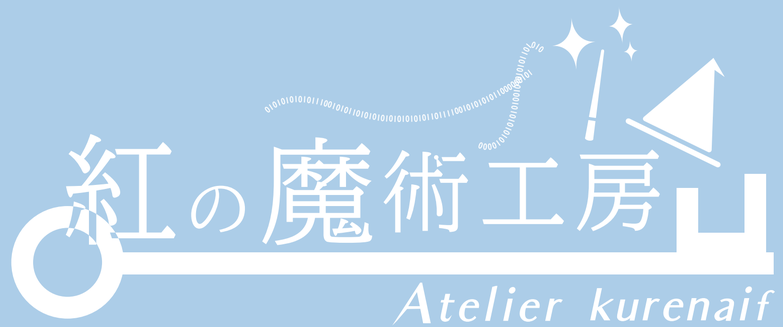
CBC Padding Oracle Attack

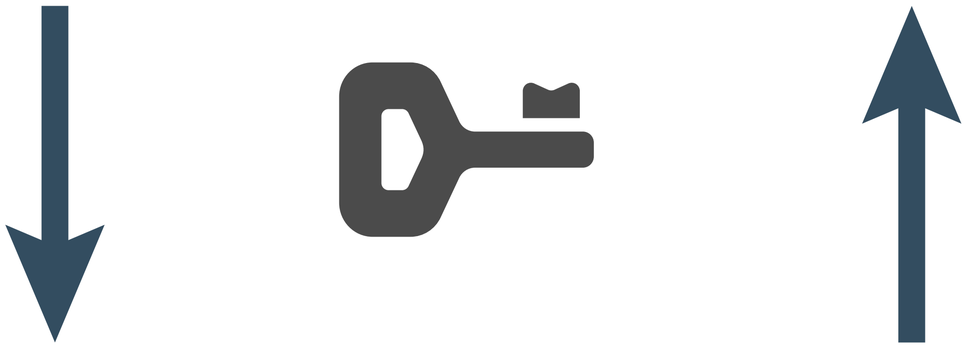


Today’s Topic

Block Cipher (CBC)

紅の魔術工房
Atelier kurenaif

long plain text(256bytes)



long cipher text(256 bytes)

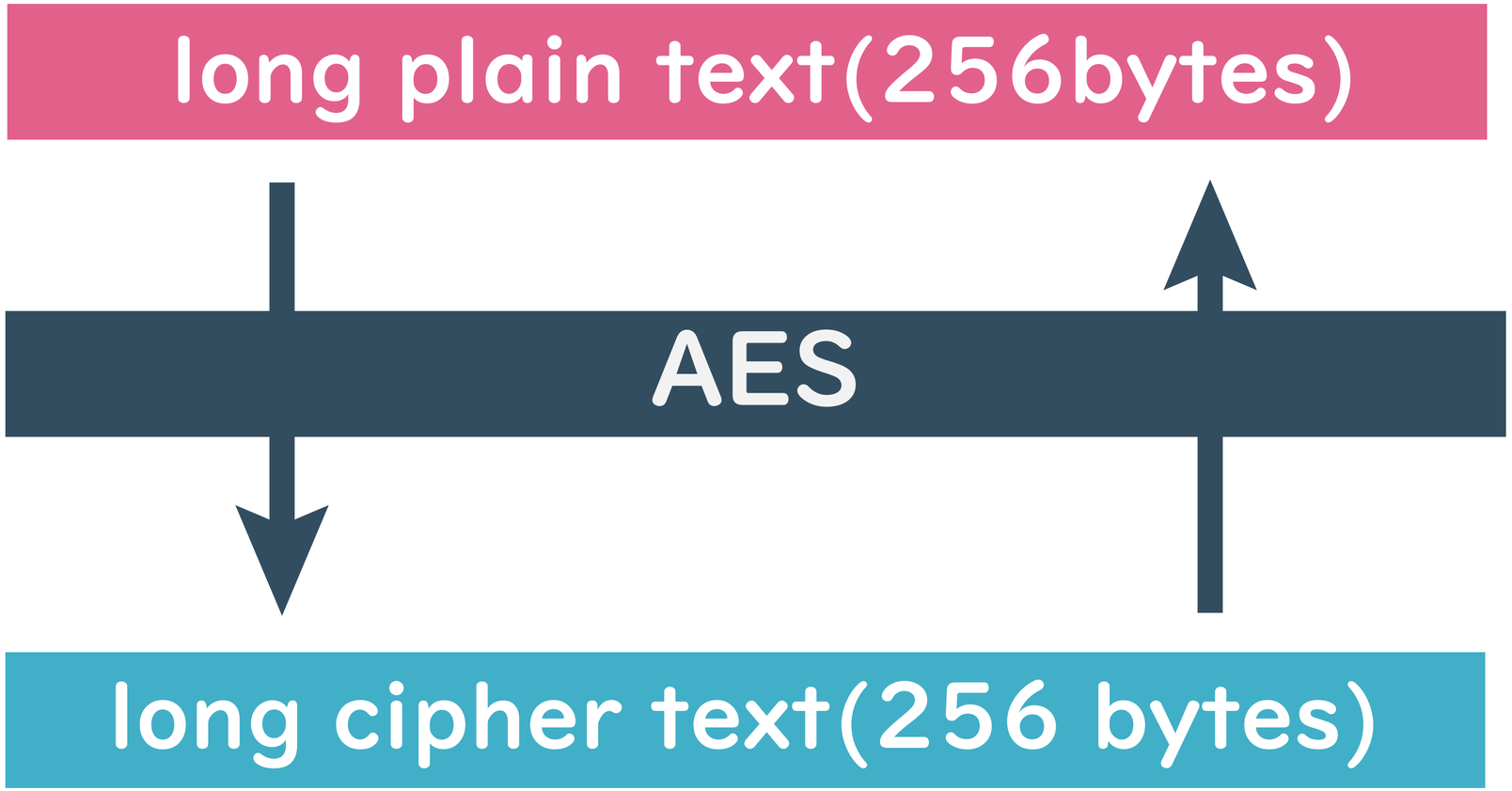
What's Block Cipher?

long plain text(256bytes)

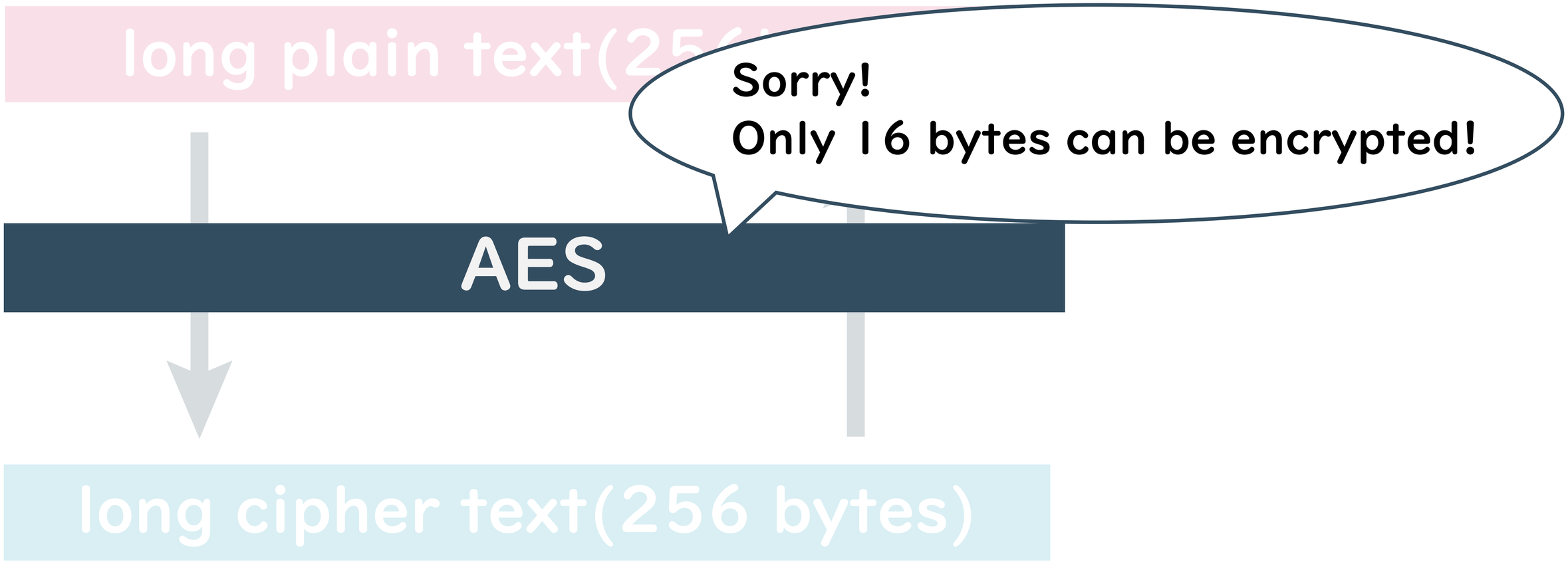
* fast
* same key
* safety

long cipher text(256 bytes)

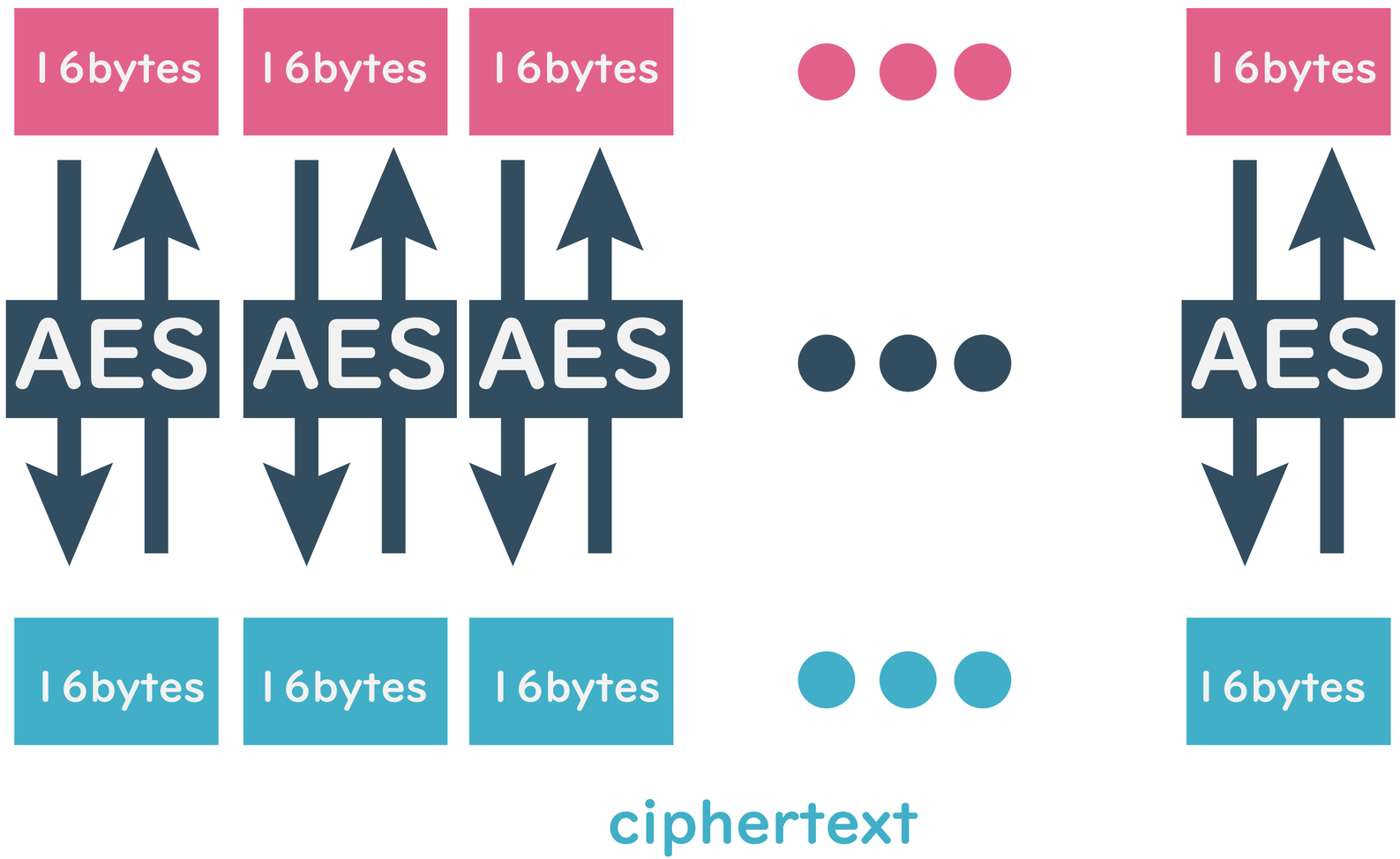
What's Block Cipher?



