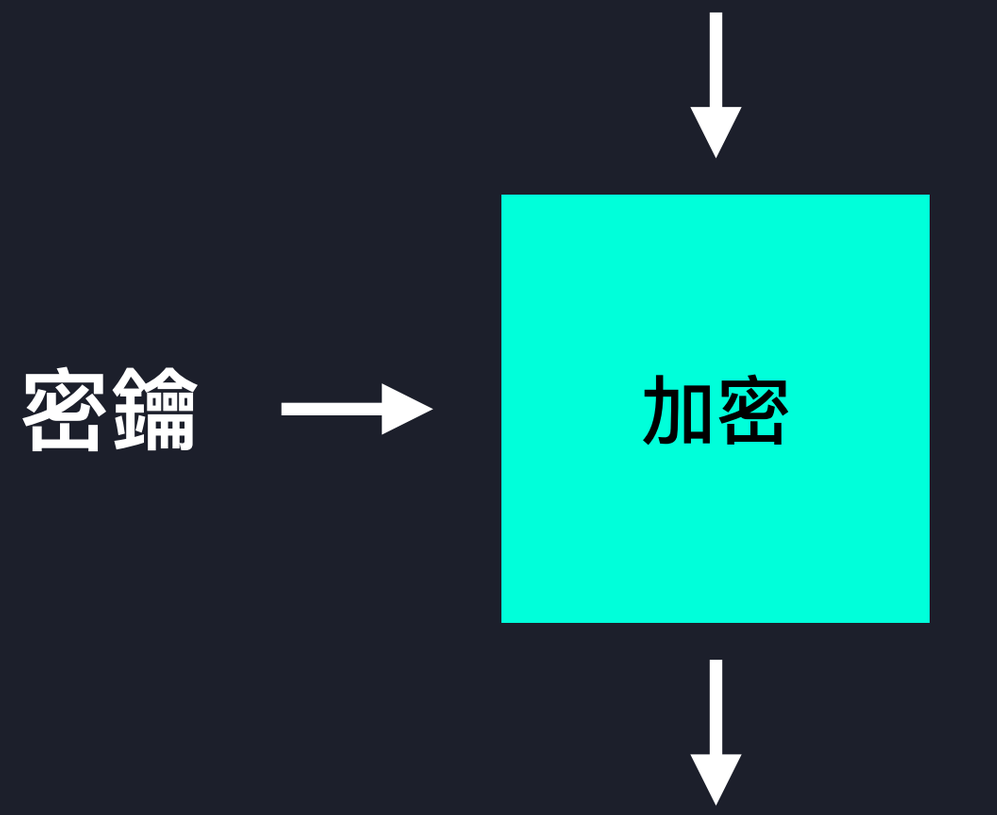
CRYPTO - Symmetric Key

OAlienO

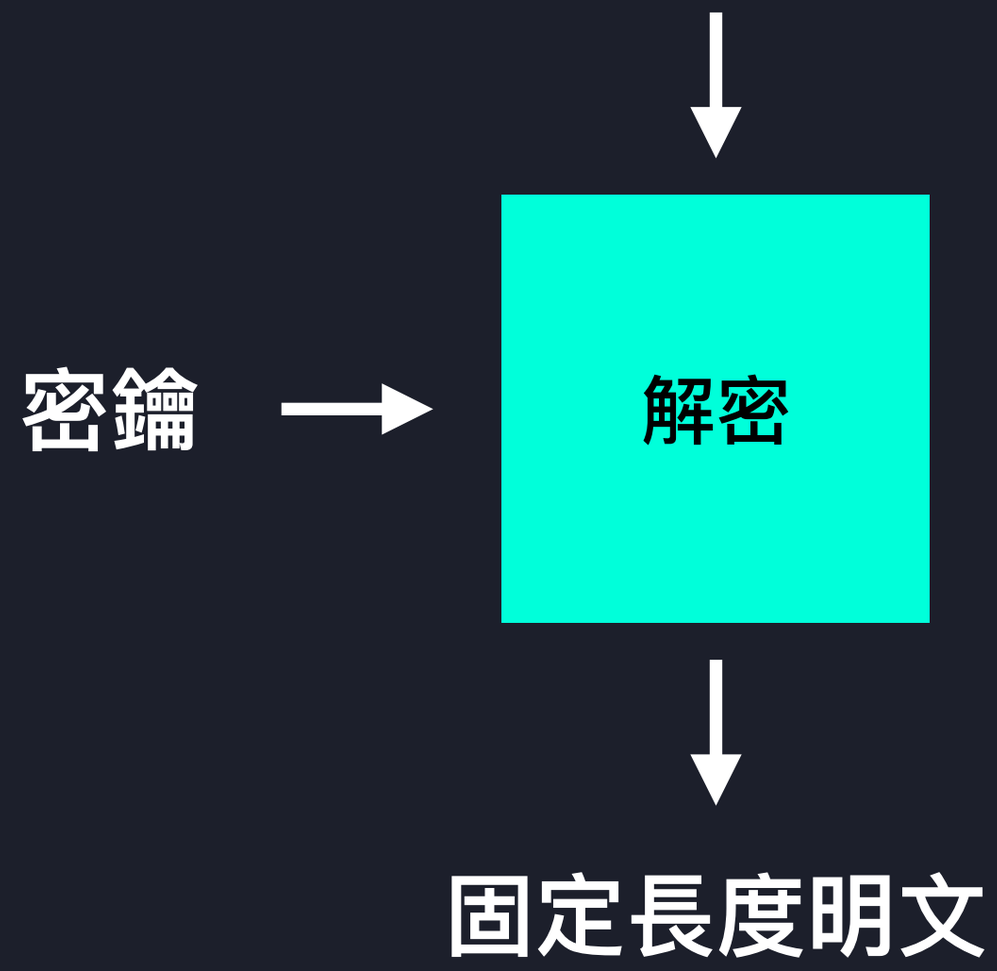
目錄

Introduction to Block Cipher

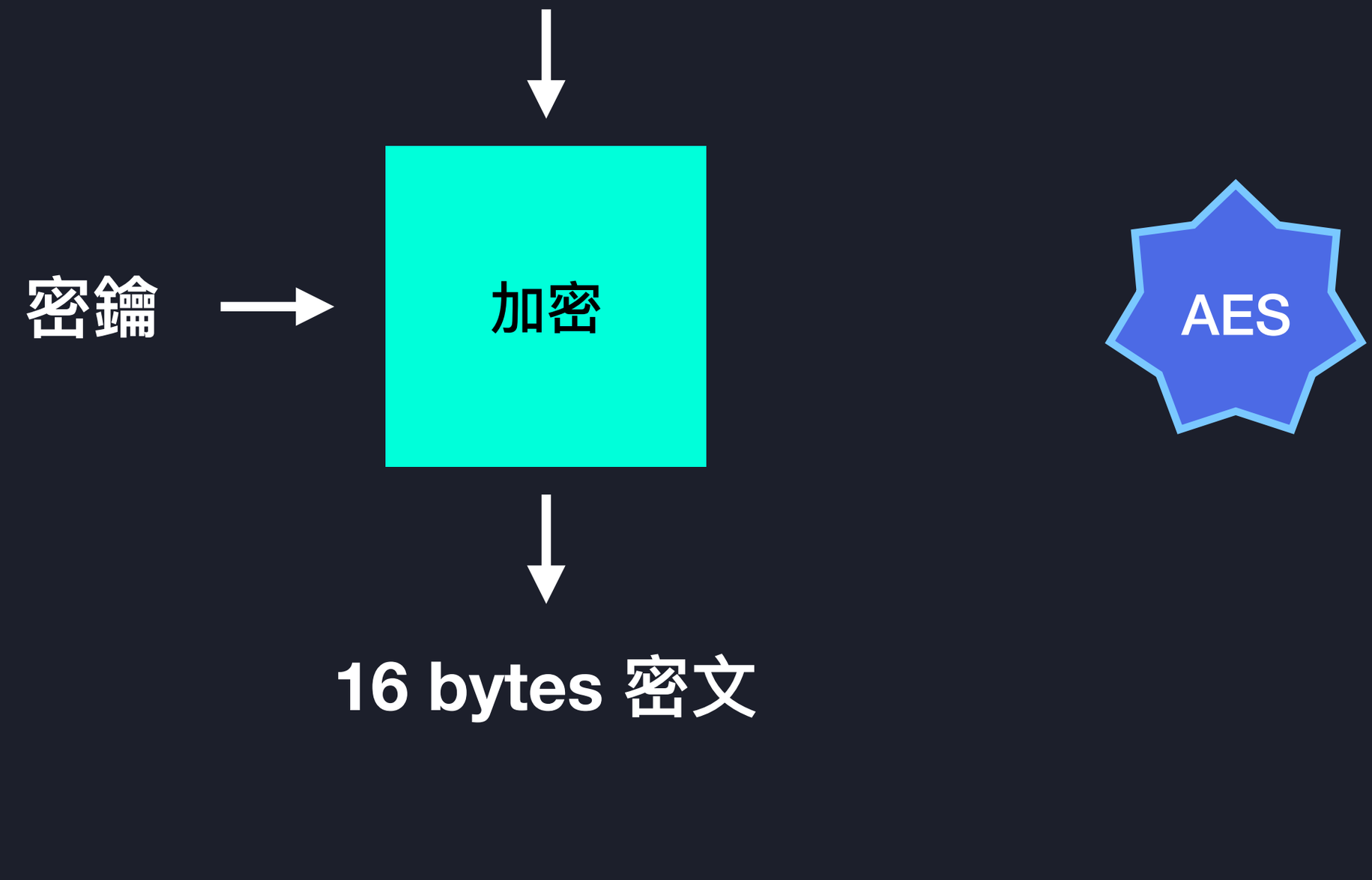
Introduction to Block Cipher



Introduction to Block Cipher



Introduction to Block Cipher



Introduction to Block Cipher

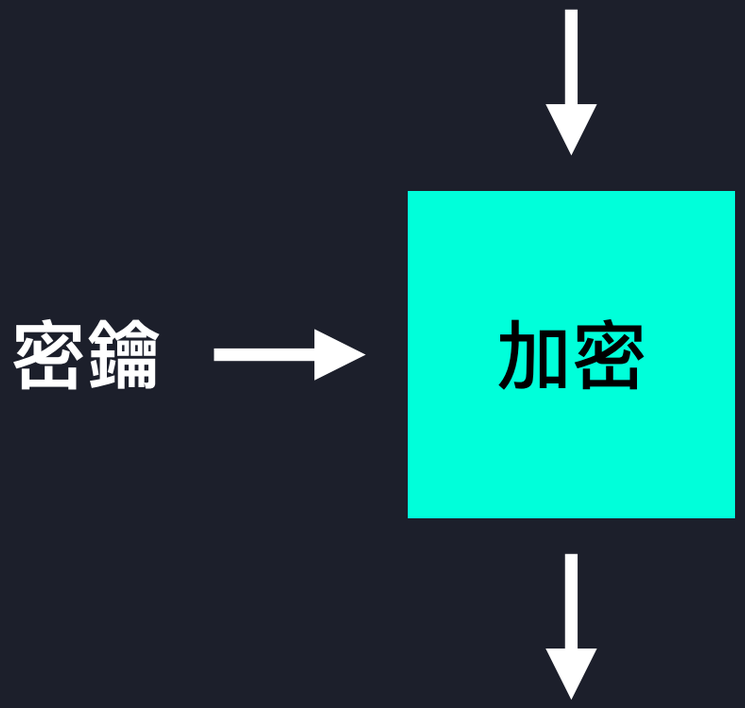
我要加密的明文不是 16 bytes 怎麼辦？

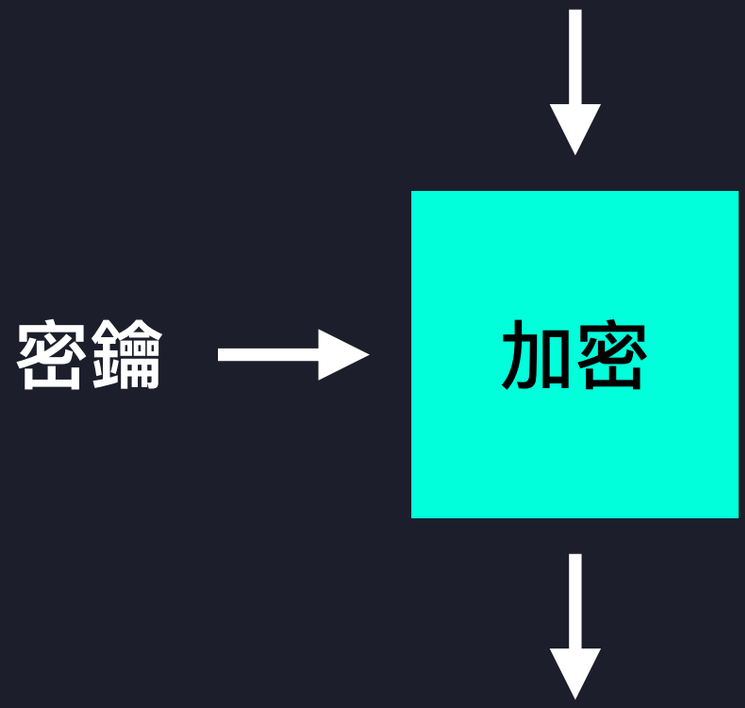
切成很多個 16 bytes

