EECS 388: Lab 3

Padding Oracle Attack
Bleichenbacher Attack

Current Assignments

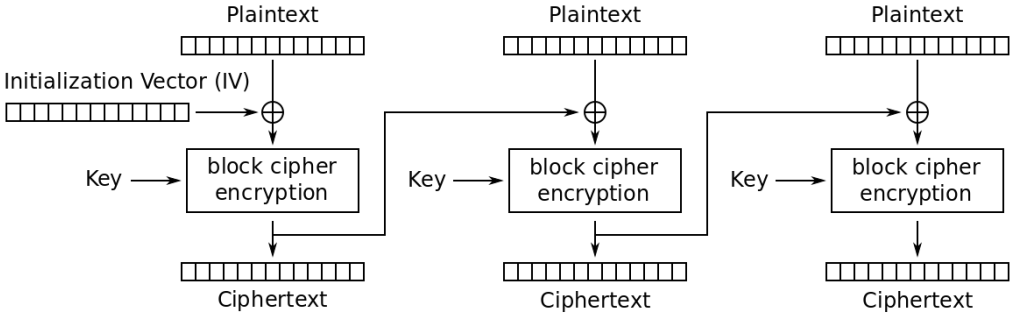
Reminder: Canvas quizzes due the day before the next lecture

- Project 1 Part 2 due **Thursday, September 19 at 6 p.m.**
  - Padding Oracle Attack
  - Bleichenbacher Attack (RSA signature forgery)

Padding Oracle Attack

Cipher Block Chaining (CBC) + MAC-then-Encrypt

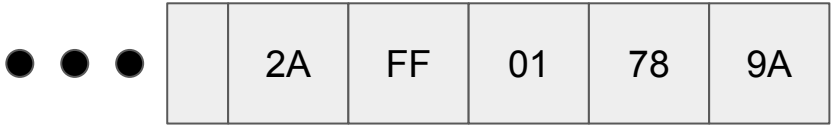
- Last block uses padding to fit the block size
- Notoriously hard to implement correctly
- Vulnerable to Padding Oracle Attack
  - https://www.youtube.com/watch?v=O5SeQxErXA4

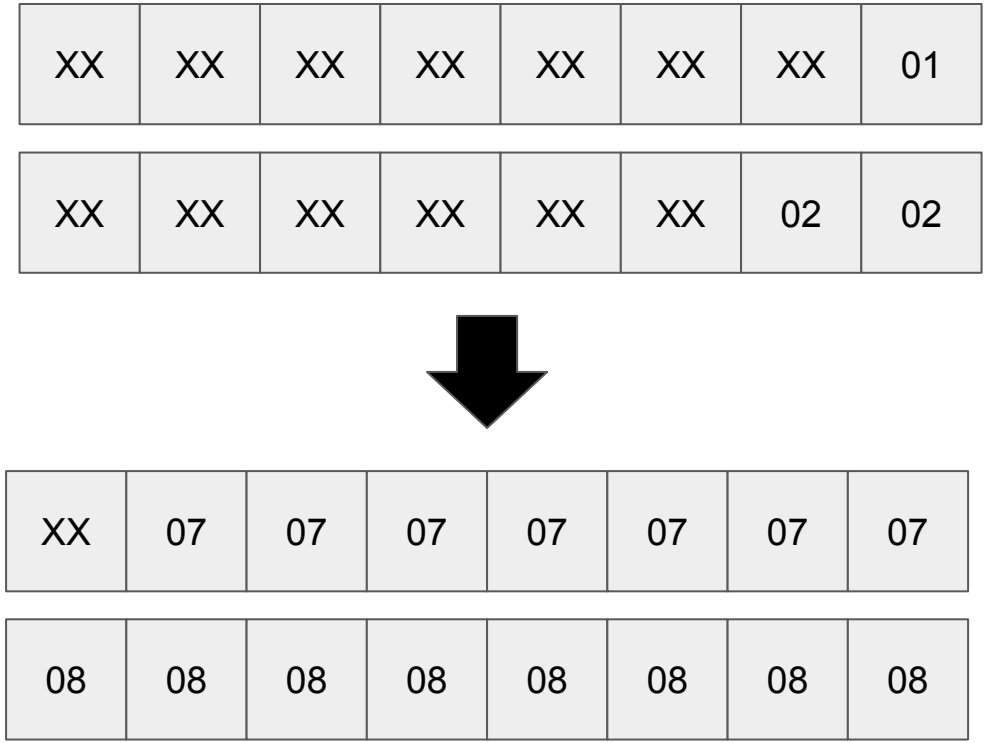


Cipher Block Chaining (CBC) mode encryption

Padding

- What if our message is not a multiple of the block size?
- Allows us to use CBC without ambiguity in the resulting message
- PKCS #7