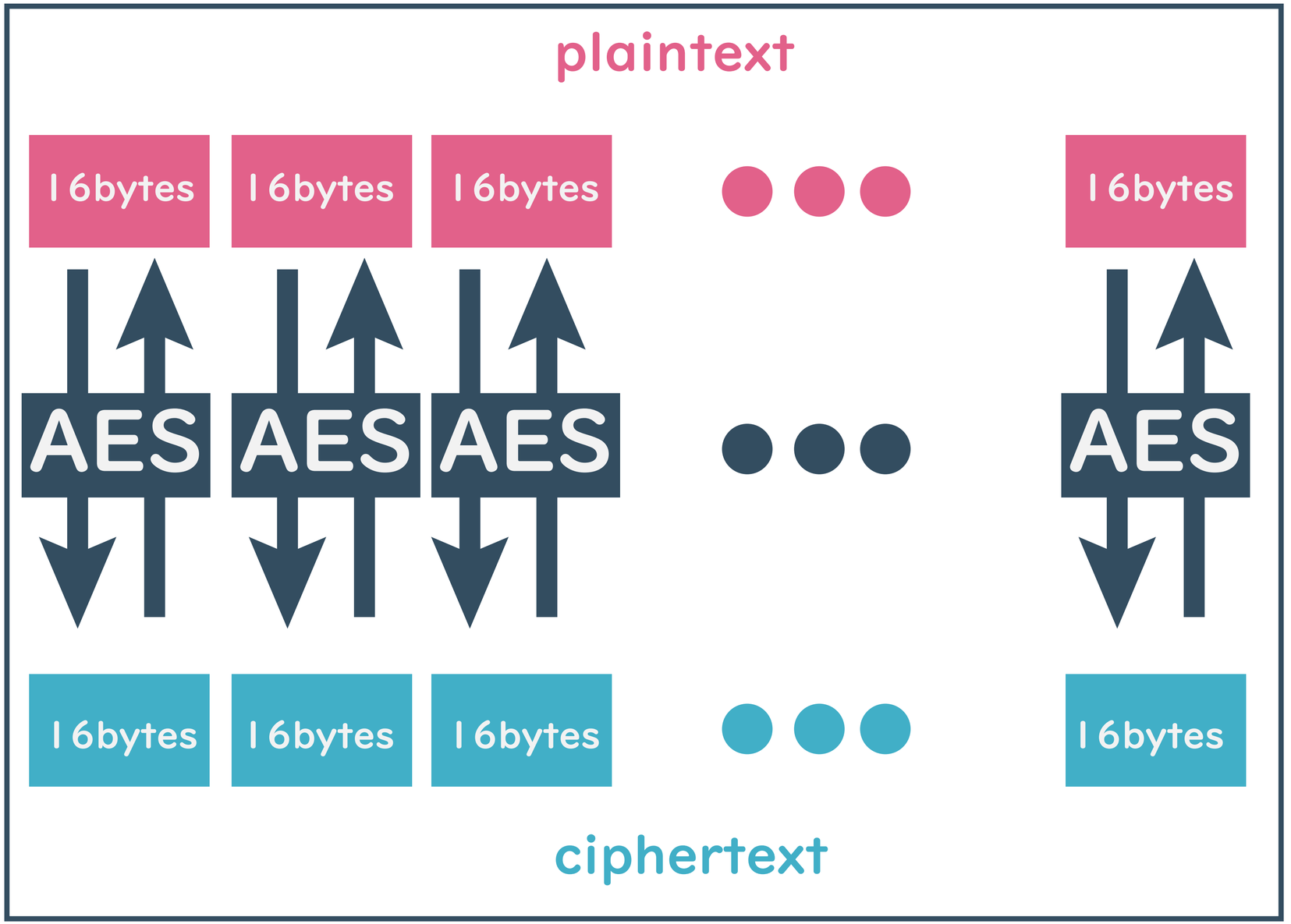
What's Block Cipher?



What's Block Cipher?



What's Block Cipher?



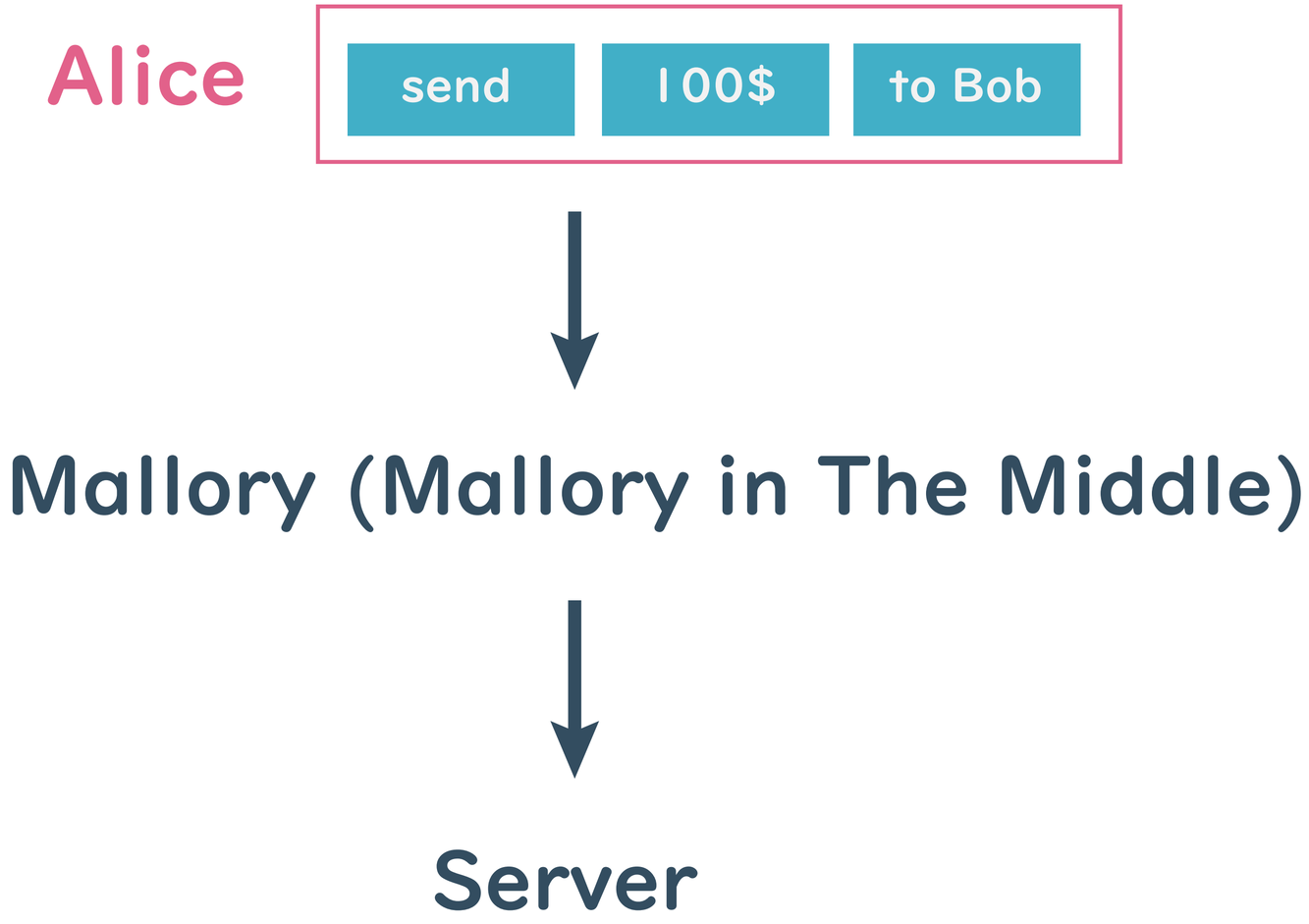
This Algorithm Called

AES-ECB

What's Block Cipher?

AES is Very Strong.

But, ECB is Very Weak



Why is the ECB so weak?

Alice

rewrite to “send 10000$ to Marroly”

Mallory (Mallory in The Middle)

Server

Why is the ECB so weak?

紅の魔術工房
Atelier kurenaif

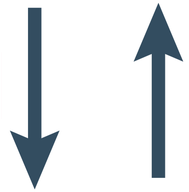
Alice

send | 100$ | to Bob

Mallory (Mallory in The Middle)

plain text

send | 10000$ | to Mallory



cipher text

send | 10000$ | to Mallory

Server

Why is the ECB so weak?

Alice

send | 100$ | to Bob

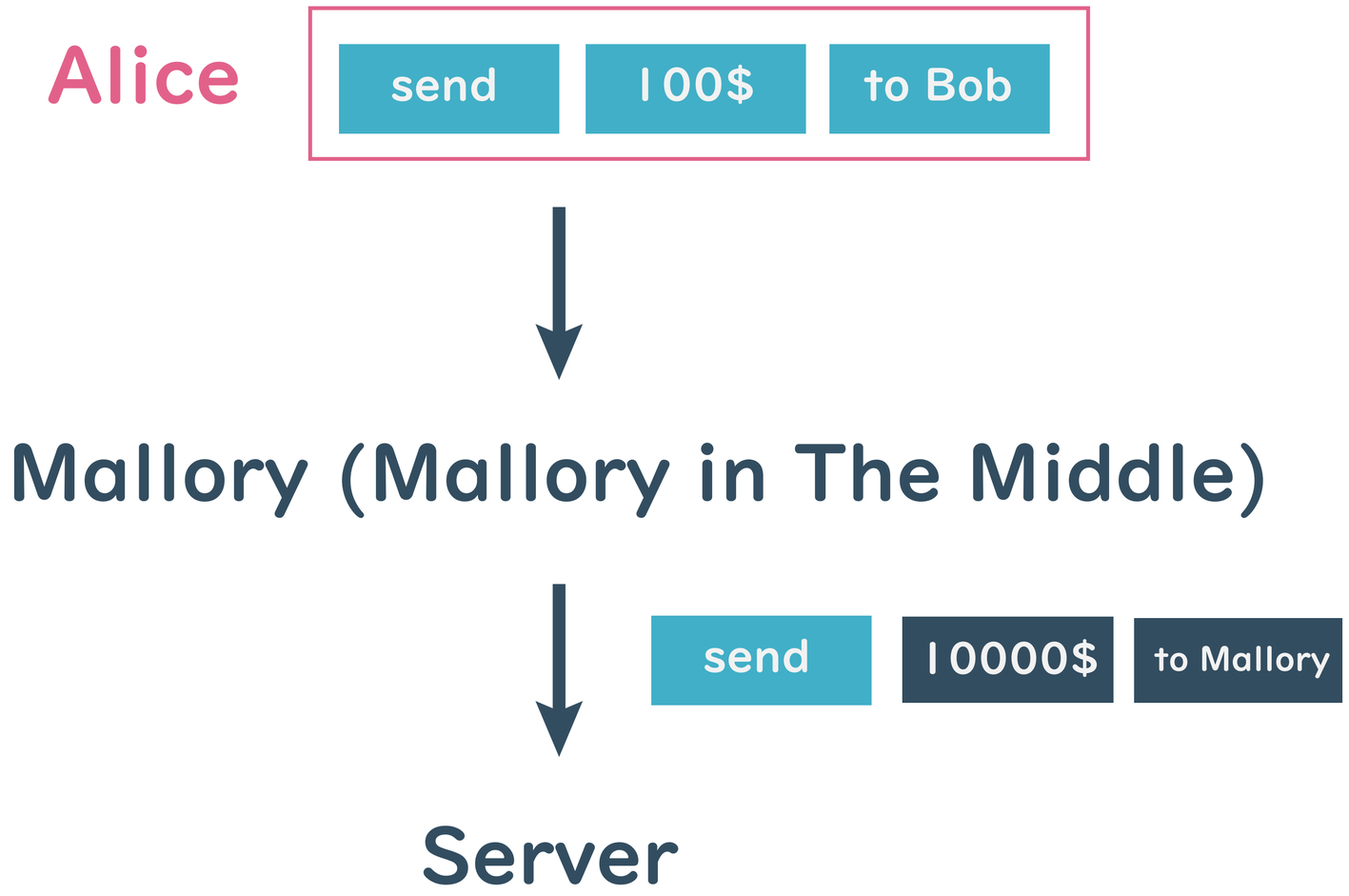
cipher text

send | 10000$ | to Mallory

Mallory (Mallory in The Middle)

Server

Why is the ECB so weak?