Introduction to Block Cipher

16 bytes 明文

14 bytes 明文 + 2 bytes 填充 (padding)

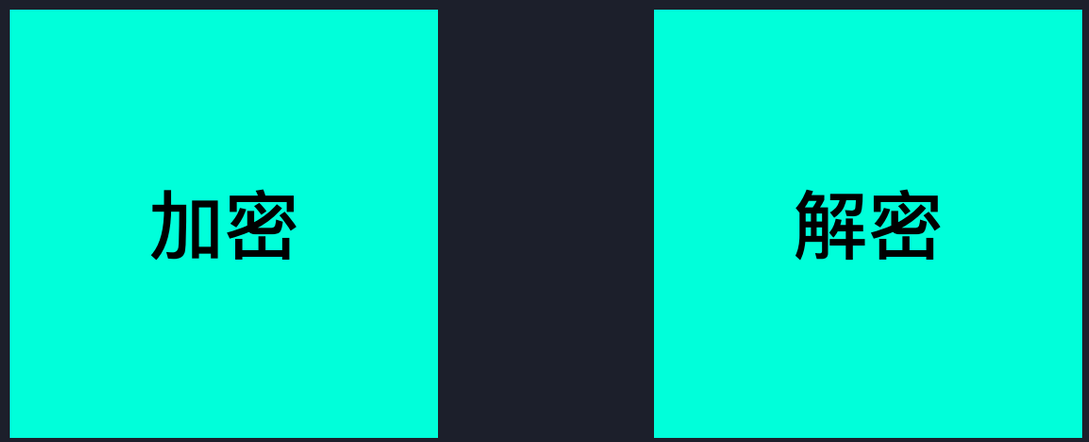




16 bytes 密文

16 bytes 密文

Introduction to Block Cipher



這個框框裡面做了什麼事？

這邊不討論

Introduction to Block Cipher

什麼是 Block Cipher Mode ?

對多個區塊密文的加工方式

Introduction to Block Cipher

常見的對稱式區塊密碼:

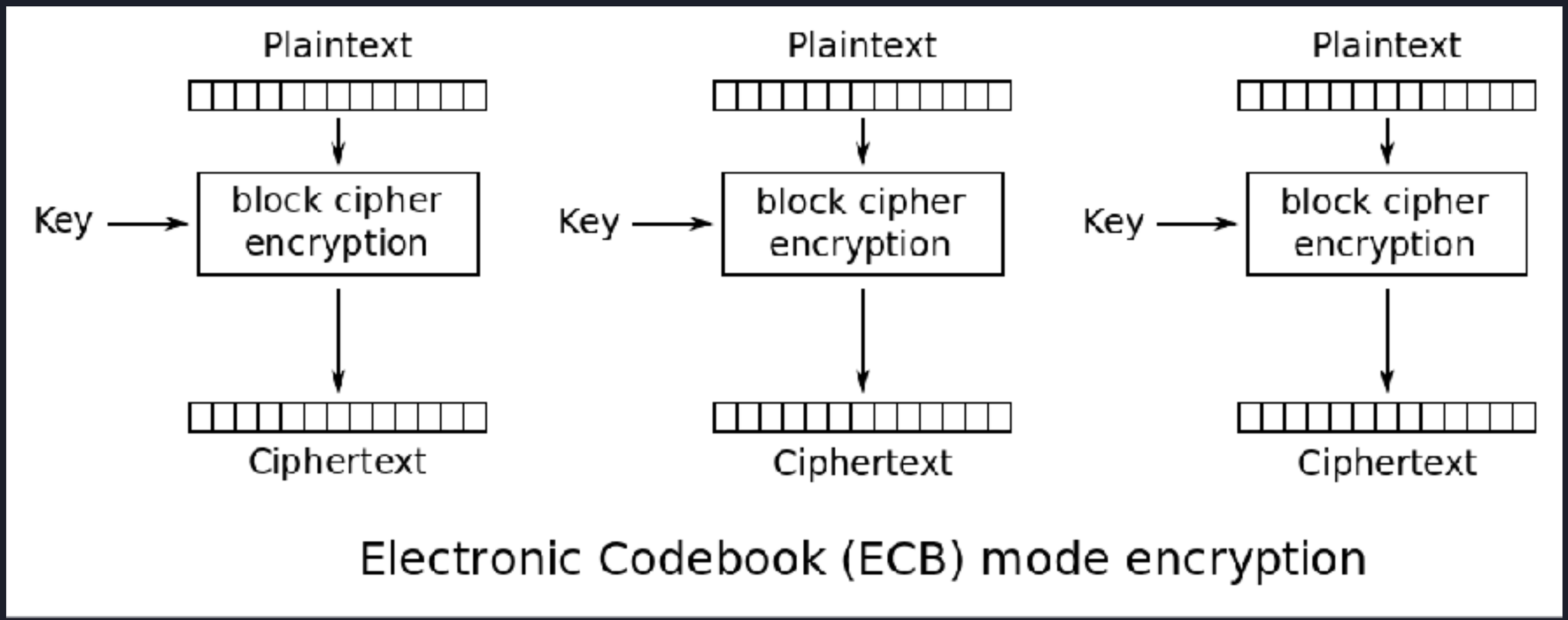
Advanced Encryption Standard (AES)

Data Encryption Standard (DES)

