O_{-1} = IV$$

- uses: stream encryption over noisy channels(compared with CFB)

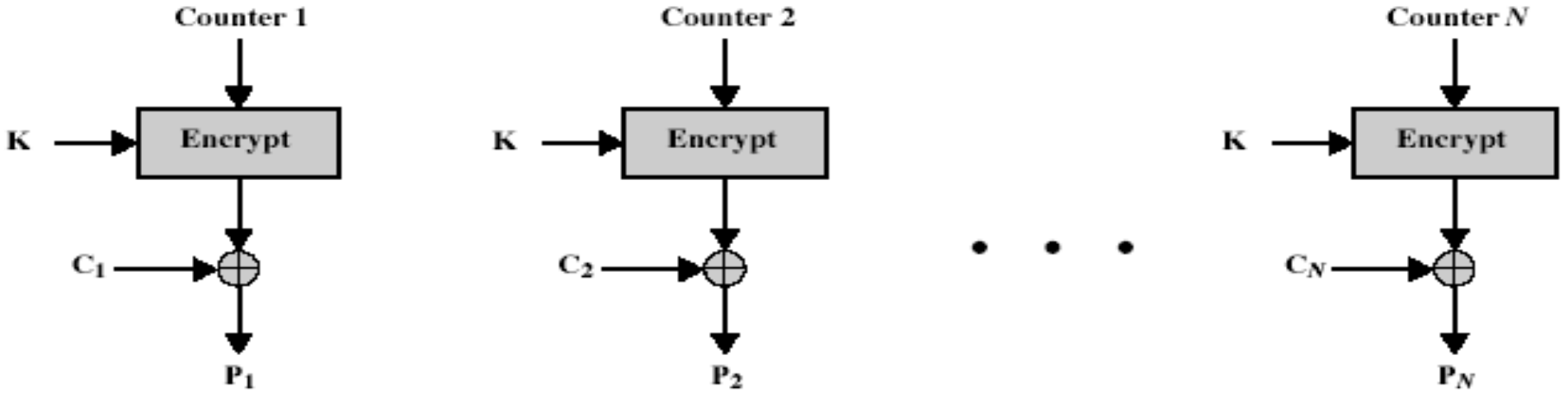
Advantages and Limitations of OFB

- used when error feedback a problem or where need to encryptions before message is available
- superficially similar to CFB
- but feedback is from the output of cipher and is independent of message
- a variation of a Vernam cipher
  - hence must never reuse the same sequence (key+IV)
- sender and receiver must remain in sync, and some recovery method is needed to ensure this occurs
- originally specified with m-bit feedback in the standards
- subsequent research has shown that only OFB-64 should ever be used
- cannot parallel processing; one error in plain/cipher would not affect other block encrypt/decrypt

Counter (CTR)