Why is the ECB so weak?

Alice

send | 100$ | to Bob

Mallory (Mallory in The Middle)

send | 10000$ | to Mallory

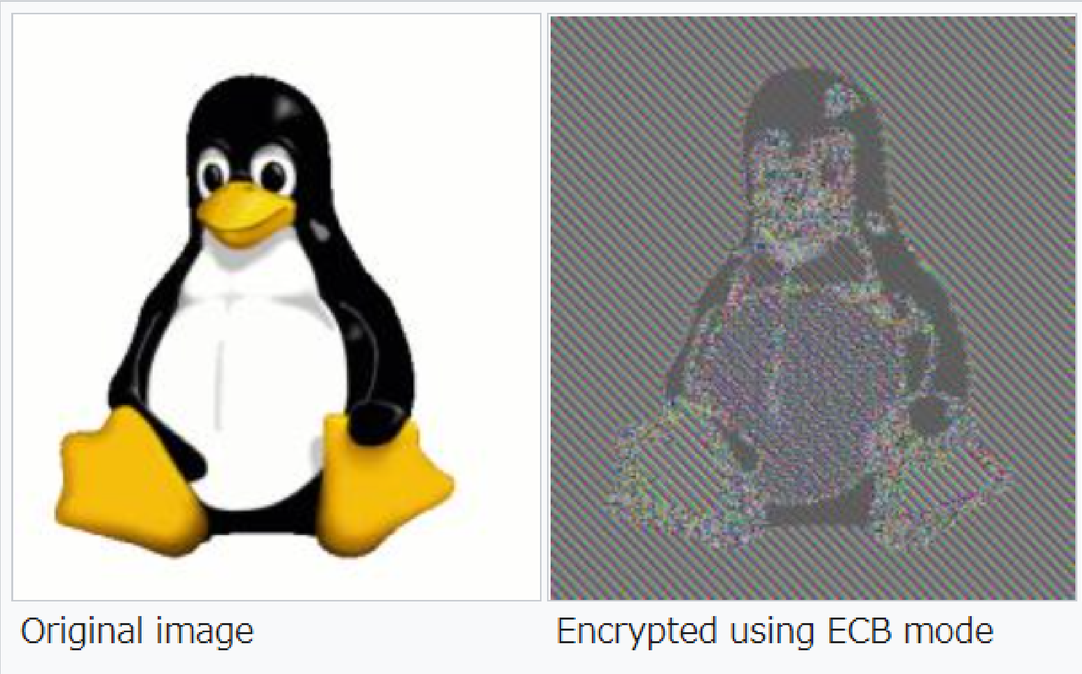
Server

easy to falsification

Why is the ECB so weak?

same plain text block leads to same cipher text block.

So, confidentiality is low.

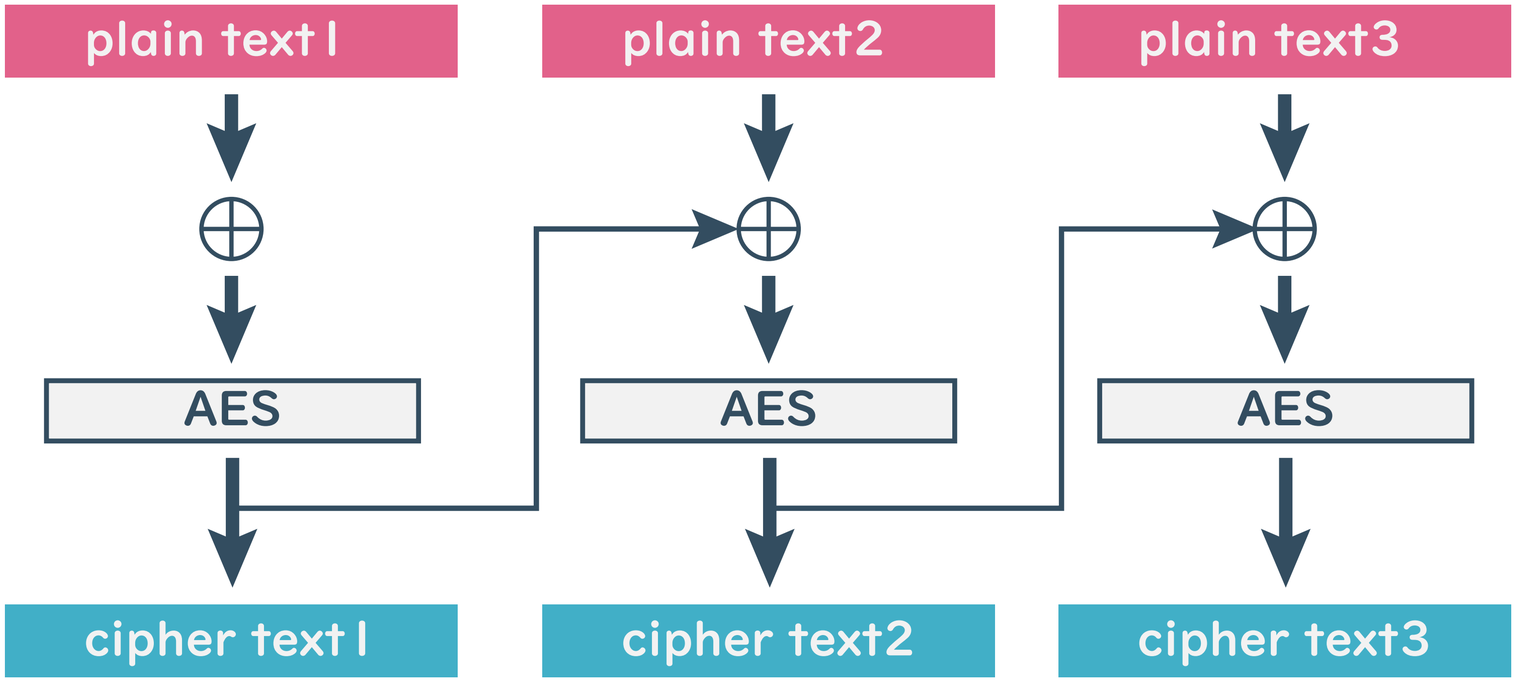


Original image

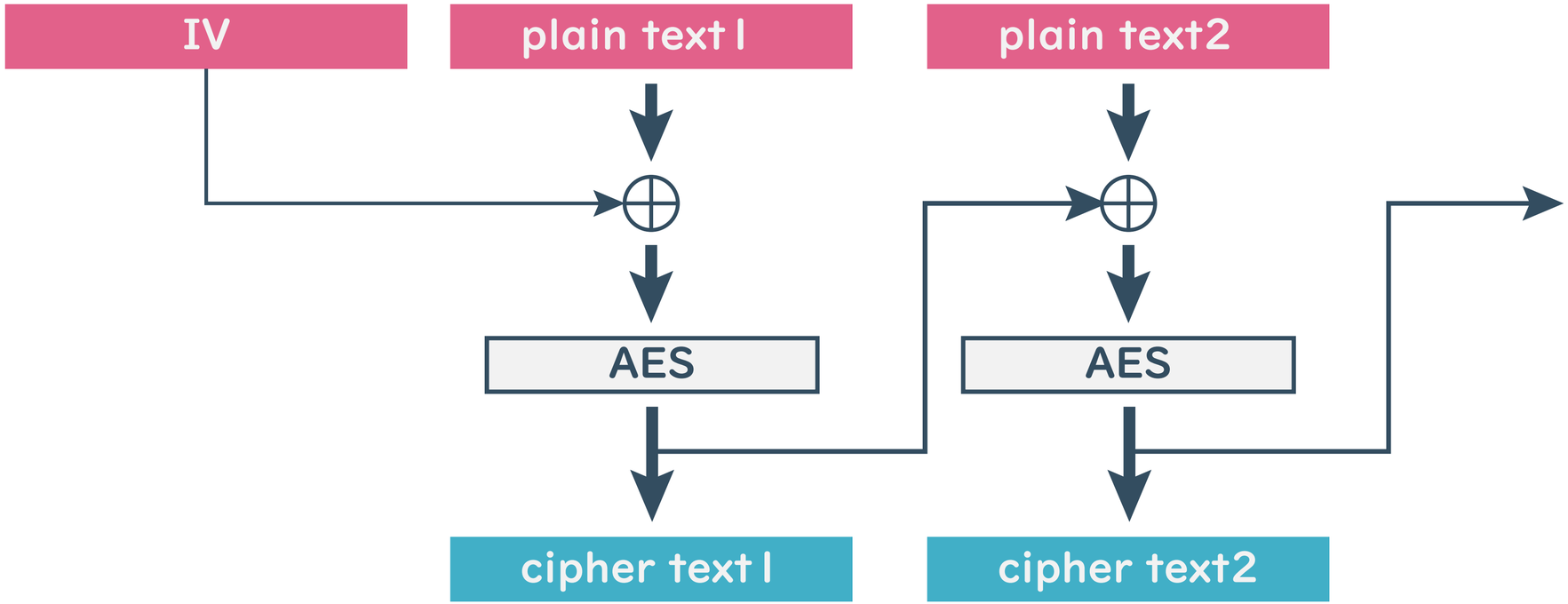
Encrypted using ECB mode

reference: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#ECB

Why is the ECB so weak?