XOR Properties

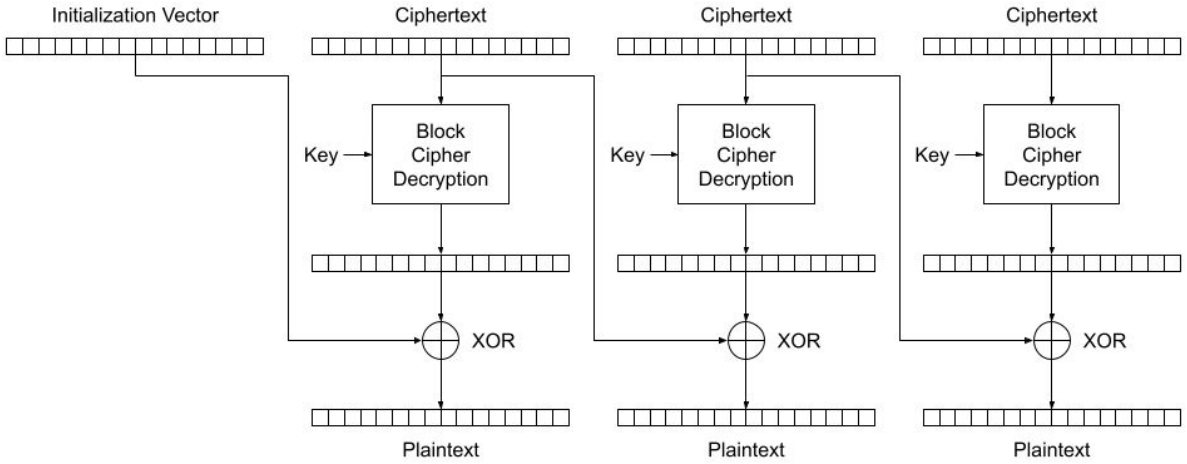
- $A \oplus A = 0$
- $A \oplus 0 = A$
- $A \oplus B = B \oplus A$
- If $A \oplus B = C$,
  then $C \oplus B = A$
  and $C \oplus A = B$

XOR truth table

Input		Output
A	B	
0	0	0
0	1	1
1	0	1
1	1	0

Padding Oracle Attack!

- You are Mallory and you've just intercepted an encrypted message from Alice to Bob. You know that Alice used CBC.
- Bob's server will tell you whether or not the padding was correct

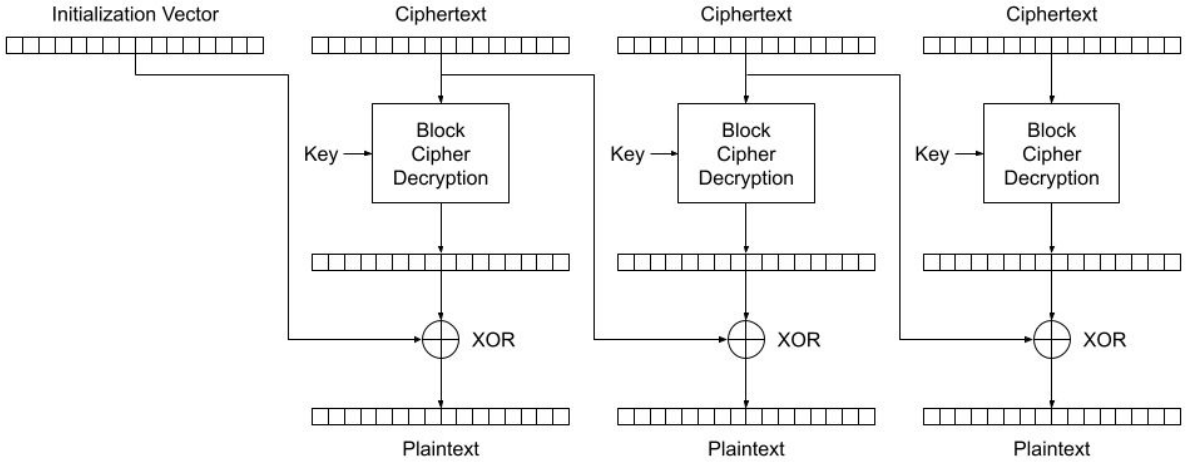


All Mallory has is ciphertext

Bob decrypts and lets you know if the padding is valid or not

Padding Oracle Attack!