Block Cipher Mode - ECB

Block Cipher Mode - ECB

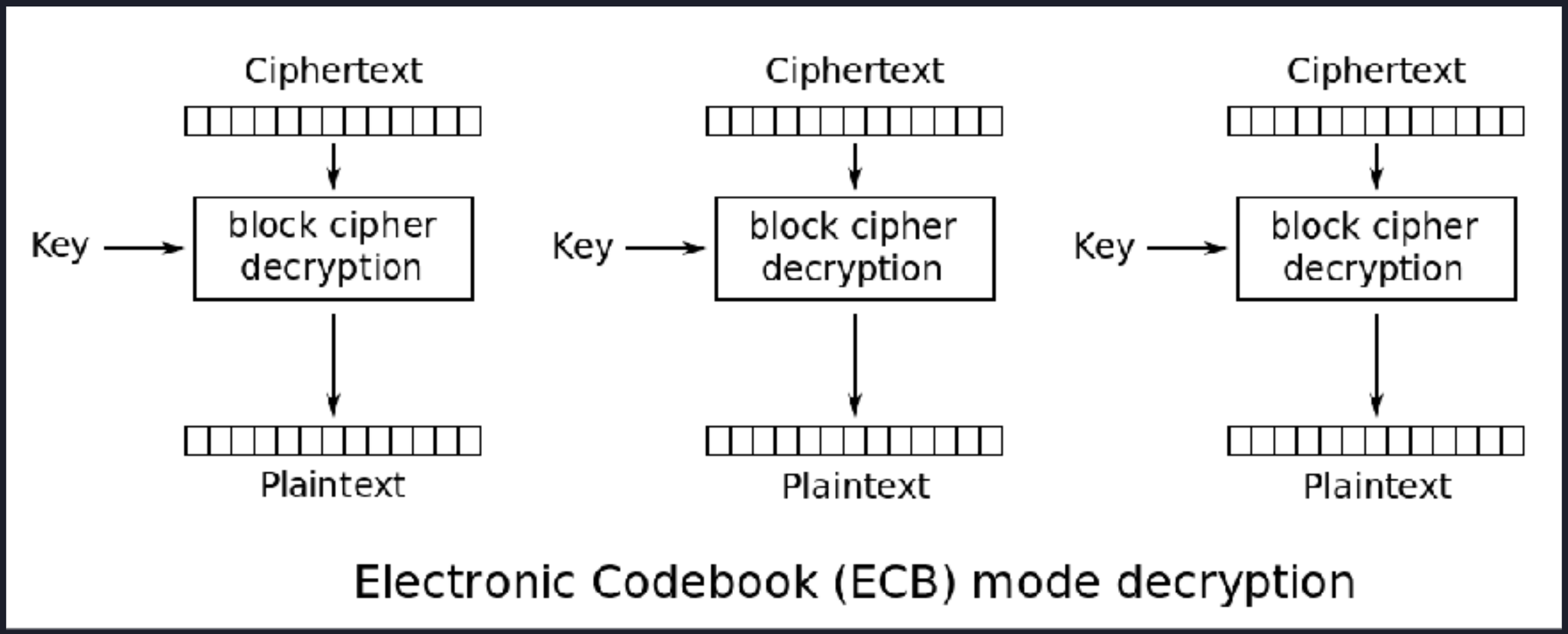
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation



Electronic Codebook (ECB) mode encryption

Block Cipher Mode - ECB

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation



Electronic Codebook (ECB) mode decryption

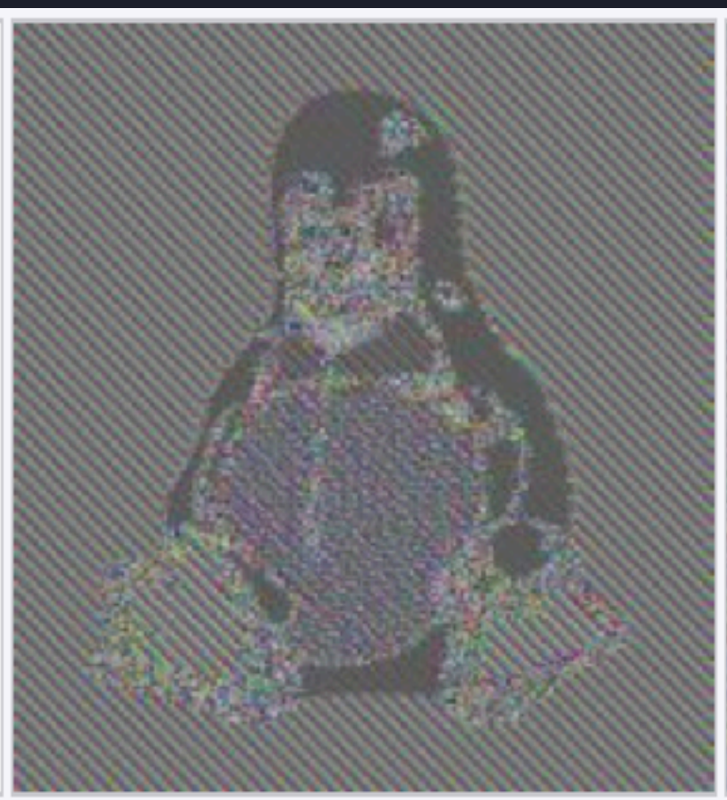
Block Cipher Mode - ECB

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

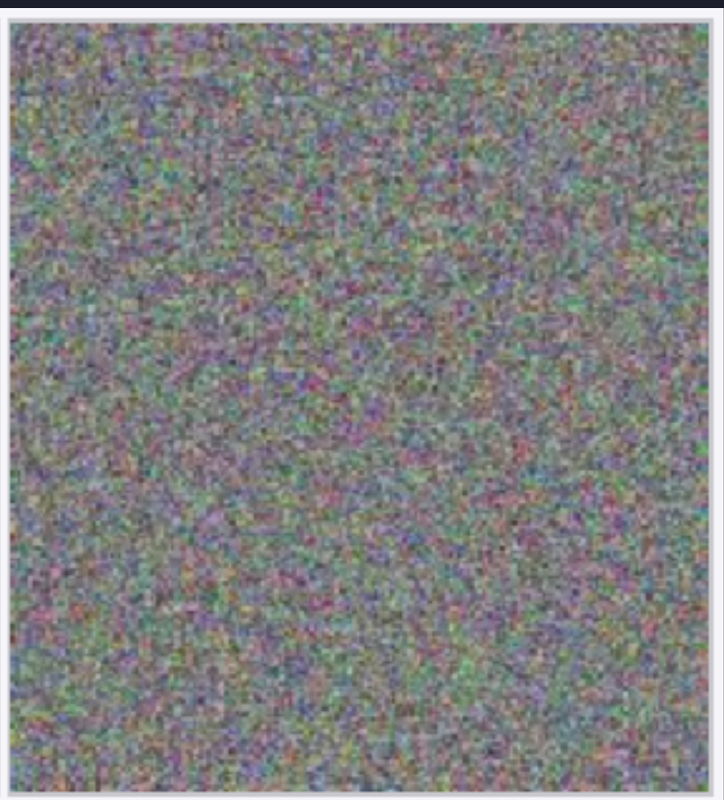
ECB 模式的缺點：

相同的明文區塊會加密出相同的密文區塊

Original image



Encrypted using ECB mode



Modes other than ECB result in pseudo-randomness

Block Cipher Mode - CBC

Block Cipher Mode - CBC

讓我們來複習一下 XOR 的特性

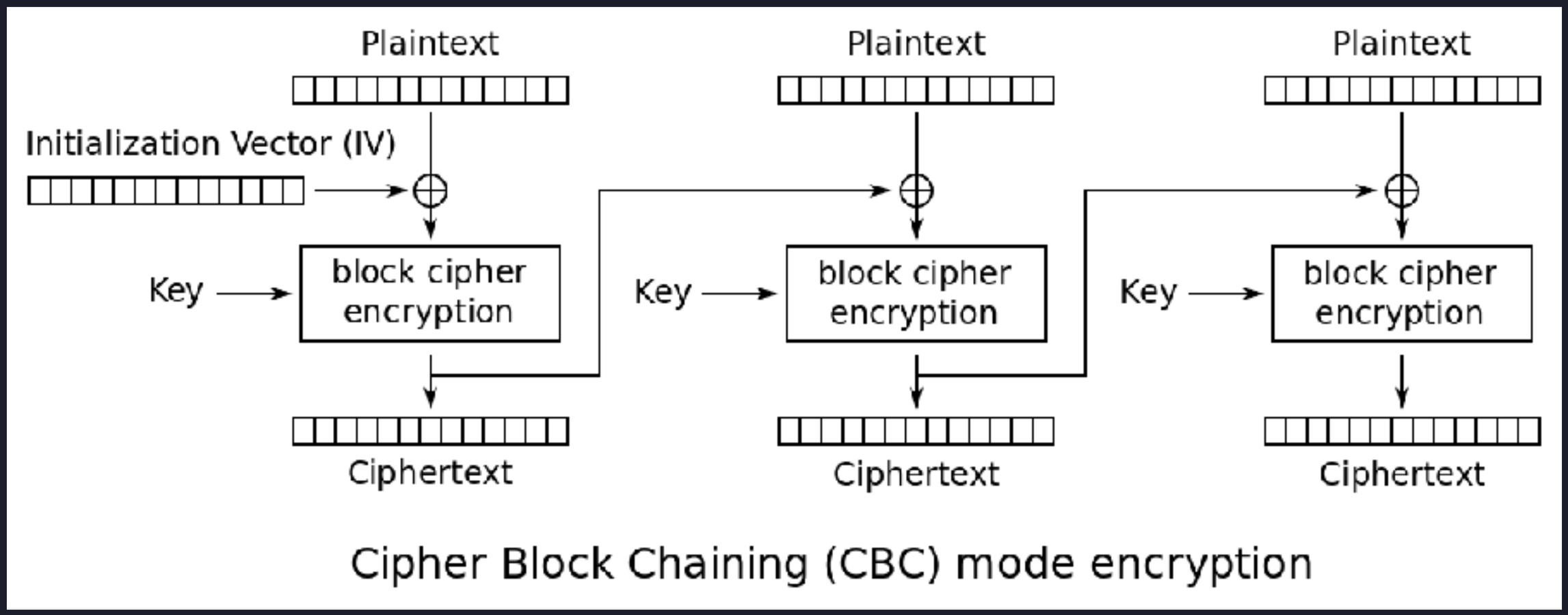
$$A \oplus A = 0$$

$$A \oplus 0 = A$$

$$A \oplus B = C \leftrightarrow A \oplus C = B$$

Block Cipher Mode - CBC

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

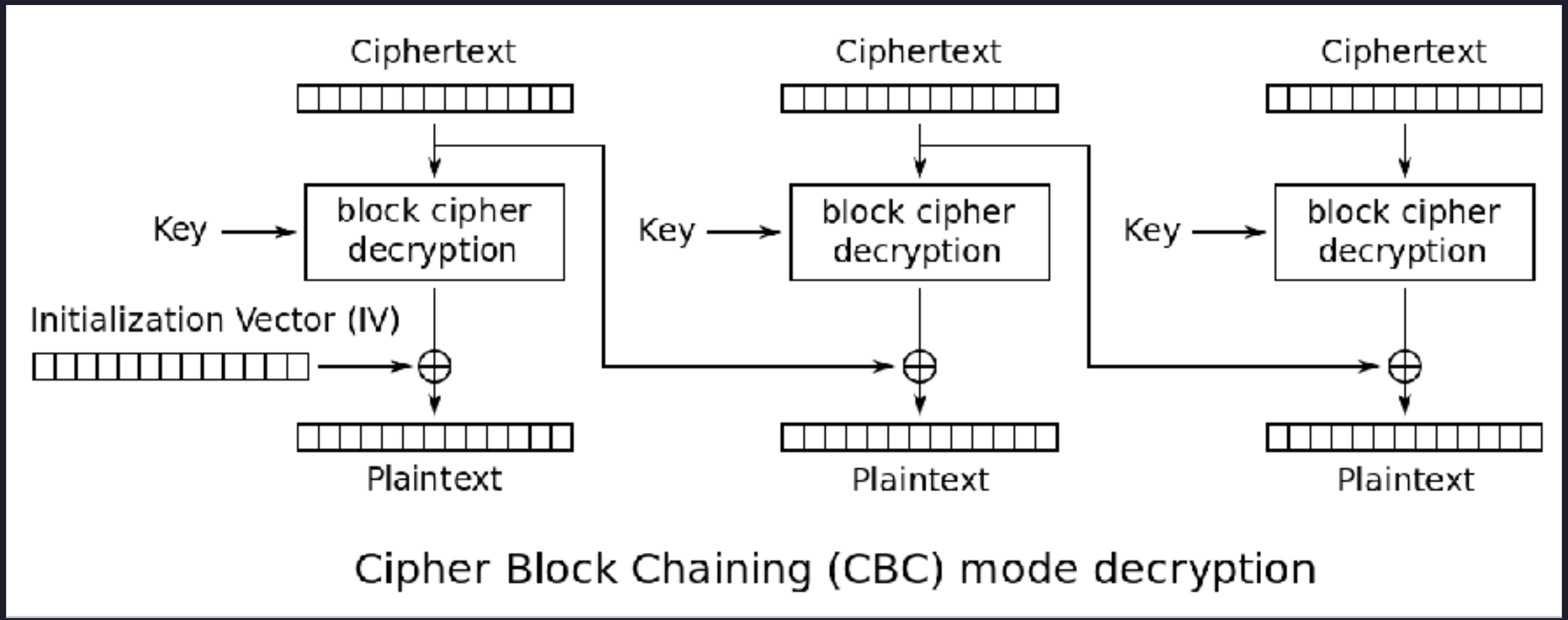