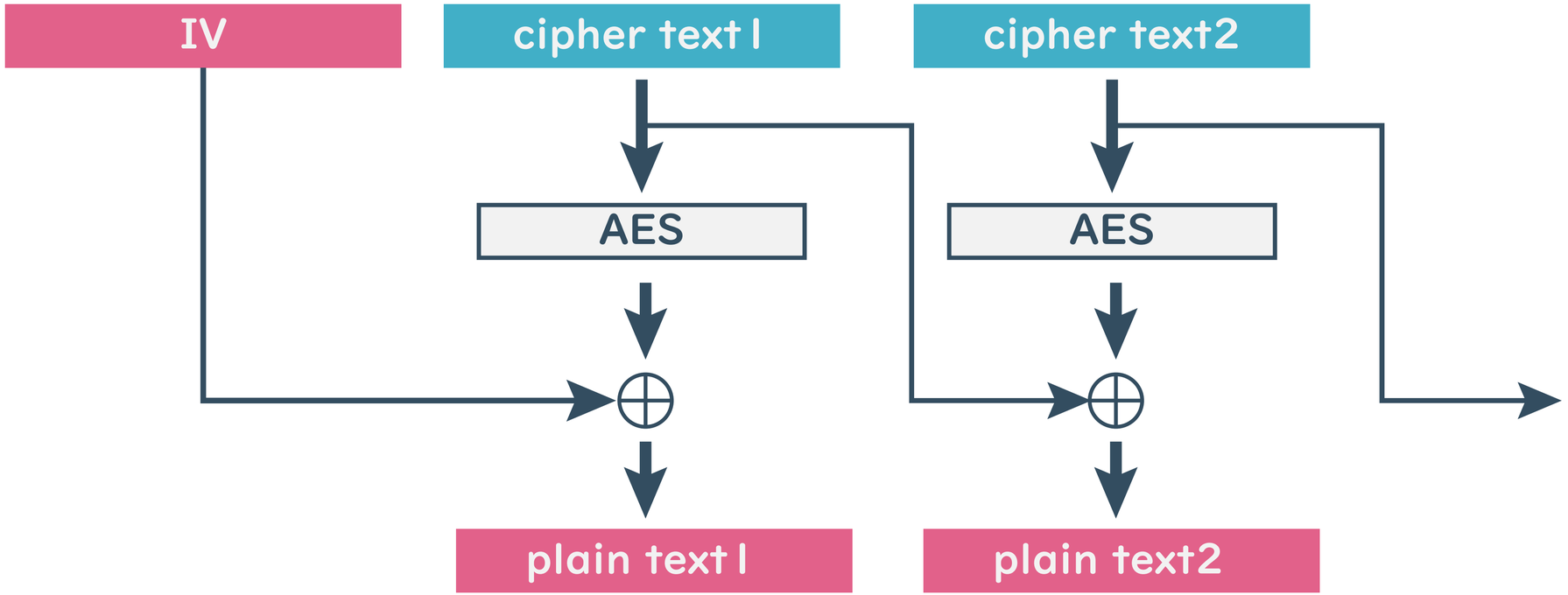

plain text1
plain text2
plain text3
AES
AES
AES
cipher text1
cipher text2
cipher text3

What's CBC?



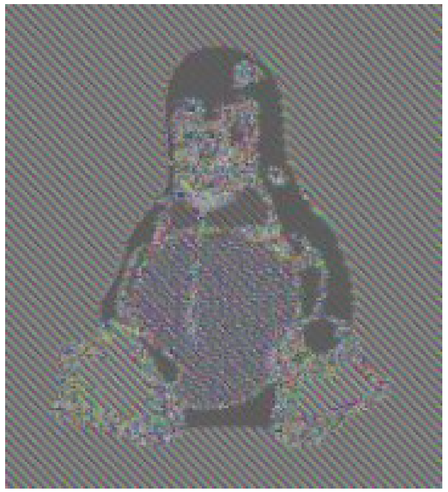
reference: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#ECB

What's CBC?

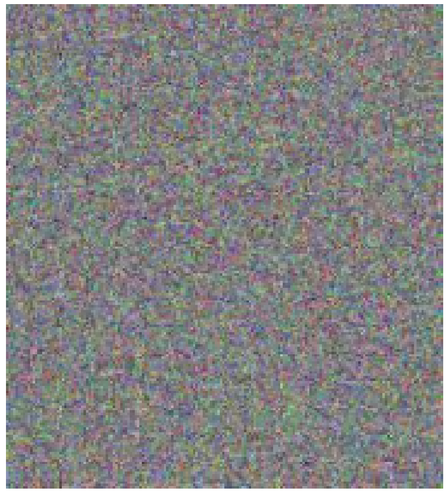


What's CBC?

Original bitmap image



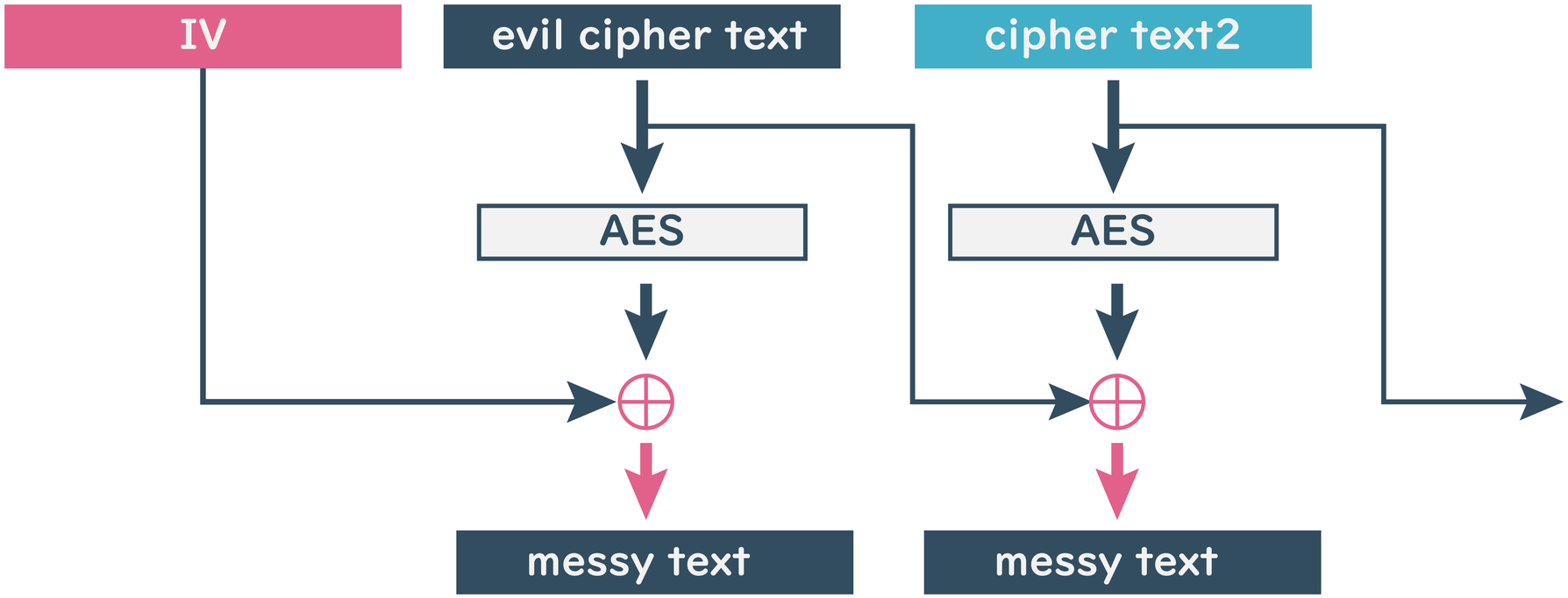
Encrypted using ECB mode



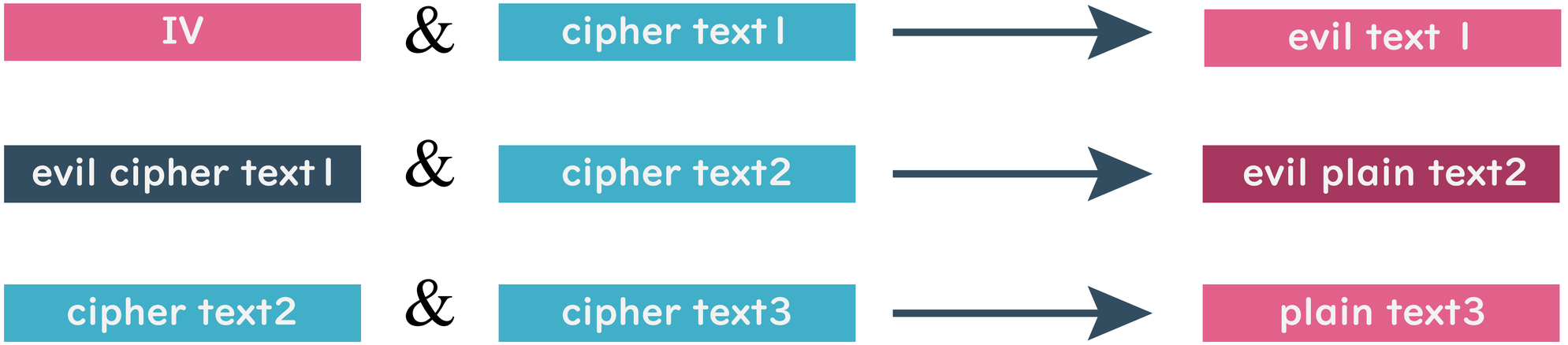
Encrypted using CBC mode

reference: https://jiang-zhenghong.github.io/blogs/PaddingOracle.html

What's CBC?


IV
evil cipher text
cipher text2
AES
AES
messy text
messy text

What's CBC?

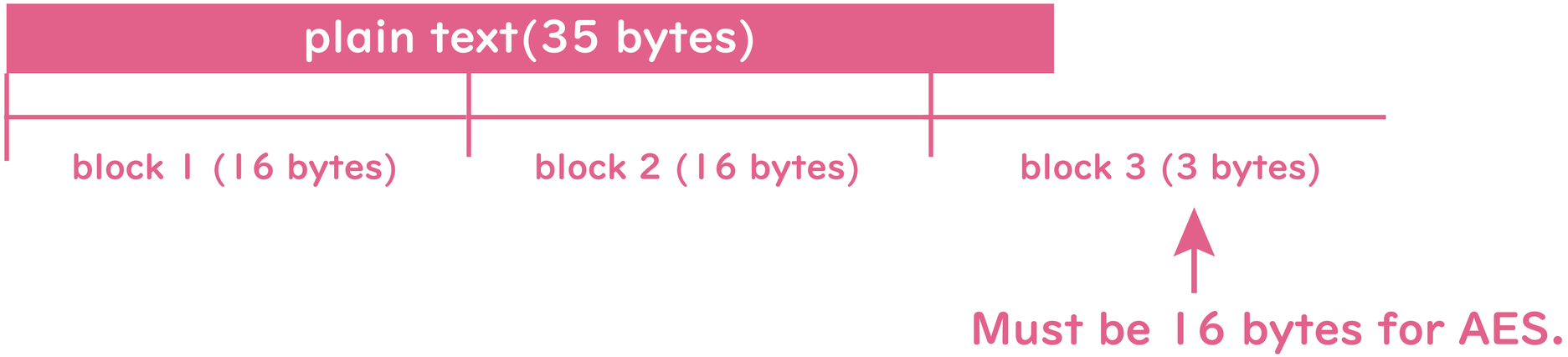


紅の魔術工房
Atelier kurenaif

when we want to change plain text 2,
evil cipher text l considering cipher text 2
is needed.

So, we simple block exchange attack
is not vaild.

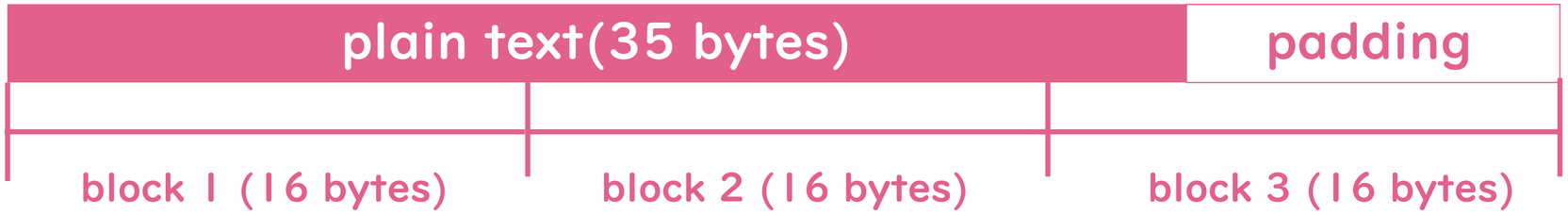
But depending on how it is used,
it could be weaker than the ECB.