- Mallory can modify the ciphertext and get feedback from Bob
- Assume Bob is using AES with PKCS #7 padding
  - Last block is padded with the number of padding bytes (`R,E,A,L,S,T,U,F,F,7,7,7,7,7,7,7`)
- What can Mallory do with this?

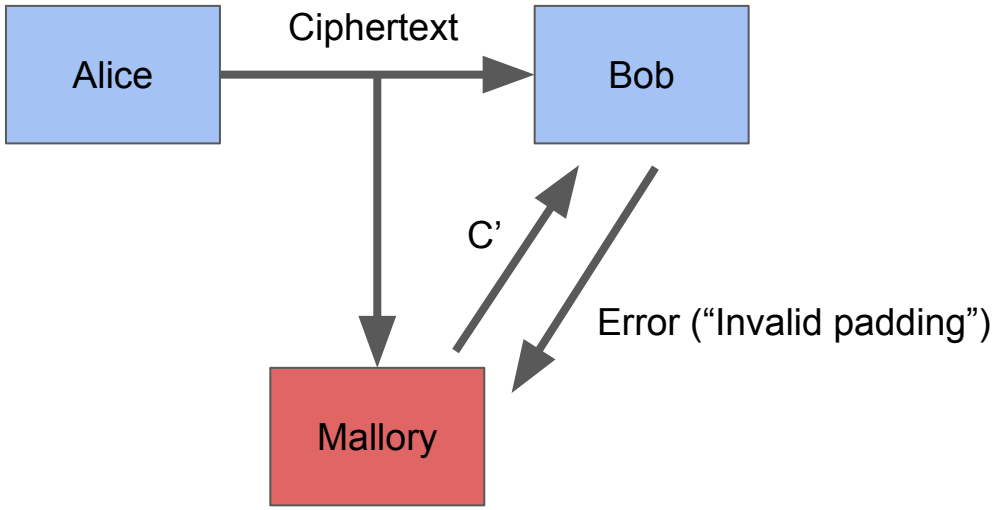


All Mallory has is ciphertext

Bob decrypts and lets you know if the padding is valid or not

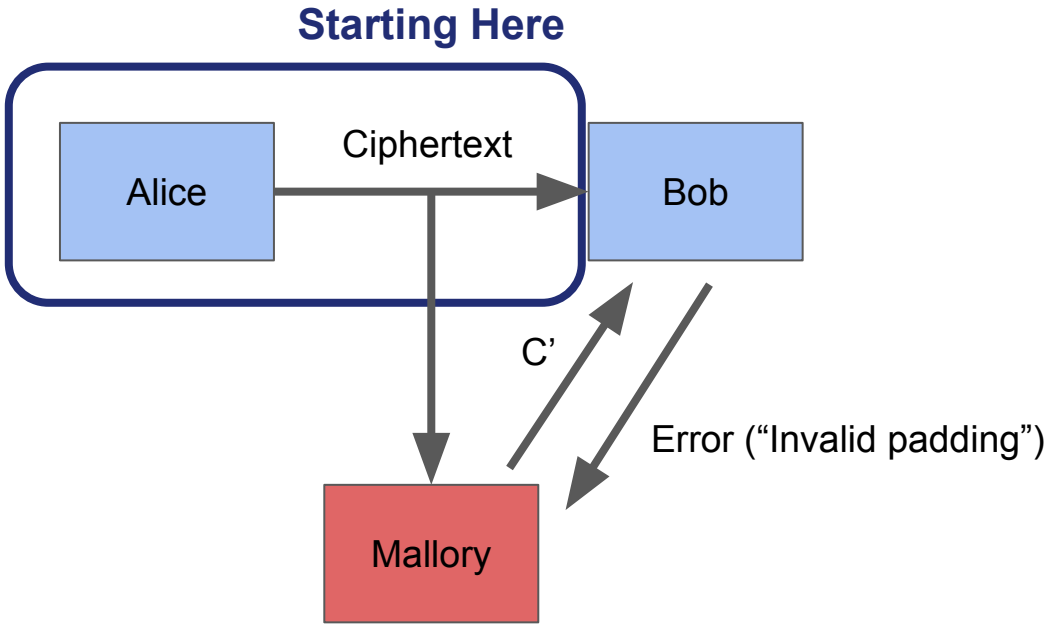
Premise

- Mallory initially only knows the ciphertext
- Mallory is able to query Bob to incrementally decrypt the ciphertext