Cipher Block Chaining (CBC) mode encryption

補足 ECB 的缺點：相同的區塊明文加密出不同的區塊密文

Block Cipher Mode - CBC

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation



Cipher Block Chaining (CBC) mode decryption

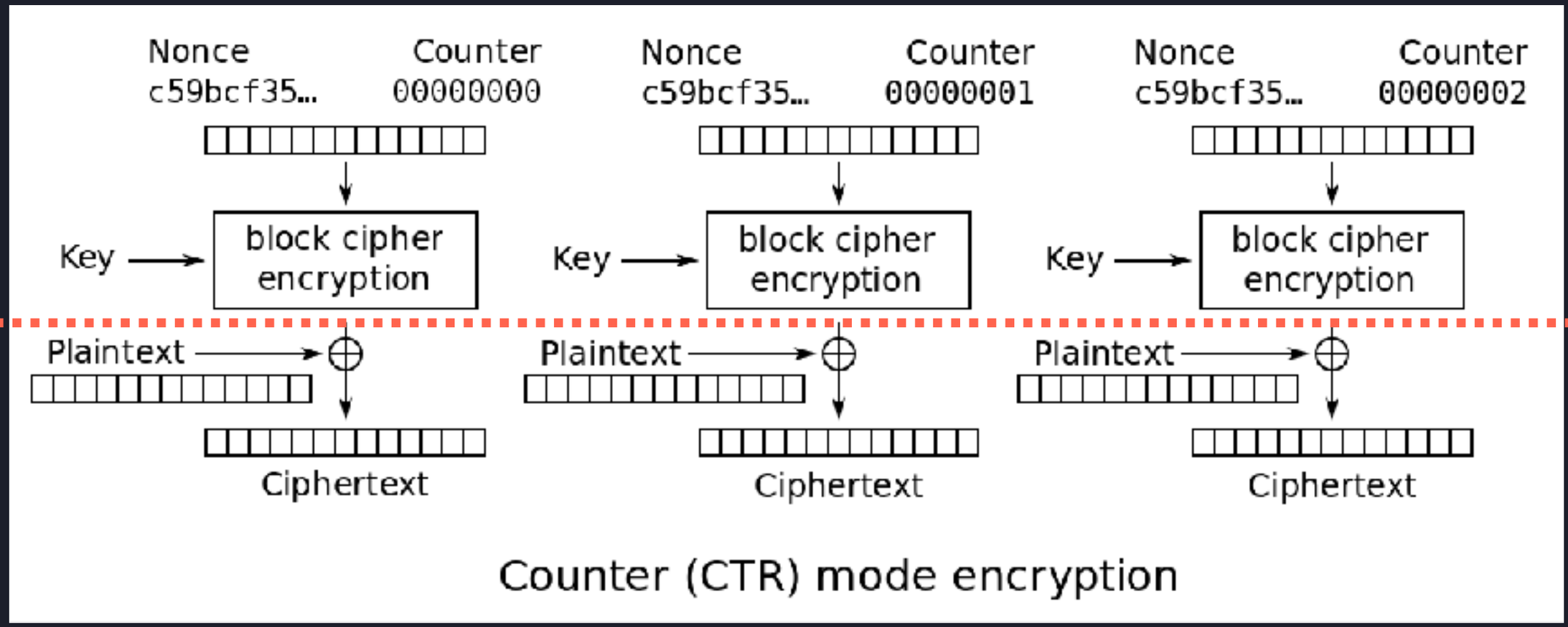
Block Cipher Mode - CTR

Block Cipher Mode - CTR

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

產生 xor key

xor cipher



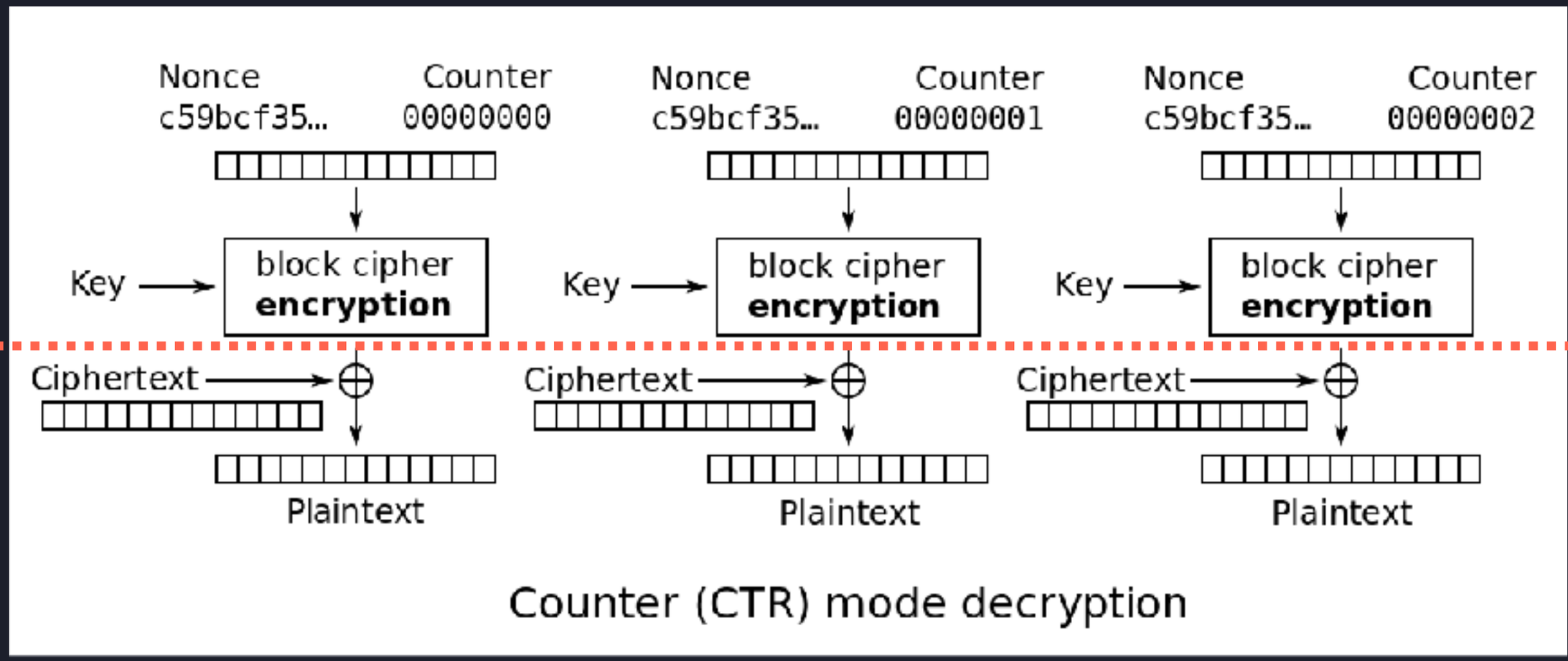
Counter (CTR) mode encryption

Block Cipher Mode - CTR

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

產生 xor key

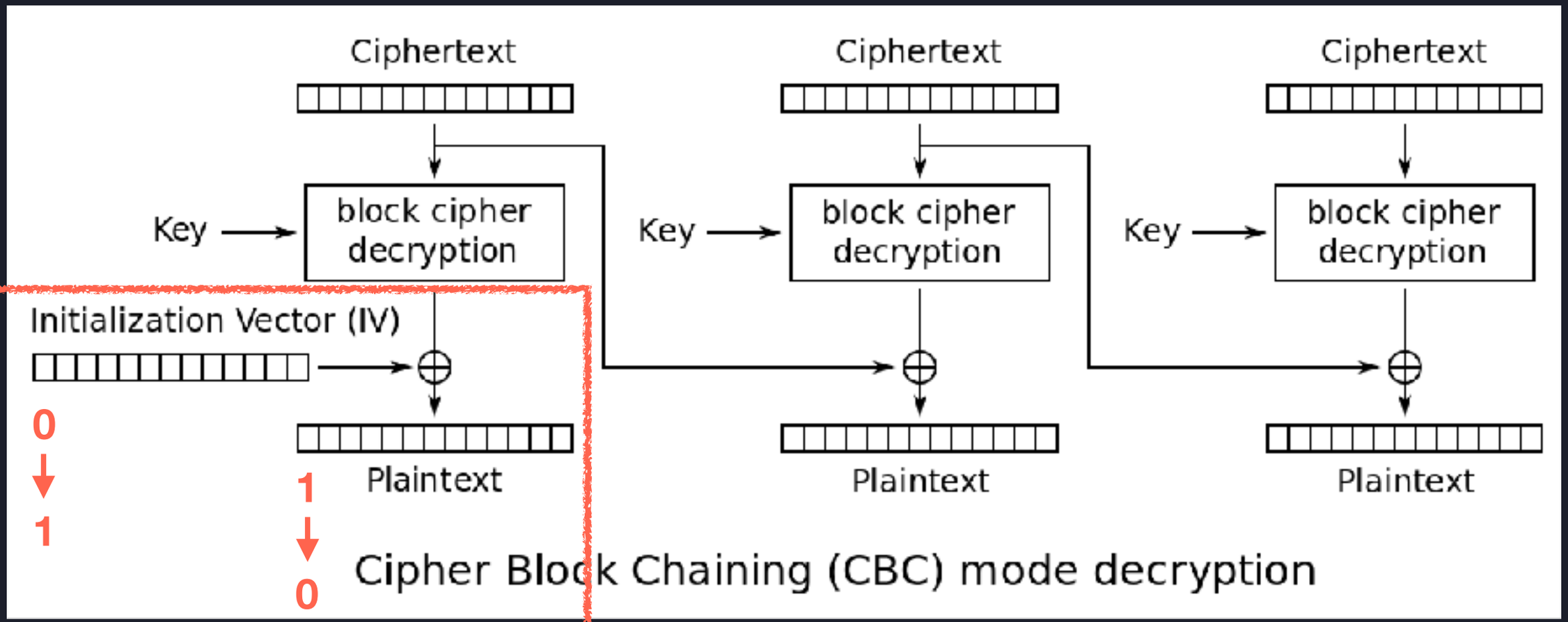
xor cipher



Counter (CTR) mode decryption

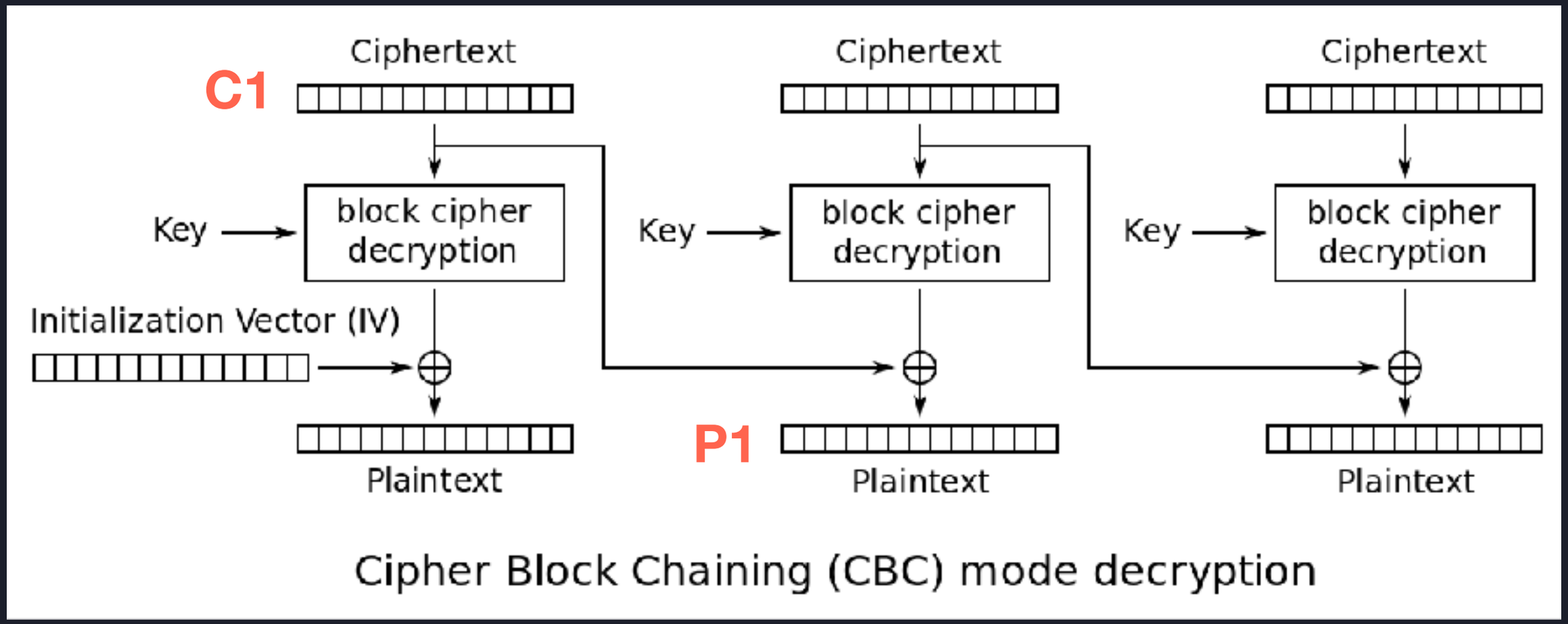
Bit-Flipping Attack

Bit-Flipping Attack - CBC



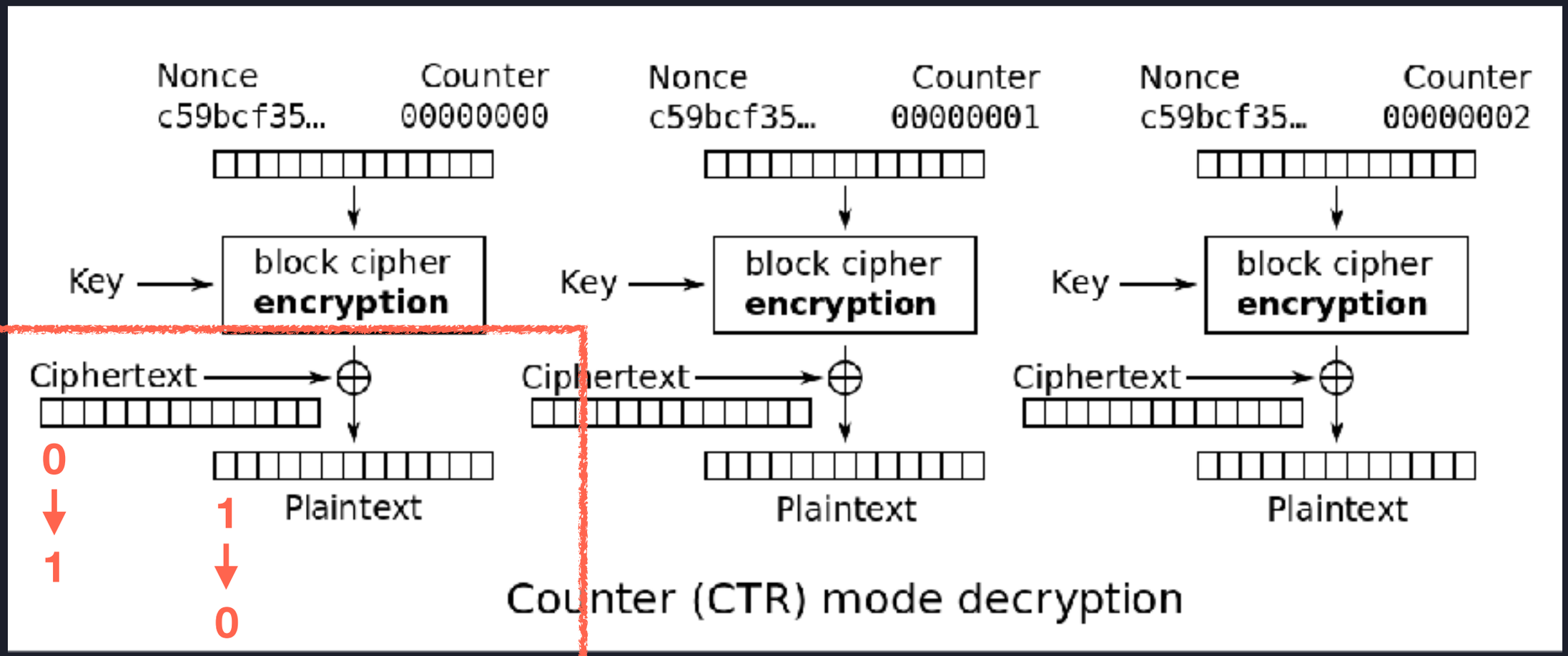
透過對 IV 或 Ciphertext flip-bit 可以讓 Plaintext flip-bit