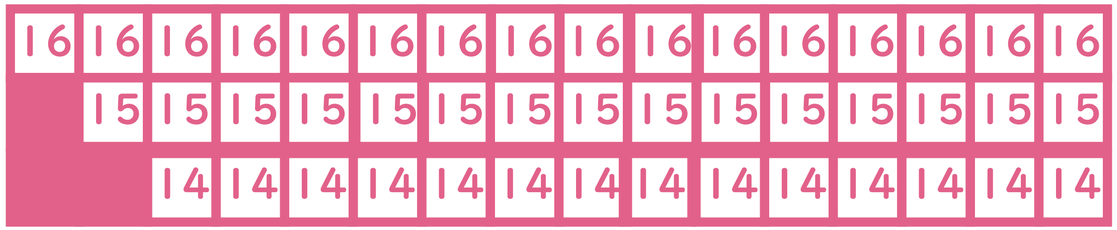
What's Padding?

Must be 16 bytes for AES.

What's Padding?



what's padding?



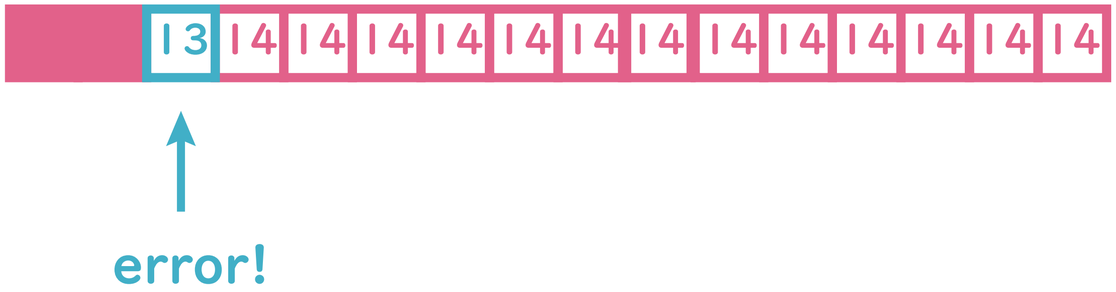
described in PKCS#7

What's Padding?

紅の魔術工房
Atelier kurenai

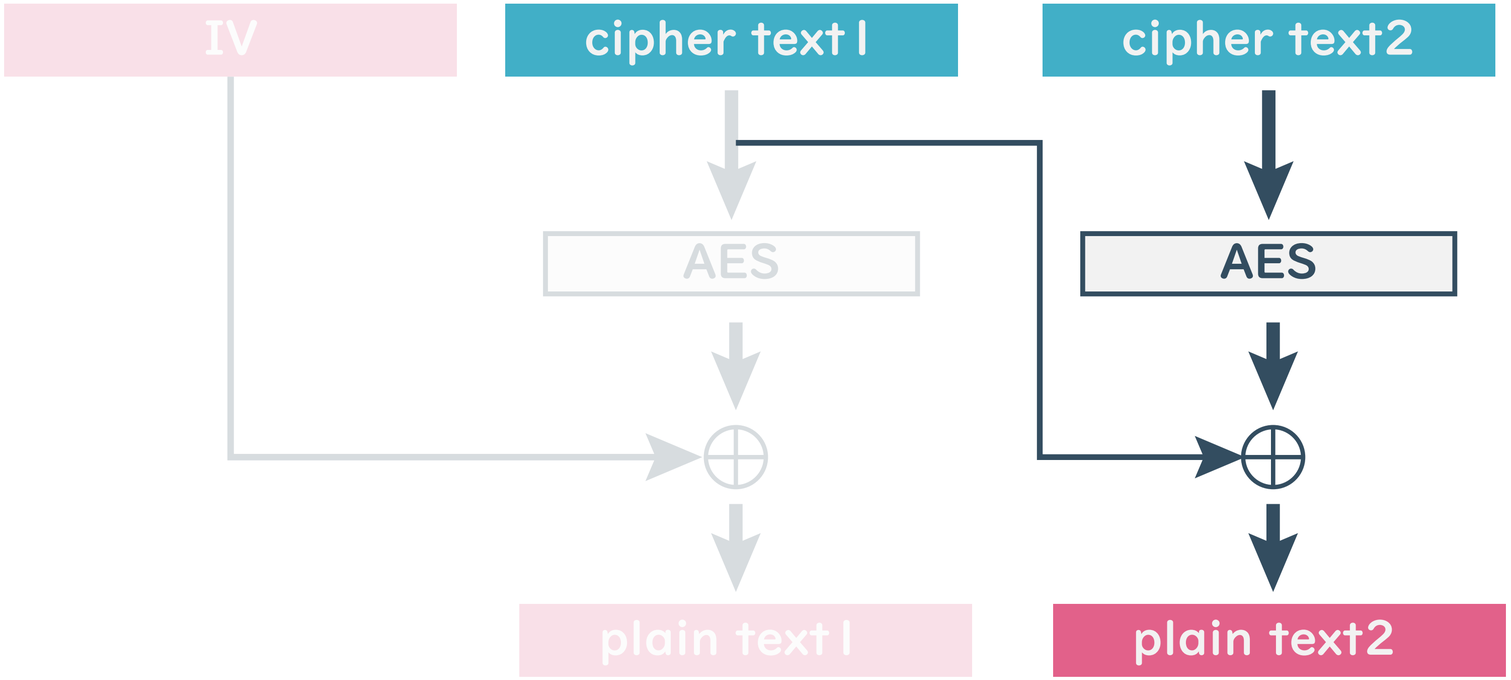
1. An attacker has (eavesdropped) cipher text
2. The cipher text is encrypted by CBC with PKCS#7 Padding
3. An attacker can know

whether an arbitrary ciphertext is a padding error or not.



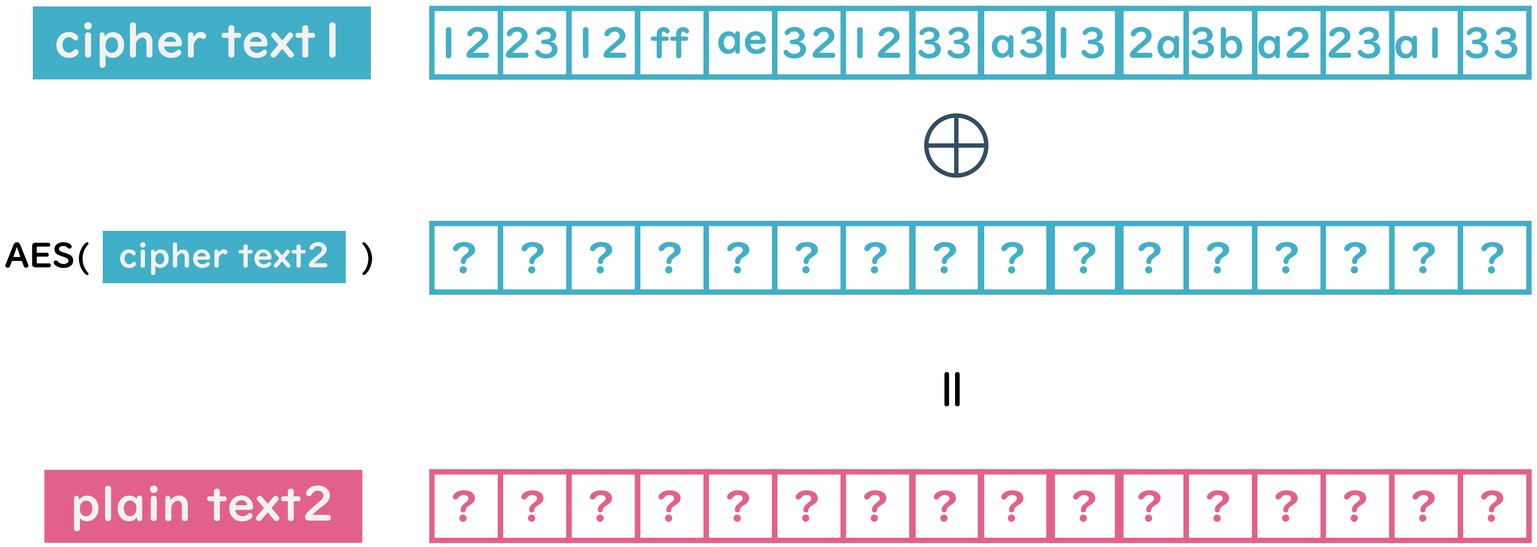
Attacker can get plain text!

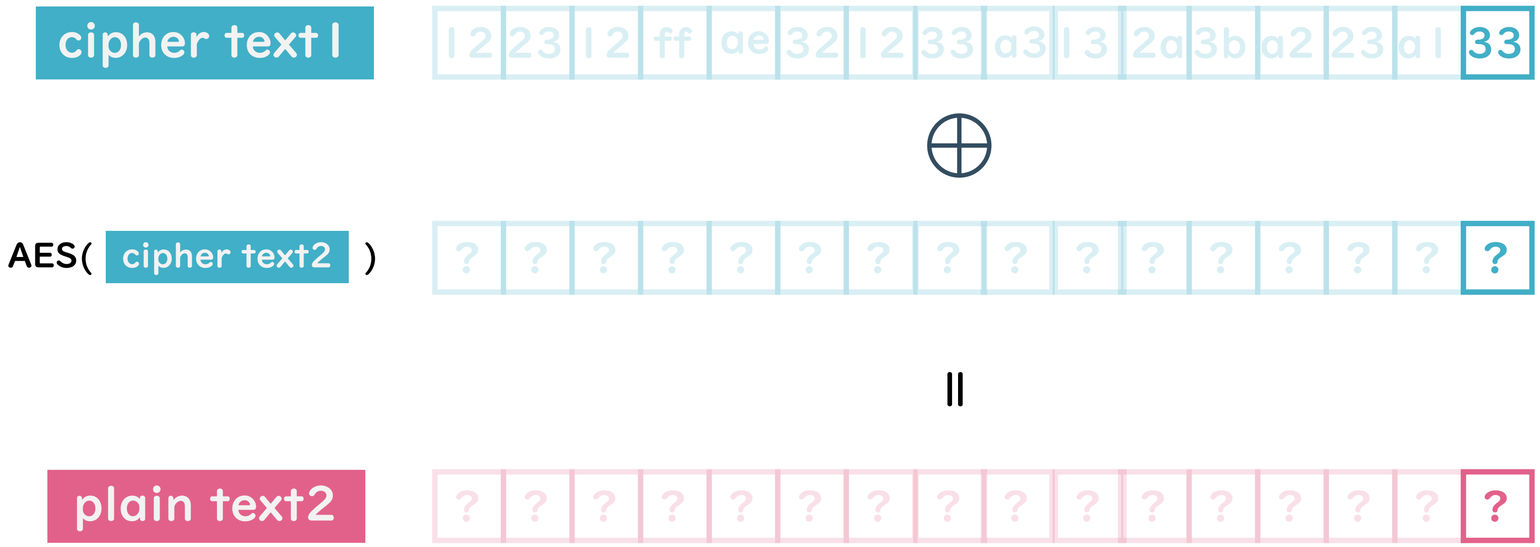
What's CBC Padding Oracle Attack?