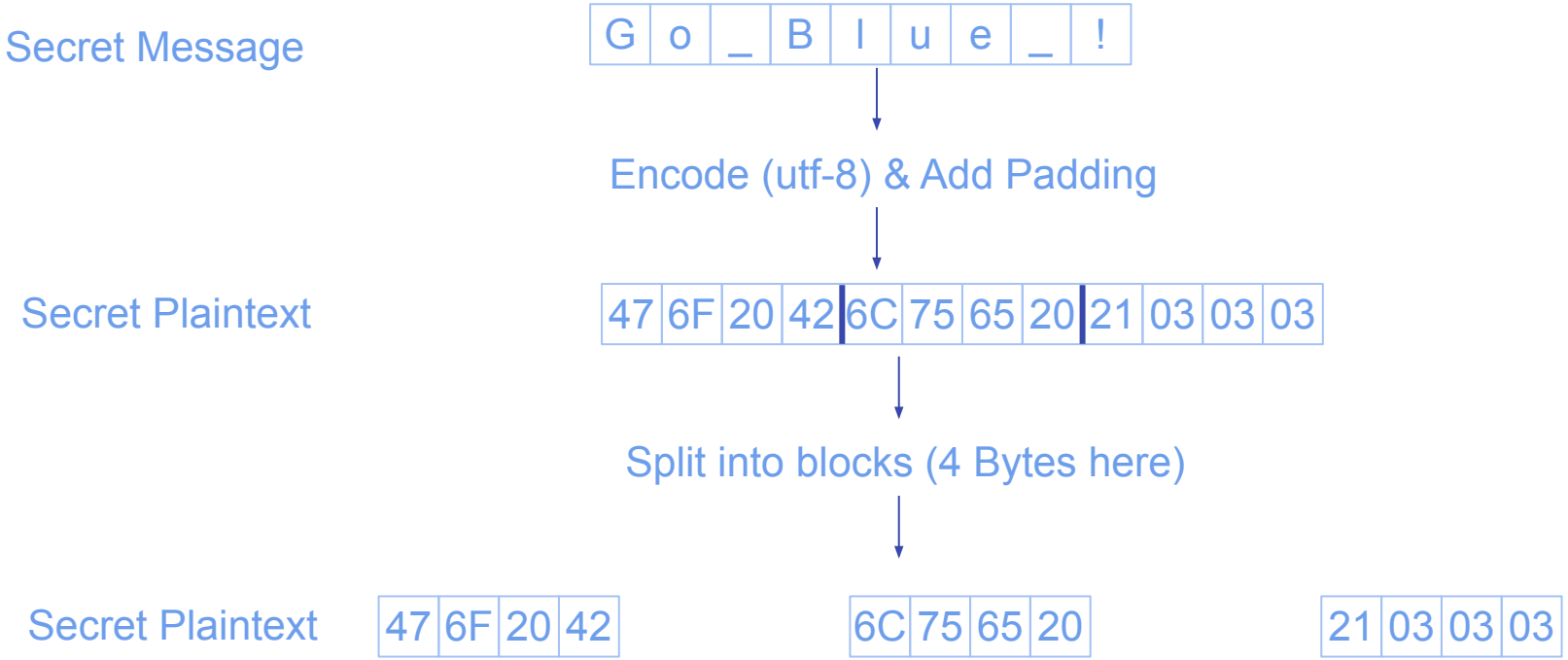


Premise

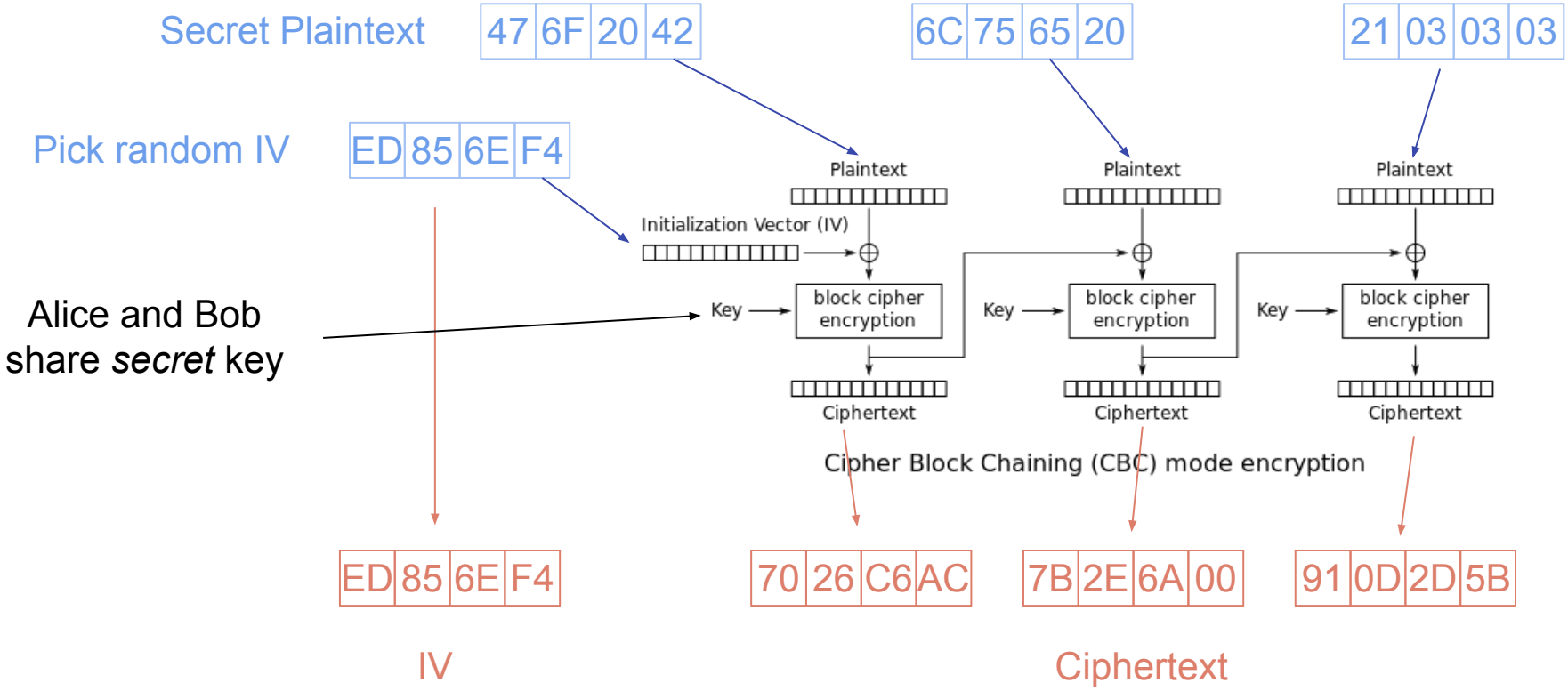
- Mallory initially only knows the ciphertext
- Mallory is able to query Bob to incrementally decrypt the ciphertext