Bit-Flipping Attack - CBC



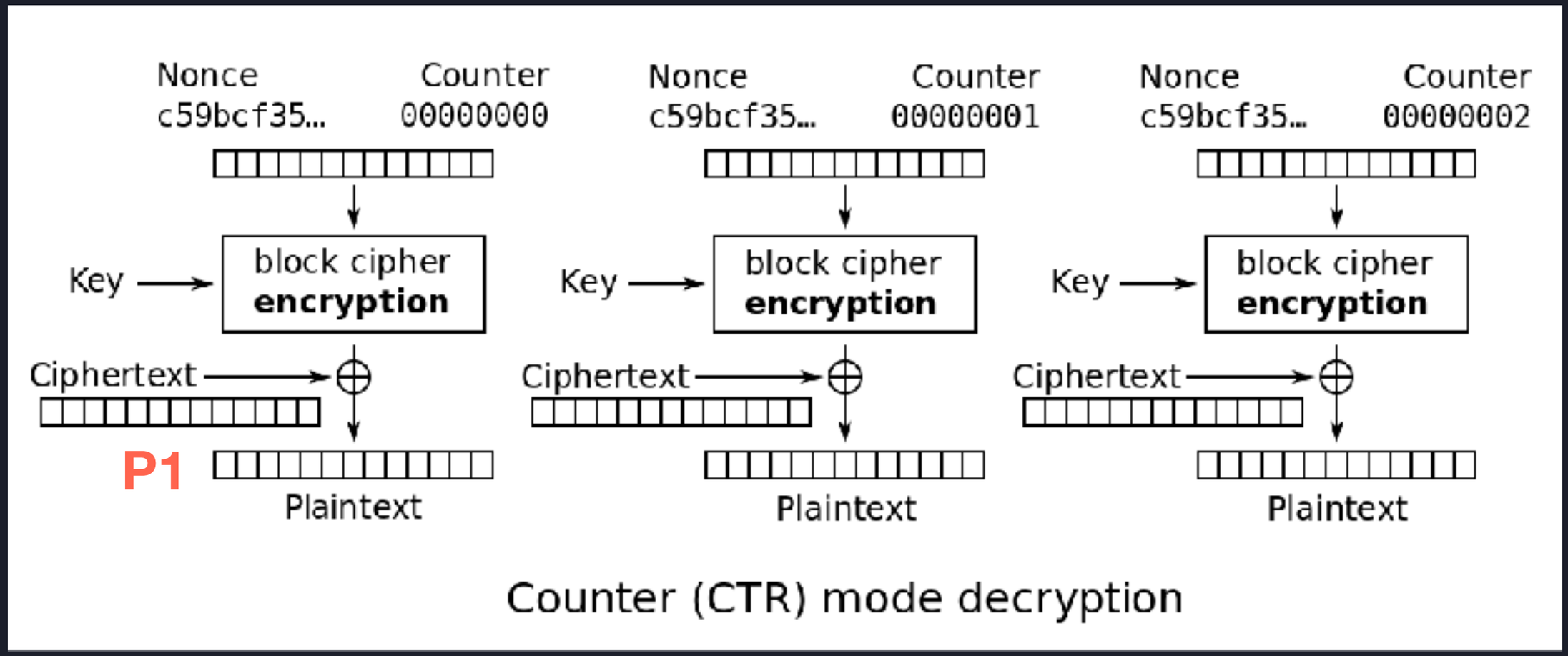
假設我們知道一組 Ciphertext, Plaintext
我們可以更改 Plaintext 為任意字串 P
透過設定 Ciphertext = C1 ⊕ P1 ⊕ P

Bit-Flipping Attack - CTR



透過對 Ciphertext flip-bit 可以讓 Plaintext flip-bit

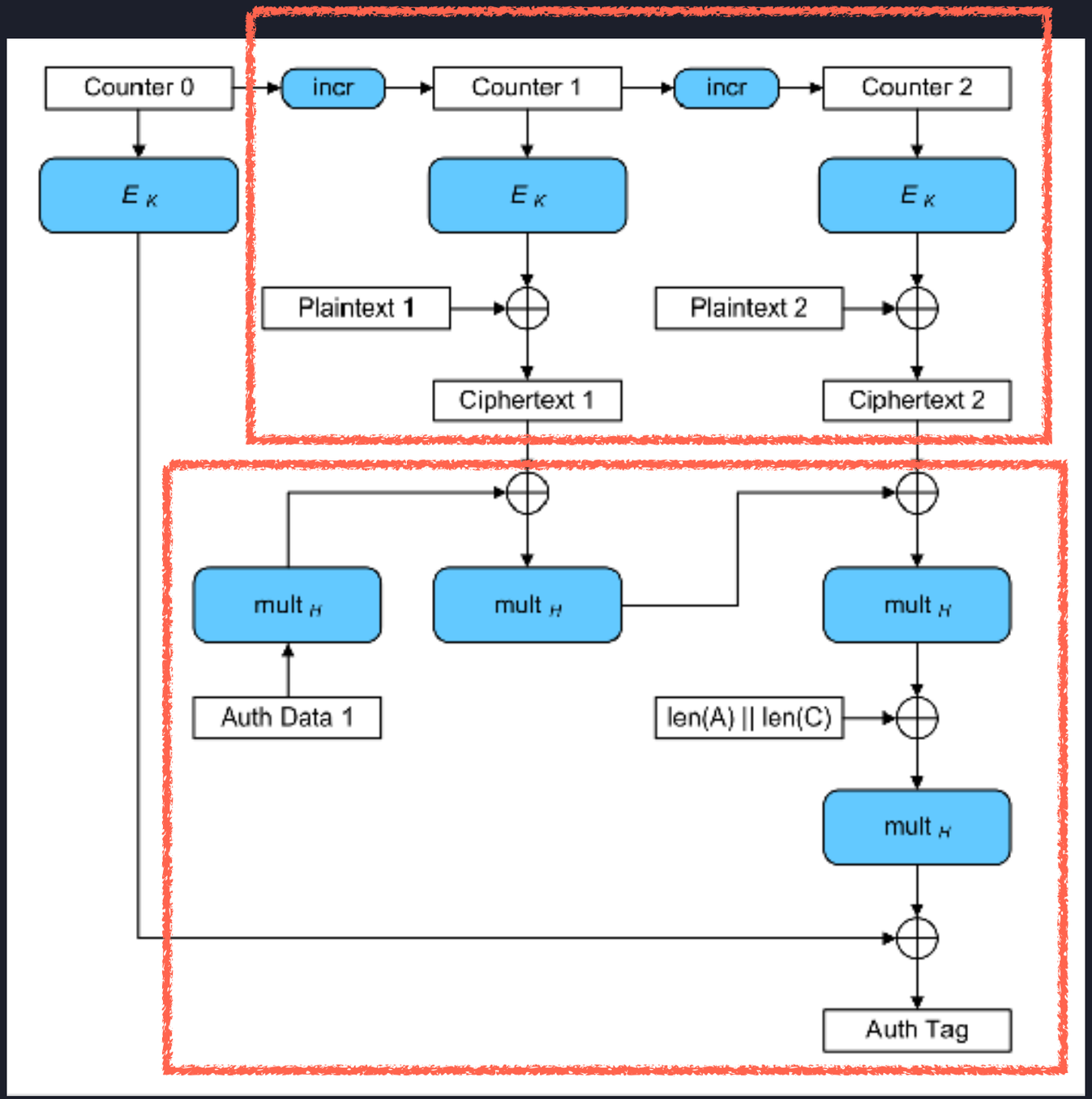
Bit-Flipping Attack - CTR



假設我們知道一組 Ciphertext, Plaintext
我們可以更改 Plaintext 為任意字串 P
透過設定 Ciphertext = C1 ⊕ P1 ⊕ P

Block Cipher Mode - GCM

Block Cipher Mode - GCM



CTR

計算 MAC (TAG)

保證密文的
integrity 和 authentication

Block Cipher Mode - GCM - CTF

Boston Key Party CTF 2016 - gsilvis counting magic

TUM CTF 2016 - ndis

Get Your Hands Dirty

Get Your Hands Dirty - command line

```
$ echo 'AAAA' > data
$ openssl enc -aes-128-cbc -e -in data -out data.enc
$ openssl enc -aes-128-cbc -d -in data.enc -out data
```

```
Cipher Types
-aes-128-cbc               -aes-128-cfb               -aes-128-cfb1
-aes-128-cfb8              -aes-128-ecb               -aes-128-ofb
-aes-192-cbc               -aes-192-cfb               -aes-192-cfb1
-aes-192-cfb8              -aes-192-ecb               -aes-192-ofb
-aes-256-cbc               -aes-256-cfb               -aes-256-cfb1
-aes-256-cfb8              -aes-256-ecb               -aes-256-ofb
-aes128                    -aes192                    -aes256
-bf                        -bf-cbc                    -bf-cfb
-bf-ecb                    -bf-ofb                    -blowfish
-cast                      -cast-cbc                  -cast5-cbc
-cast5-cfb                 -cast5-ecb                 -cast5-ofb
-des                       -des-cbc                   -des-cfb
-des-cfb1                  -des-cfb8                  -des-ecb
-des-ede                   -des-ede-cbc               -des-ede-cfb
-des-ede-ofb               -des-ede3                  -des-ede3-cbc
-des-ede3-cfb              -des-ede3-cfb1             -des-ede3-cfb8
-des-ede3-ofb              -des-ofb                   -des3
-desx                      -desx-cbc                  -rc2
-rc2-40-cbc                -rc2-64-cbc                -rc2-cbc
-rc2-cfb                   -rc2-ecb                   -rc2-ofb
-rc4                       -rc4-40                    -seed
-seed-cbc                  -seed-cfb                  -seed-ecb
-seed-ofb
```