(a) Encryption

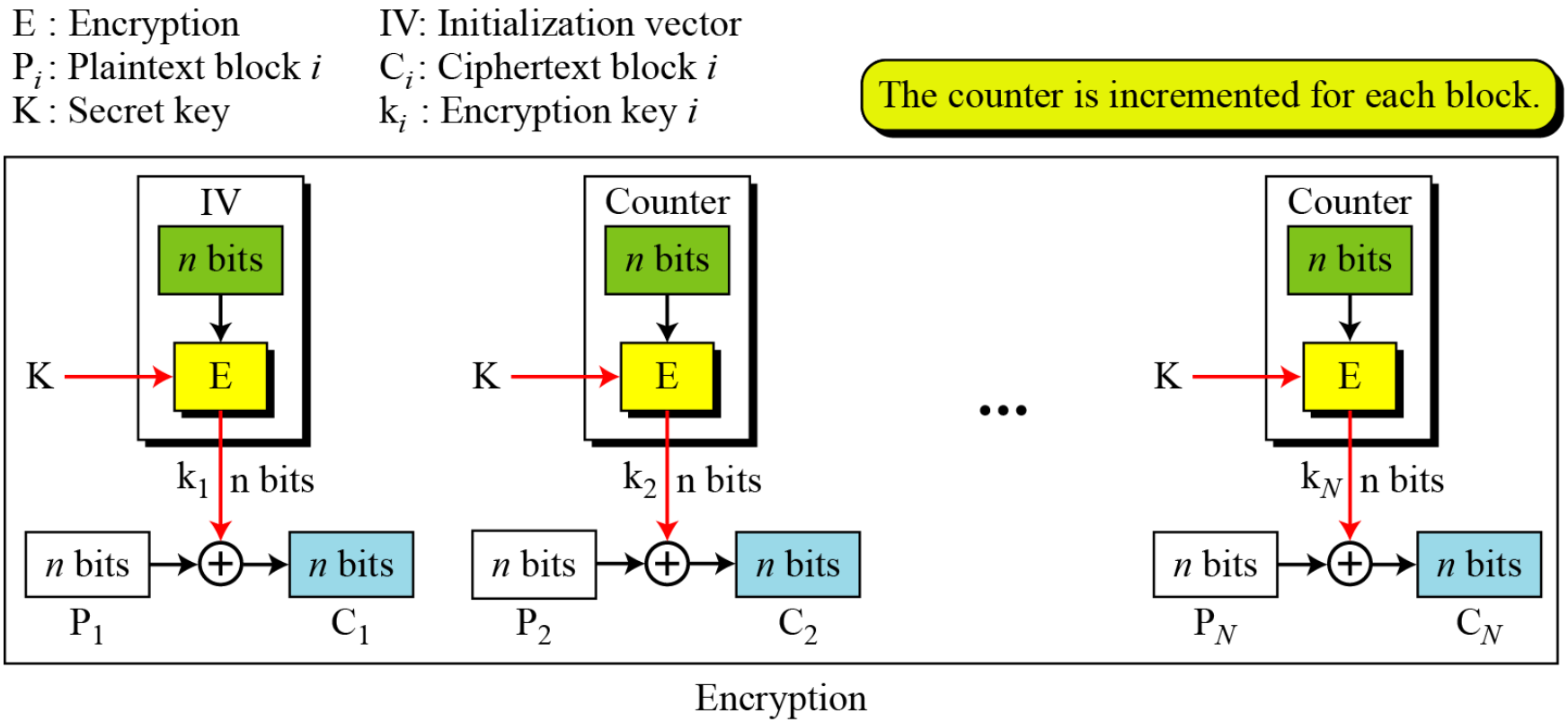


(b) Decryption

8.1.5 Counter (CTR) Mode

In the counter (CTR) mode, there is no feedback. The pseudorandomness in the key stream is achieved using a counter.

Figure 8.8 *Encryption in counter (CTR) mode*



Counter (CTR)

- a “new” mode, though proposed early on
- similar to OFB but encrypts counter value rather than any feedback value
- must have a different key & counter value for every plaintext block (never reused)

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

$$O_i = DES_{K1}(i)$$

- uses: high-speed network encryptions

Advantages and Limitations of CTR

- **efficiency**
  - **can do parallel encryptions**
  - **in advance of need**
  - **good for bursty high speed links (ATM)**
- **random access to encrypted data blocks**
- **provable security (good as other modes)**
- **but must ensure never reuse key/counter values, otherwise could break (cf OFB)**

Counter with cipher block chaining message authentication code (CCM)

- Counter with cipher block chaining message authentication code (counter with CBC-MAC; CCM)
- an authenticated encryption algorithm designed to provide both authentication and confidentiality
- CCM mode is only defined for block ciphers with a block length of 128 bits

進階

Comparison of Different Modes

Table 8.1 *Summary of operation modes*

Operation Mode	*Description*	*Type of Result*	*Data Unit Size*
ECB	Each n-bit block is encrypted independently with the same cipher key.	Block cipher	n
CBC	Same as ECB, but each block is first exclusive-ored with the previous ciphertext.	Block cipher	n
CFB	Each r-bit block is exclusive-ored with an r-bit key, which is part of previous cipher text	Stream cipher	$r \leq n$
OFB	Same as CFB, but the shift register is updated by the previous r-bit key.	Stream cipher	$r \leq n$
CTR	Same as OFB, but a counter is used instead of a shift register.	Stream cipher	n

Videos

- Modes of AES Encryption - Part 1 - http://www.youtube.com/watch?v=BGHCcDvJTek&feature=related
- Rijmen-Daemen in Belgium http://www.youtube.com/watch?v=Fk1jGo8uzcY
- Vincent Rijmen - IAIK - Graz University of Technology

http://www.iaik.tugraz.at/content/about_iaik/people/rijmen_vincent/

Homework

- 查出 802.11 加密的弱點 及 802.11x 如何改善
  - WLAN 802.11x 中加密用何種 mode
  - 802.11i提供使用Temporal Key Integrity Protocol (TKIP)及counter mode with the CBC-MAC protocol (CCMP)，其中TKIP延用RC4的演算法而CCMP則是利用AES演算法。
- 整理 5 種 modes 的特質及用途

	Block? Stream ?	Tx errors 對解密的影響	加密時,同樣明文是否產生相同密文	特質or應用	平行處理
ECB					
CBC					
CFB					
OFB					
CTR					