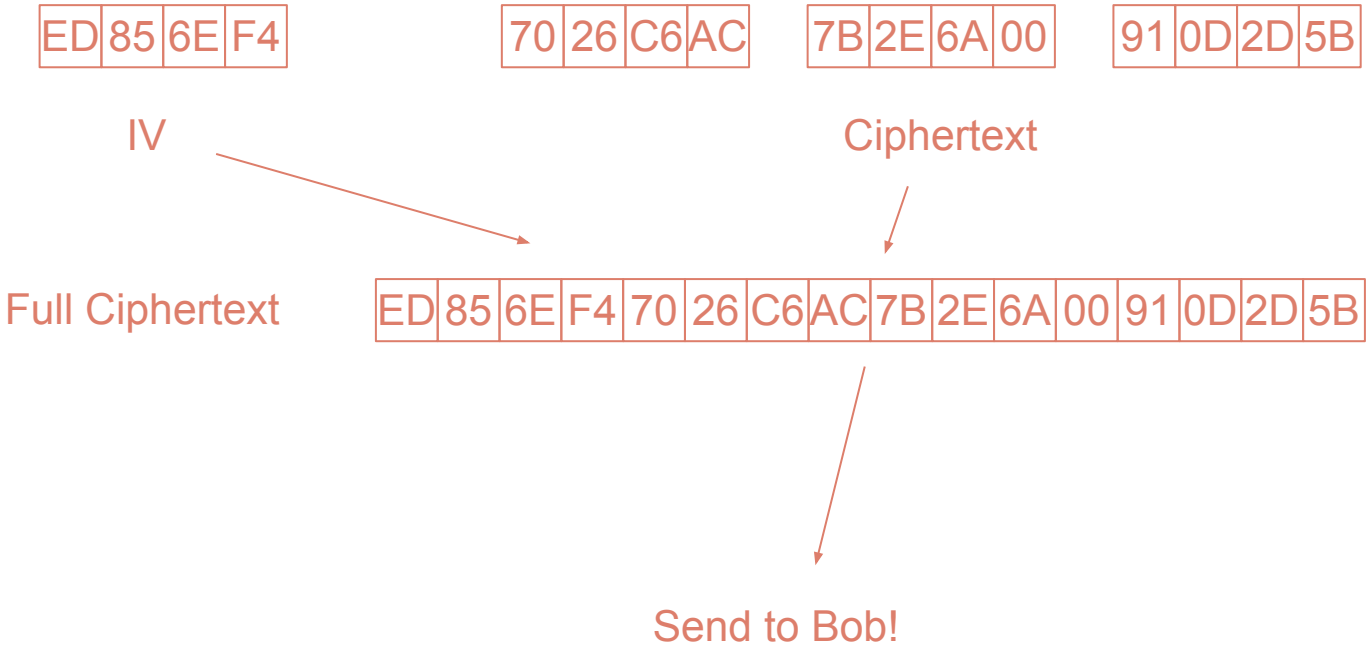
Alice’s Encryption



Alice's Encryption (cont.)

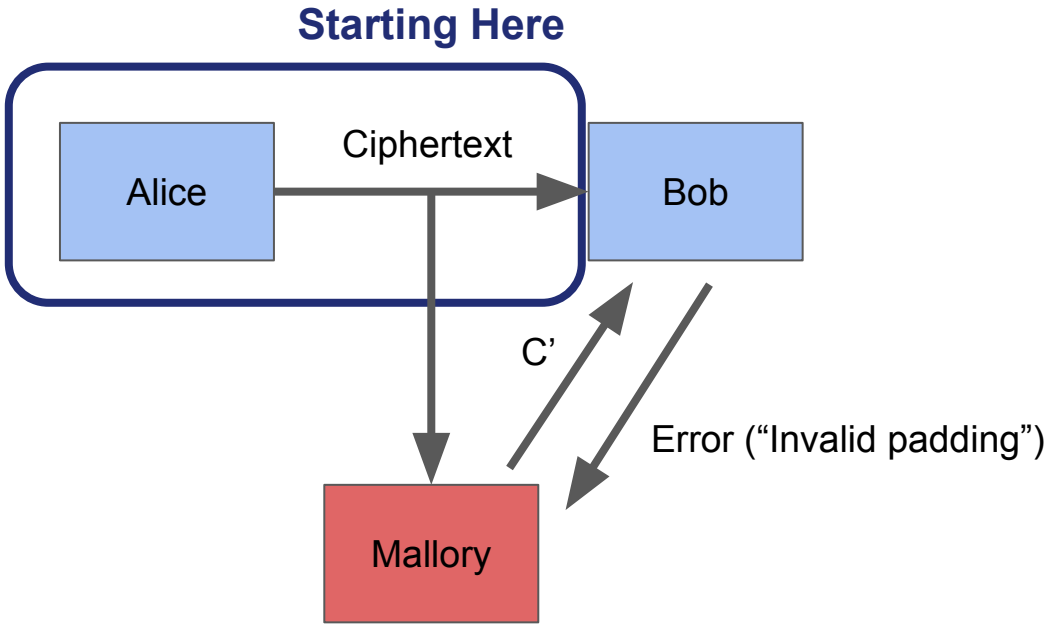


Alice’s Encryption (cont.)