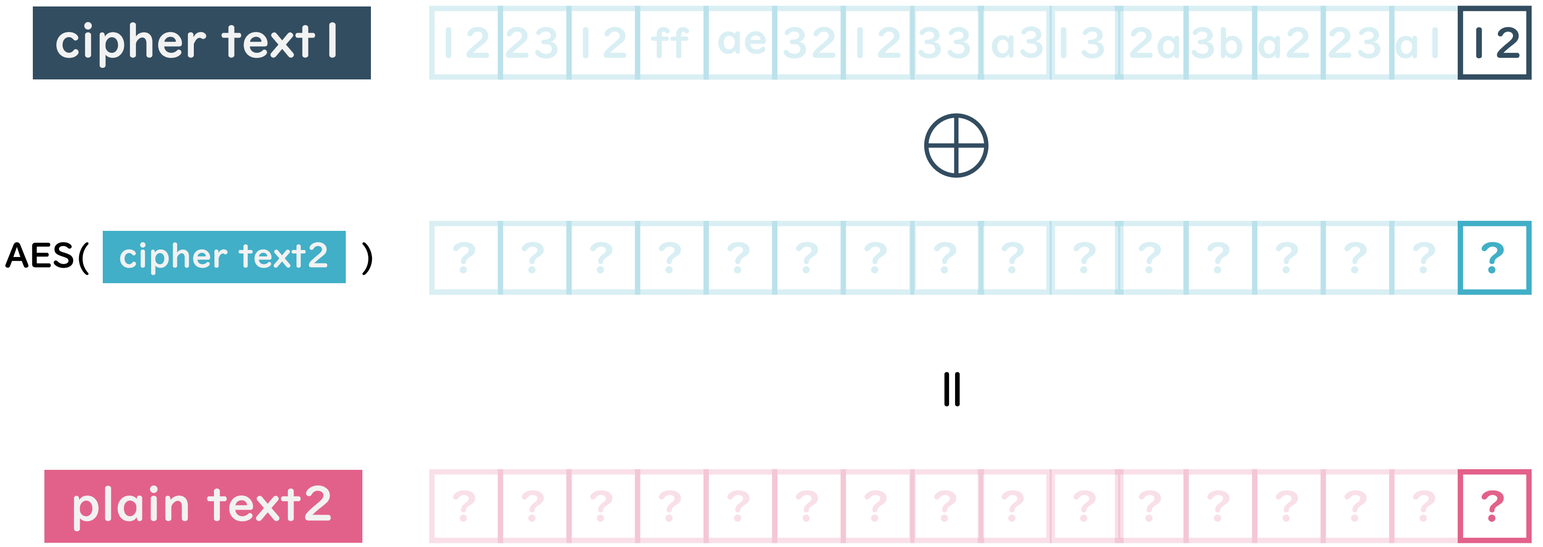
plain text2 = AES(cipher text2) ⊕ cipher text1

What's CBC Padding Oracle Attack?



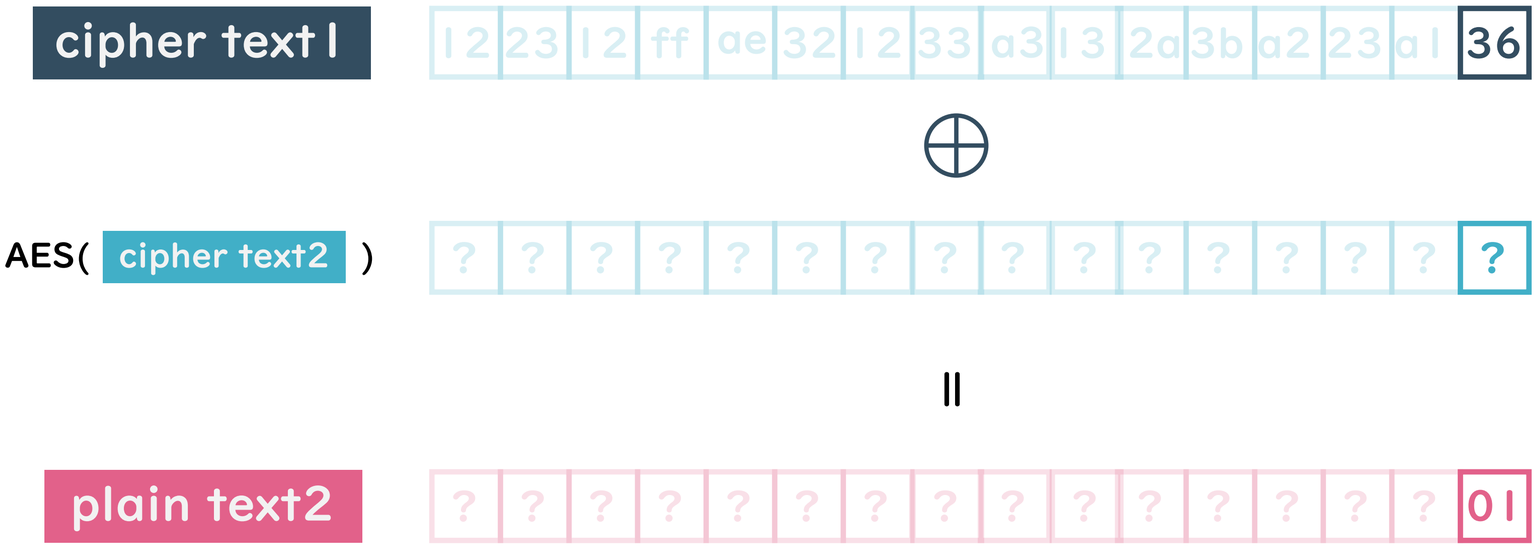


change last byte to
0~255 (check all cases!)



when Almost all case,
server response
“padding error”

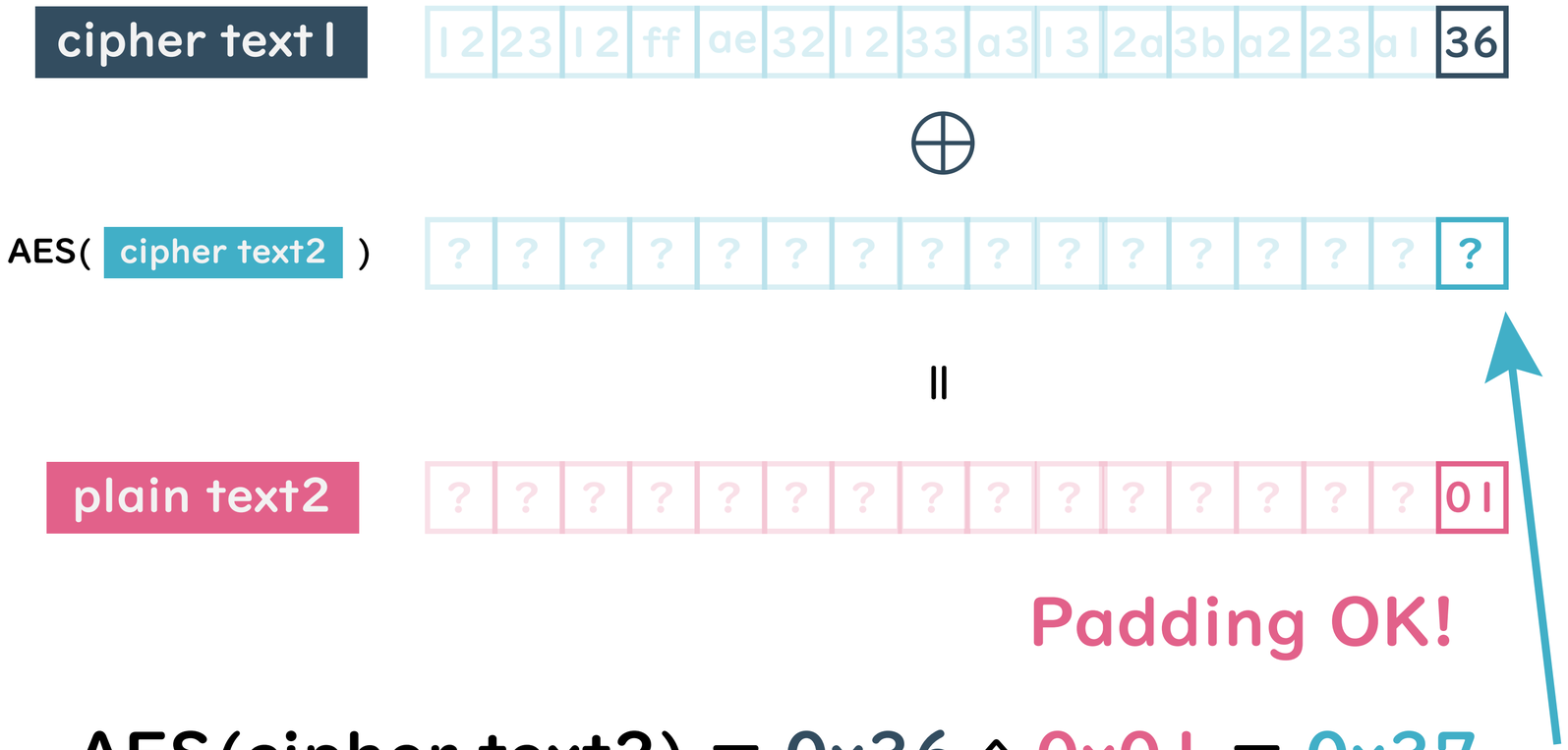
Padding Error!



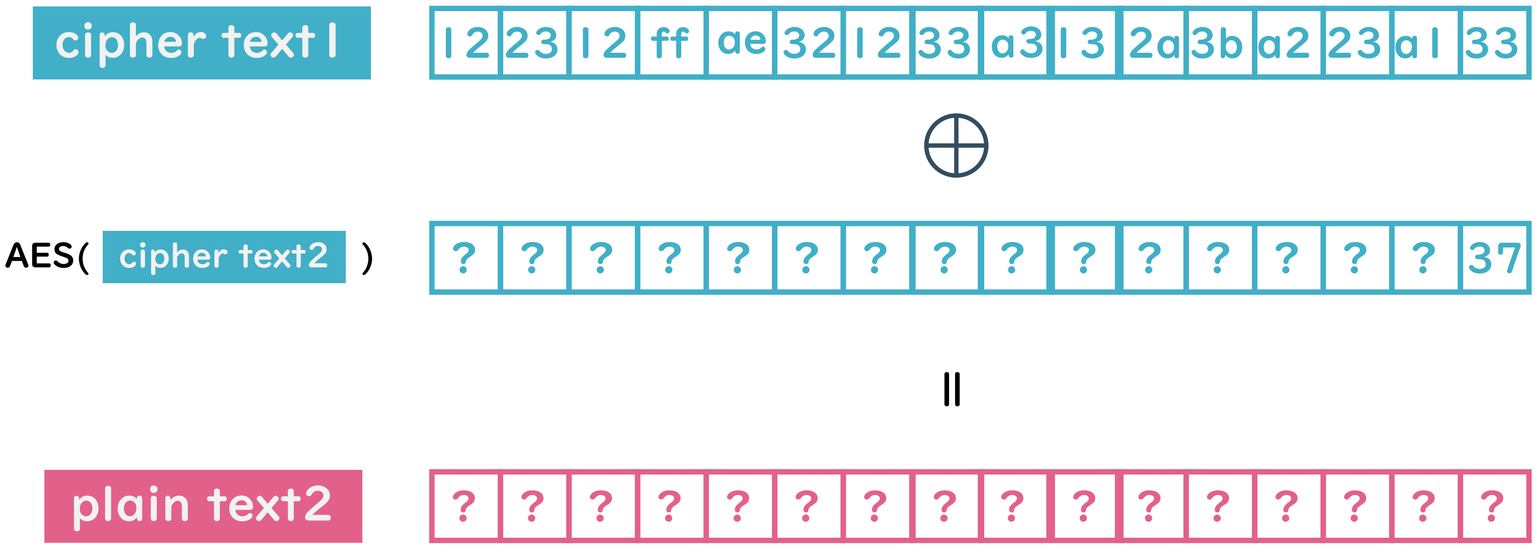
But one case,
server response
“padding OK”

Padding OK!