Get Your Hands Dirty - python

https://www.dlitz.net/software/pycrypto/api/current/Crypto.Cipher.AES-module.html

使用 pycrypto 套件

```
from Crypto.Cipher import AES
key, iv = 'A' * 16, 'B' * 16
aes_enc = AES.new(key, AES.MODE_ECB, iv)
aes_enc.encrypt('C' * 16) # b'\xbf\x1ej>.\xc2\xdb_\x9a1&\x17\xee\xfc\x95S'
aes_dec = AES.new(key, AES.MODE_ECB, iv)
aes_dec.decrypt(b'\xbf\x1ej>.\xc2\xdb_\x9a1&\x17\xee\xfc\x95S') # b'CCCCCCCCCCCCCCCC'
```

Meet in the Middle Attack

Meet in the Middle Attack

DES 的密鑰長度是 56 bits (7 bytes)

暴力破解：

我們知道一組明文密文 (P, C)

暴力嘗試所有的密鑰可能

理論上最多需要 2^{56} 次運算

Double DES :

為了增加暴力破解的複雜度

改成使用兩層 DES

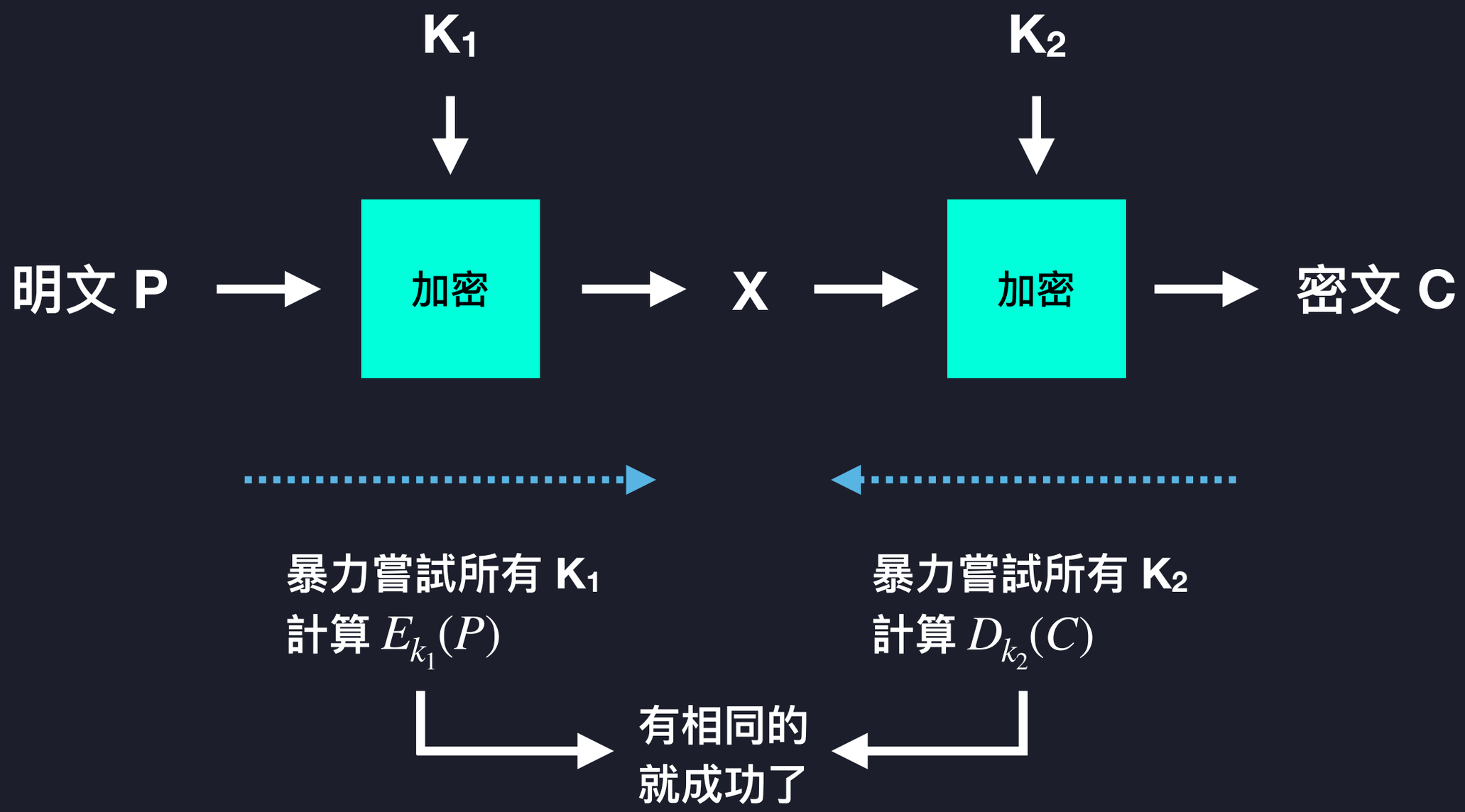
加密：$E_{k_1}(E_{k_2}(P)) = C$

解密：$D_{k_2}(D_{k_1}(C)) = P$

暴力嘗試最多所需運算次數提升到 2^{112} 次

Meet in the Middle Attack

https://www.coursera.org/learn/symmetric-crypto/lecture/spsdV/double-des-and-meet-in-the-middle-attack