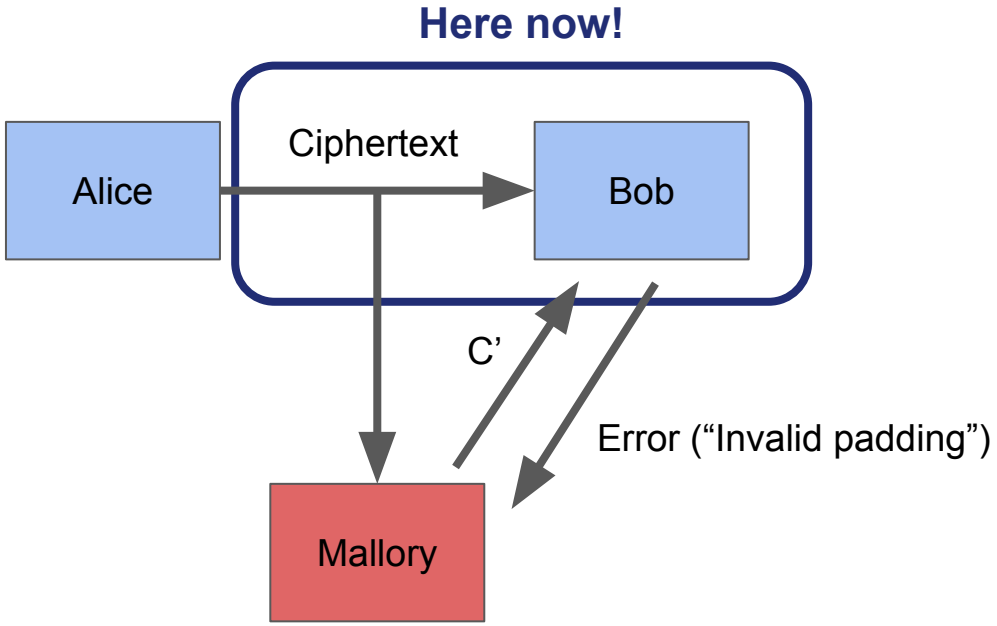
Premise

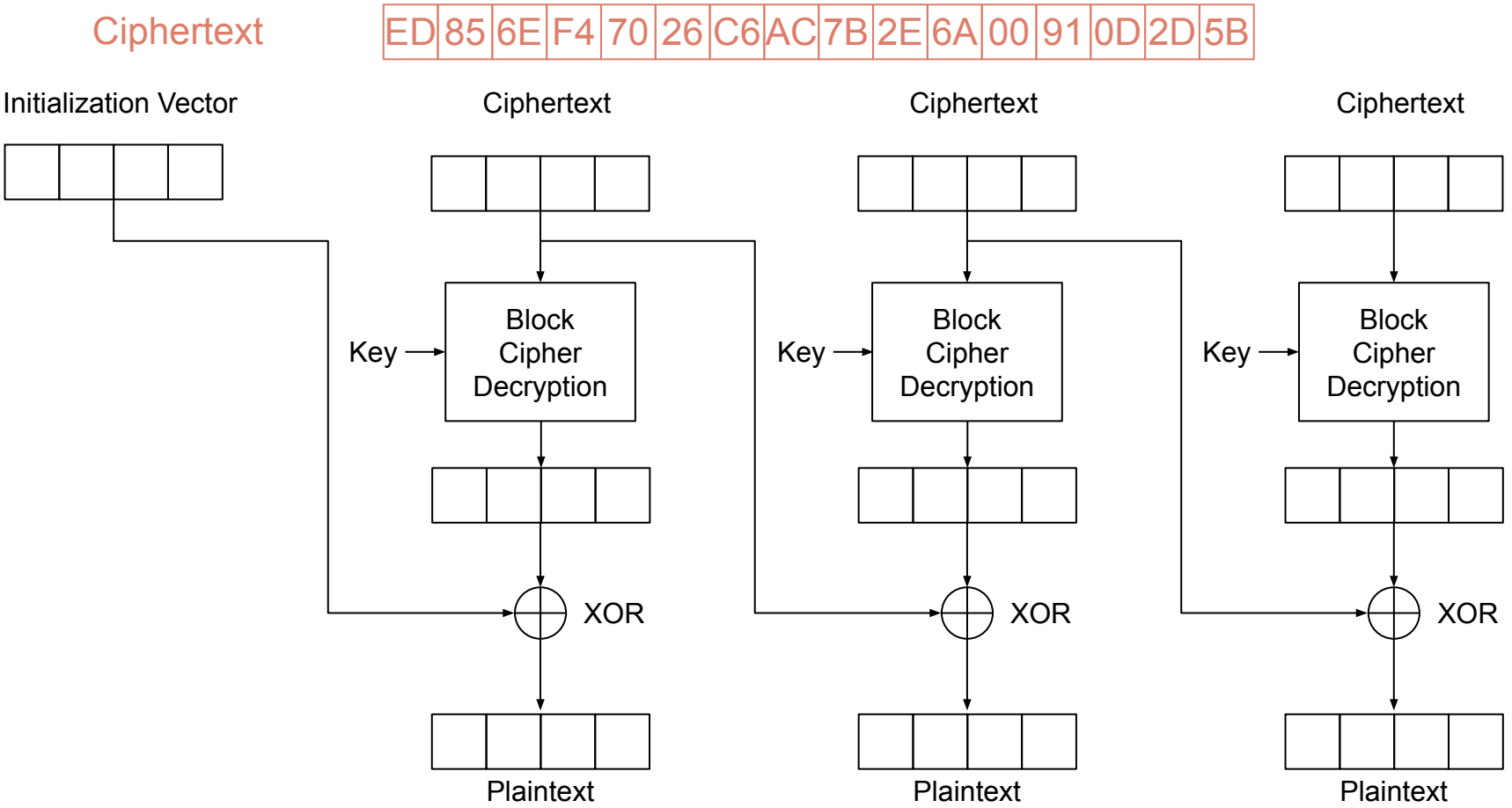
- Mallory initially only knows the ciphertext
- Mallory is able to query Bob to incrementally decrypt the ciphertext