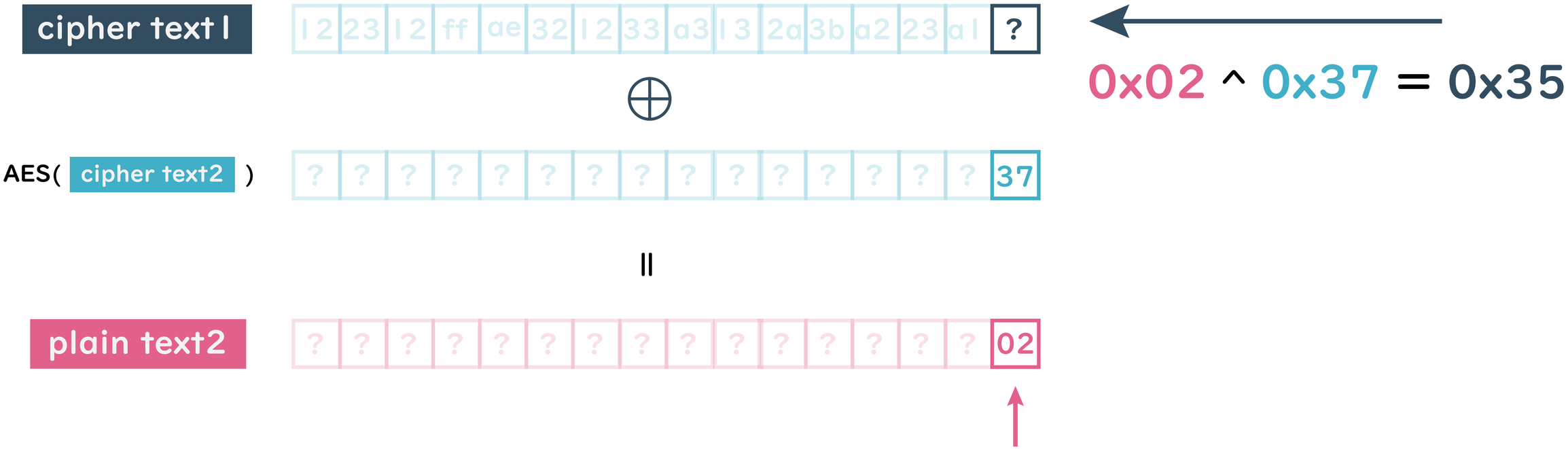
At that time, the attacker can know
that plain text 2 ends with 0x01.



AES(cipher text2) = 0x36 ^ 0x01 = 0x37

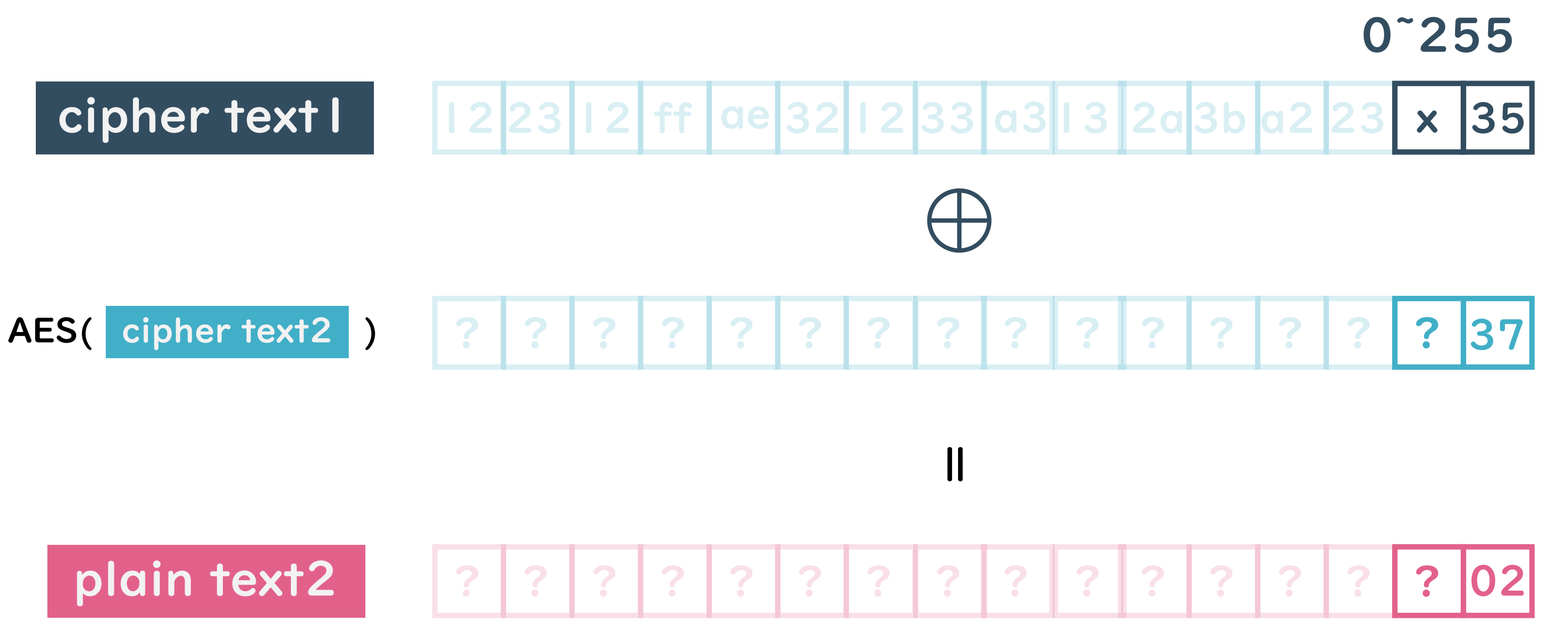


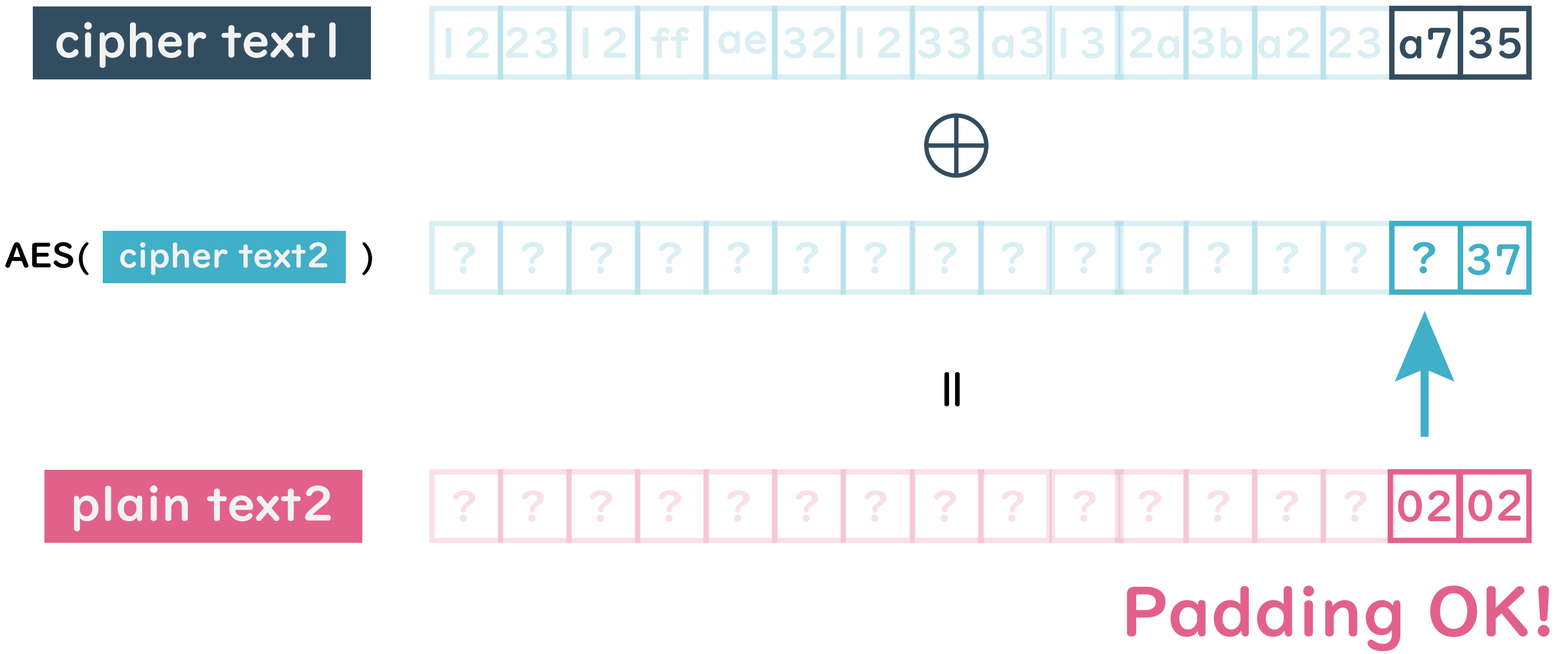
plain text2 = 0x33 ^ 0x37 = 0x04



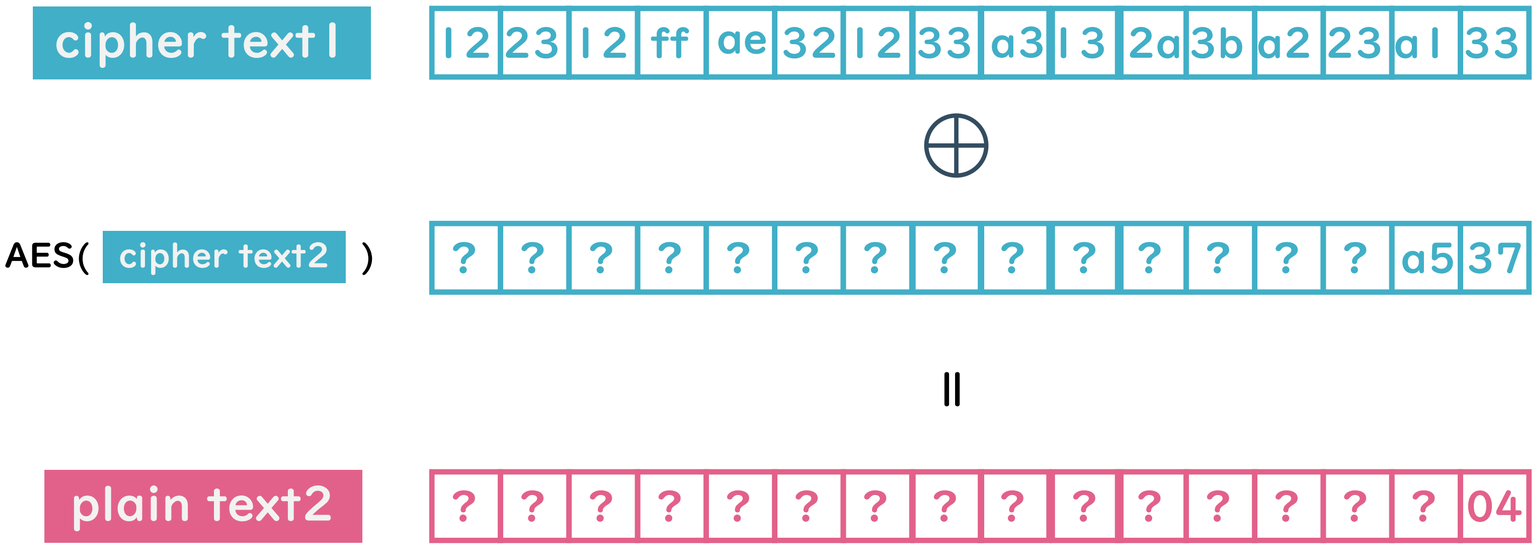
0x02 ^ 0x37 = 0x35

To expose second byte, set last byte to “0x02”