將需要運算的次數降到 2^{56}
但是需要 2^{56} 的空間

Meet in the Middle Attack

Double DES 失敗了怎麼辦？

Triple DES

Padding Oracle Attack

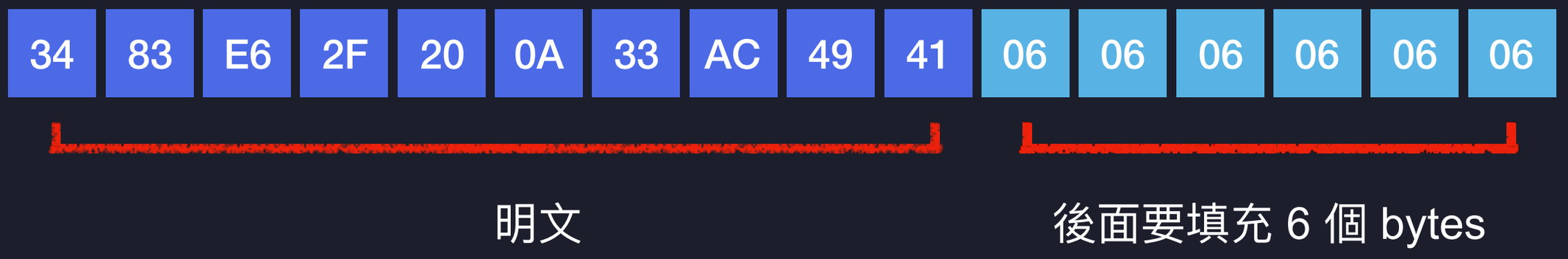
Padding Oracle Attack

https://en.wikipedia.org/wiki/Padding_%28cryptography%29#PKCS7

什麼是 PKCS#7 填充字元標準？

要填充 5 個 bytes 就填充 5 個 0x05

要填充 2 個 bytes 就填充 2 個 0x02



Padding Oracle Attack

攻擊對象：

使用 PKCS#7 填充字元標準的 CBC Block Cipher

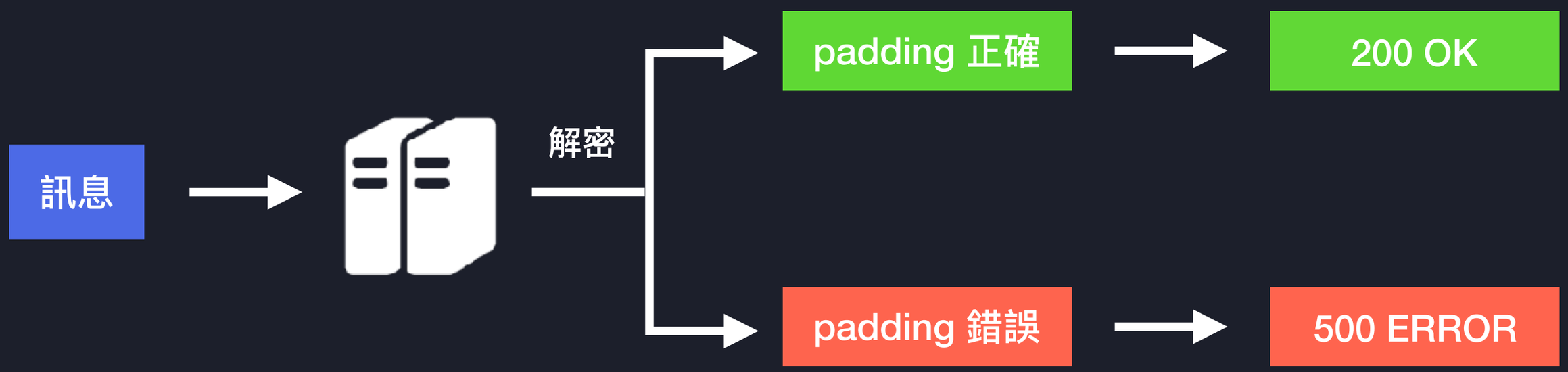
目標：

解開被伺服器加密的訊息

情境：

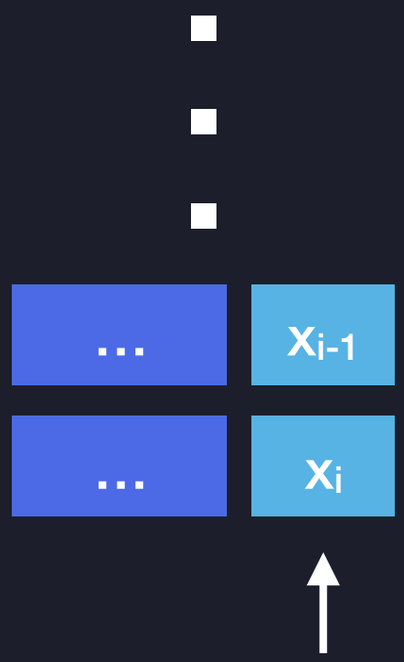
伺服器能幫我們解密任意訊息

但我們只能知道有沒有 padding 錯誤



Padding Oracle Attack

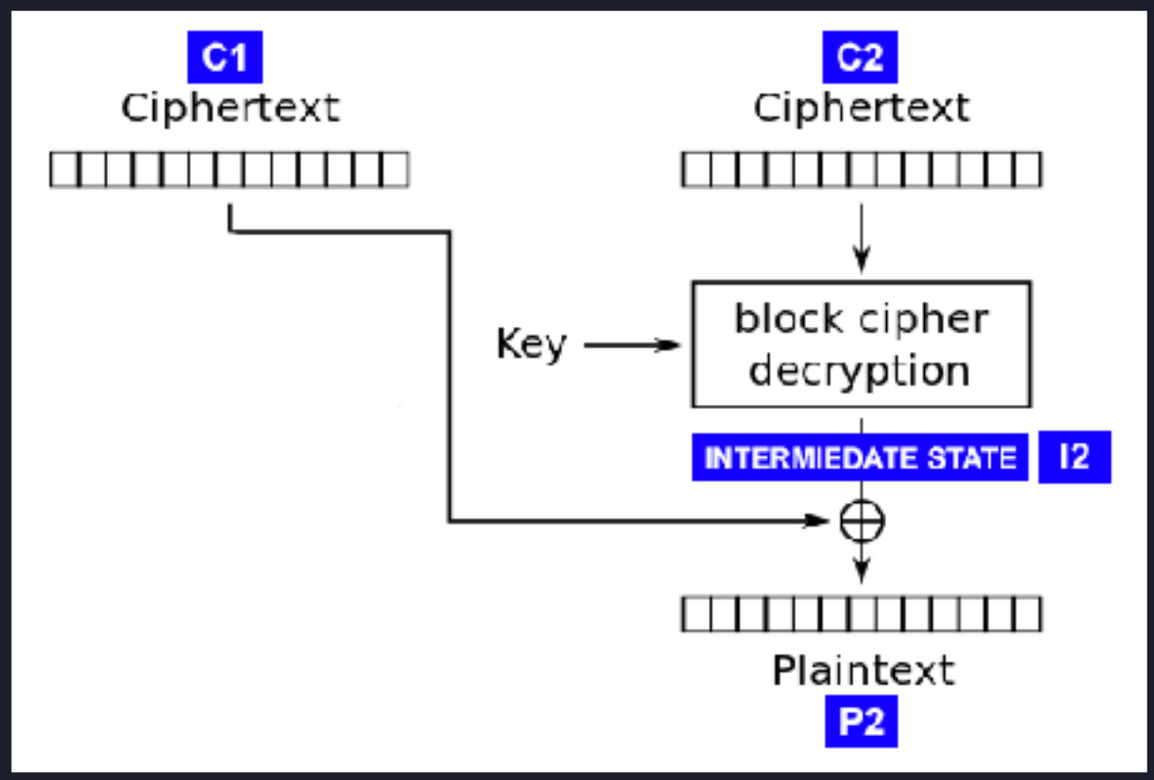
https://robertheaton.com/2013/07/29/padding-oracle-attack/



嘗試 x = 0x00 - 0xFF

構造 C1

目標 C2



padding 錯誤

padding 正確

代表 Plaintext 有很大的機會是 0x01 結尾的

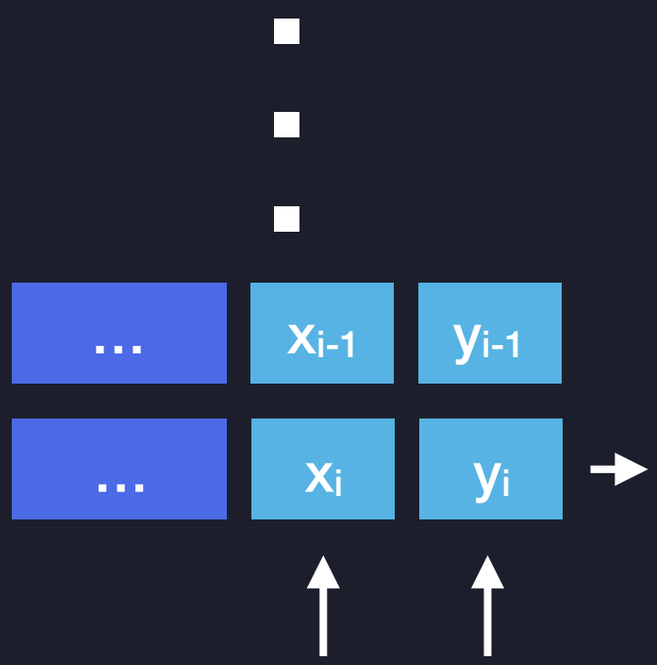
0x02 結尾的話代表倒數第二個 byte 也要是 0x02

I2[-1] 就會是 $x_i \oplus 0x01$

P2[-1] 就會是 I2[-1] ⊕ C1[-1]

Padding Oracle Attack

https://robertheaton.com/2013/07/29/padding-oracle-attack/

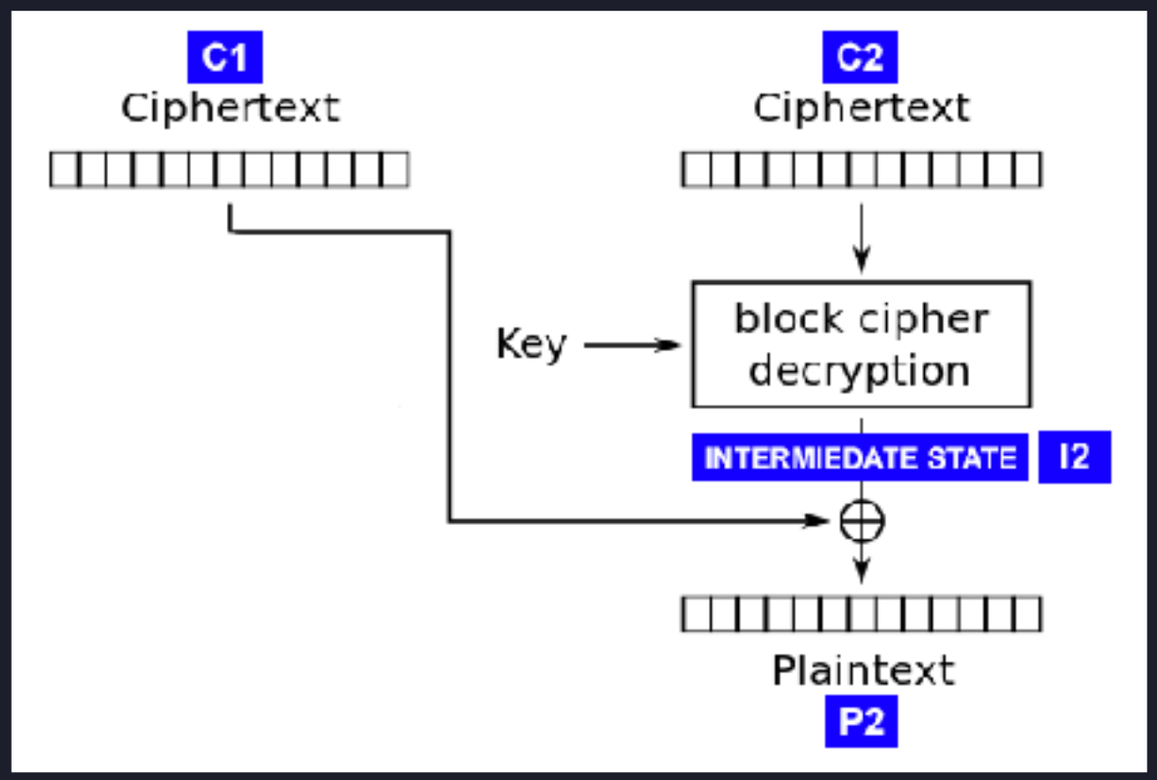


嘗試 x = 0x00 - 0xFF

設定 y = I2[-1] ⊕ 0x02

構造 C1

目標 C2



padding 錯誤

padding 正確

代表 Plaintext 倒數第二個 byte一定是 0x02

我們透過 y 設定 Plaintext 結尾為 0x02

I2[-2] 就會是 x_i ⊕ 0x02

P2[-2] 就會是 I2[-2] ⊕ C1[-2]

Padding Oracle Attack

兩層迴圈：
一次解出一個 byte 直到解完一個 block
一次解出一個 block 直到解完所有 blocks

嘗試次數：
解出一個 byte 最多需要 256 次嘗試
解出一個 block (16 bytes) 最多需要 4096 次嘗試

第一個區塊：
我們需要前一個區塊來解目前的區塊
所以我們需要知道原始 IV 和能夠操控 IV 才能解出第一個區塊

Padding Oracle Attack - CTF

原汁原味 padding oracle attack :

CSAW CTF 2016 Quals - Neo
HITCON CTF 2016 Quals - Hackpad
BAMBOOFOX CTF 2018 - mini-padding

padding 相關攻擊技巧 :

HITCON CTF 2017 Quals - Secret Server
HITCON CTF 2017 Quals - Secret Server Revenge
BAMBOOFOX CTF 2018 - baby-lea-revenge
BAMBOOFOX CTF 2018 - baby-lea-impossible