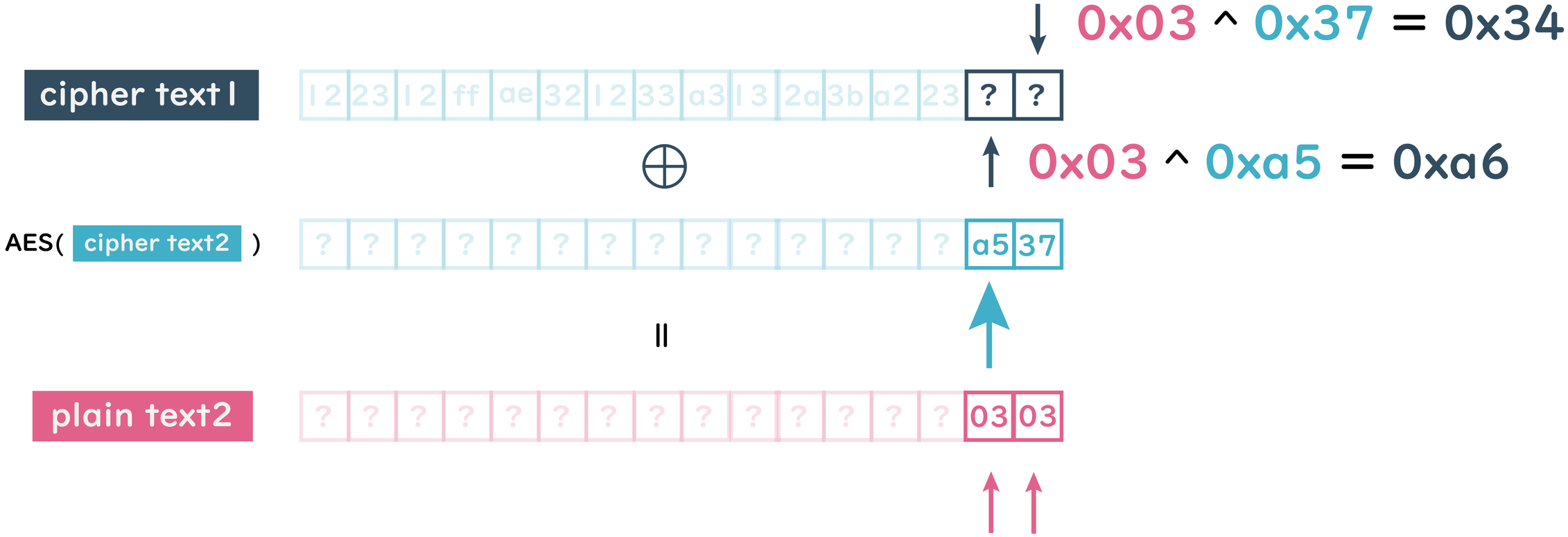


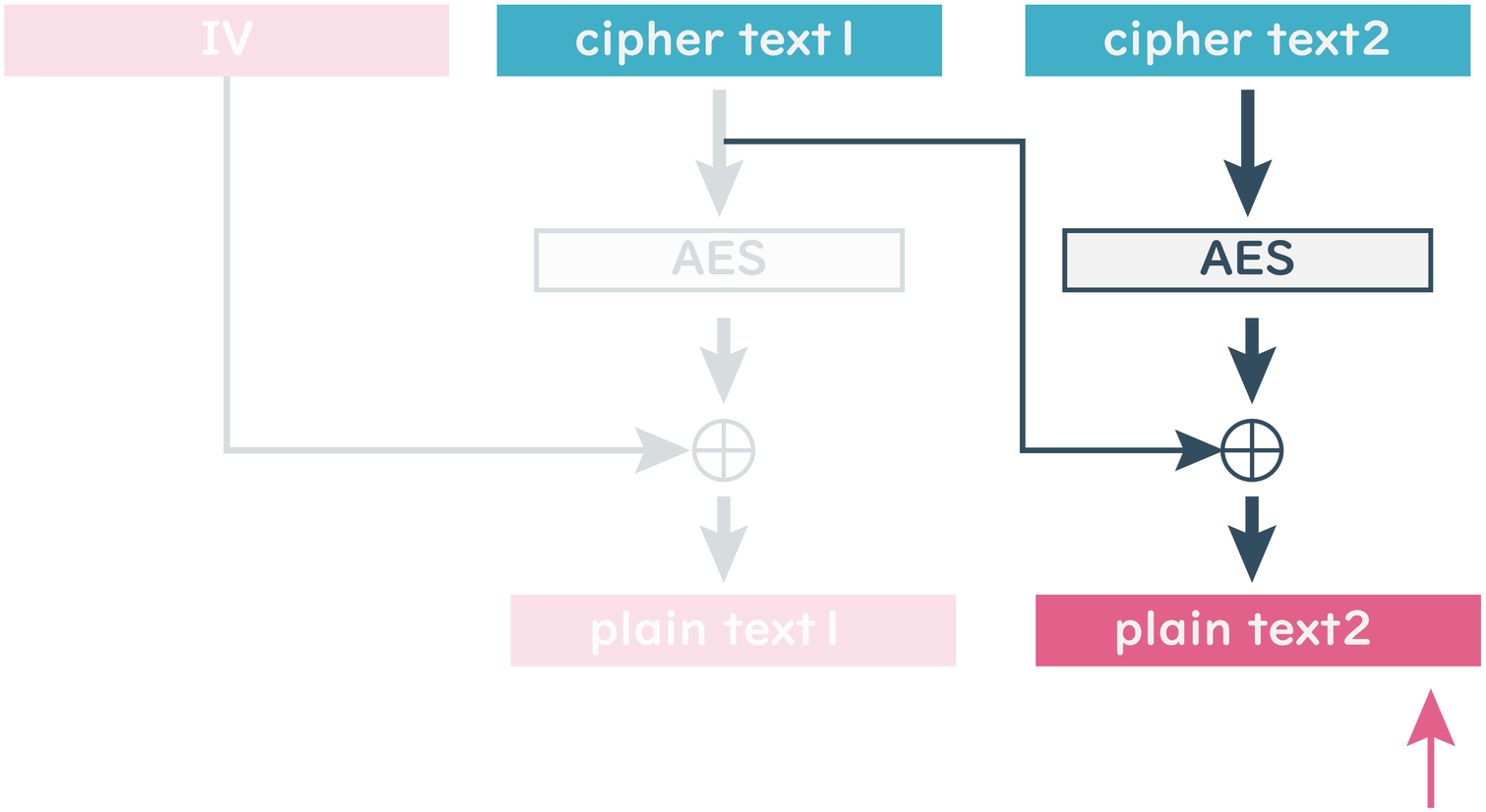


AES(cipher text2) = 0xa7 ^ 0x02 = 0xa5

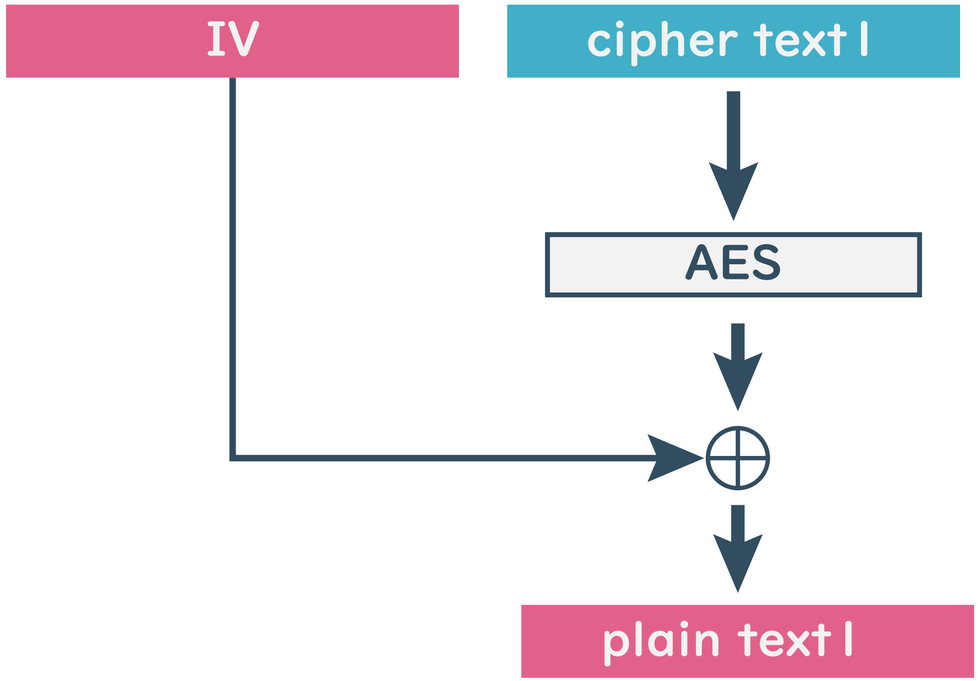


plain text2 = 0xa1 ^ 0xa5 = 0x04

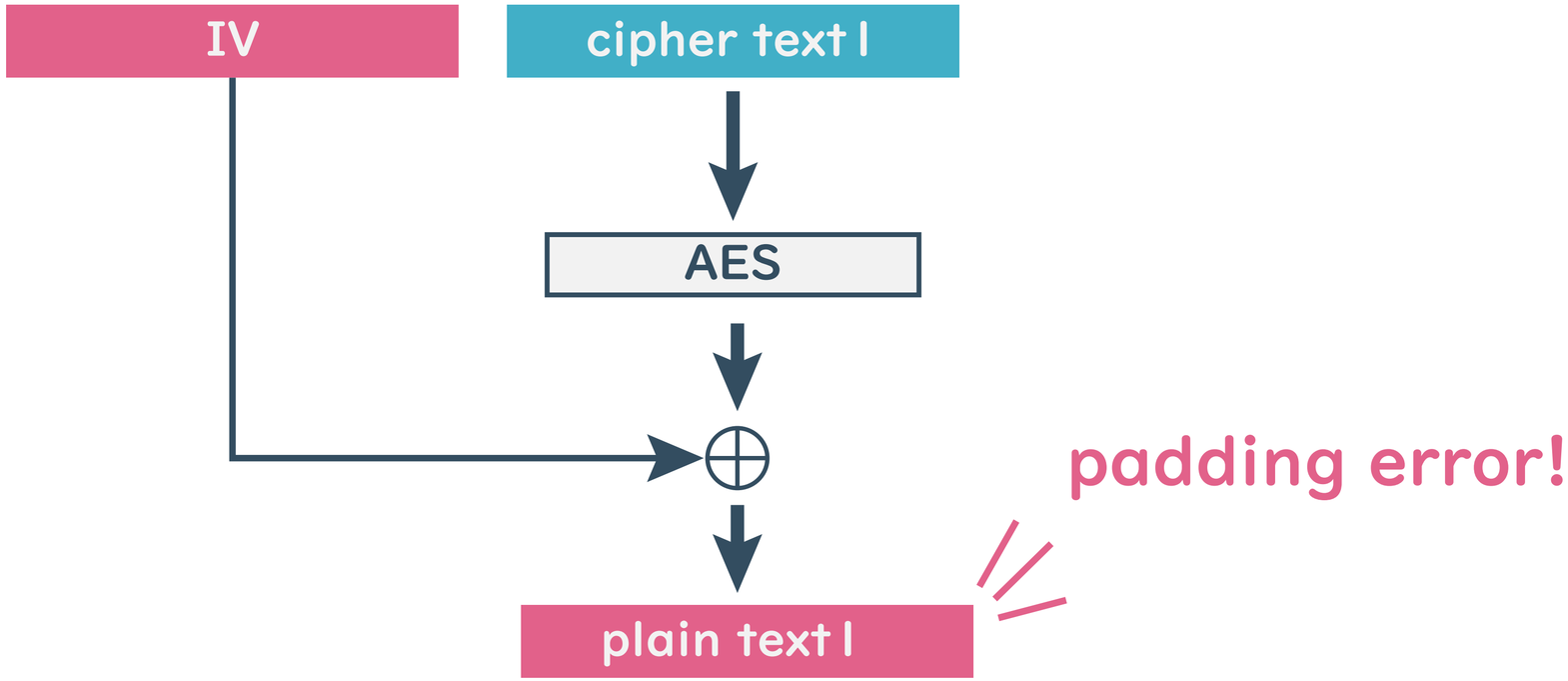

0x03 ^ 0x37 = 0x34
cipher text 1
12 23 12 ff ae 32 12 33 a3 13 2a 3b a2 23 ? ?
0x03 ^ 0xa5 = 0xa6
AES(cipher text2)
? ? ? ? ? ? ? ? ? ? ? ? ? ? a5 37
=
plain text2
? ? ? ? ? ? ? ? ? ? ? ? ? ? 03 03
To expose third byte, set last byte to “0x03”



When we could expose all of plain text2,
plain text1 is next target!



When delete cipher text2,
plain text l is last block



padding error!

So, when we apply same algorithm in this situation, we can exopse plain text l :)