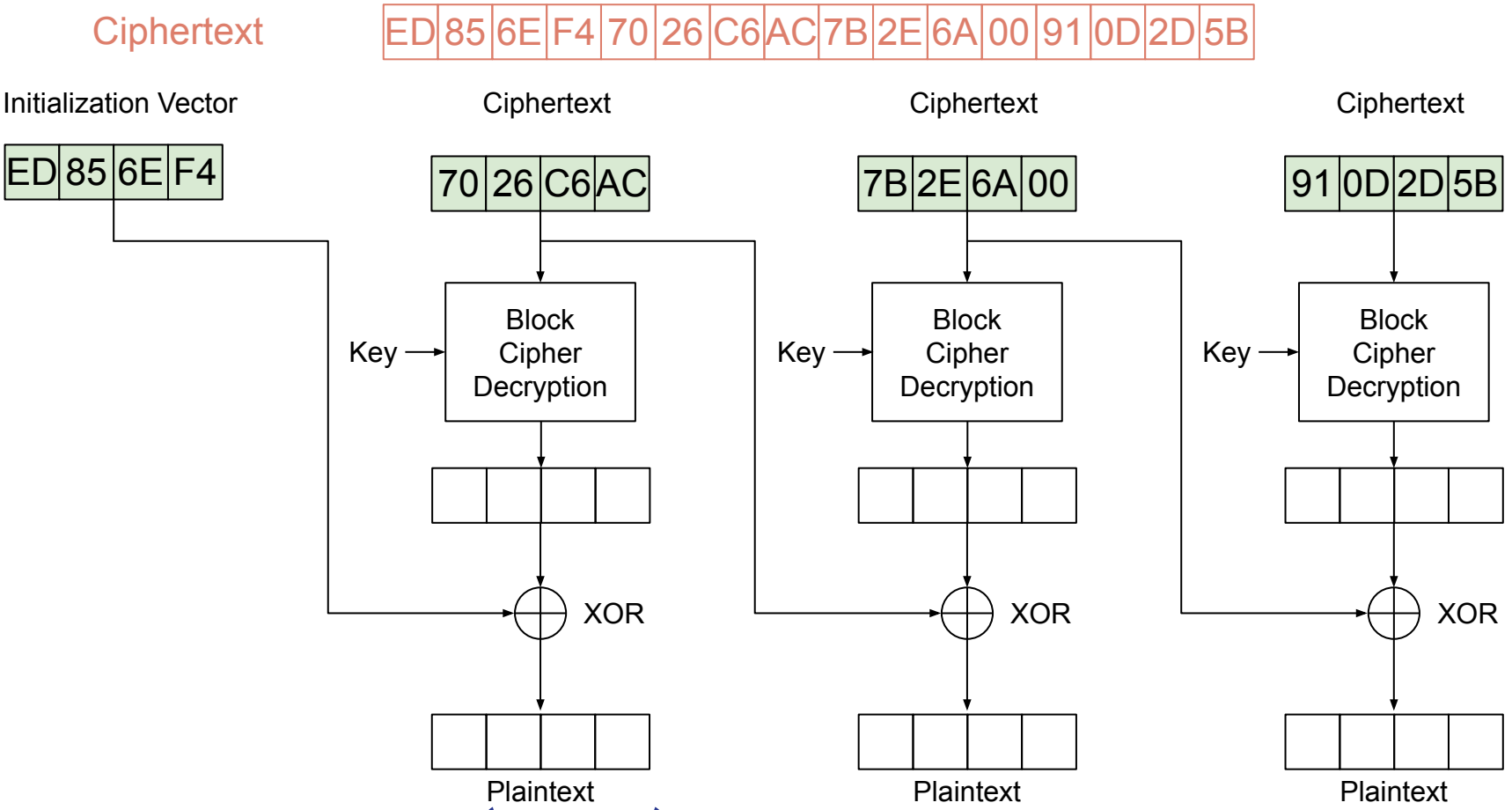
Premise

- Mallory initially only knows the ciphertext
- Mallory is able to query Bob to incrementally decrypt the ciphertext

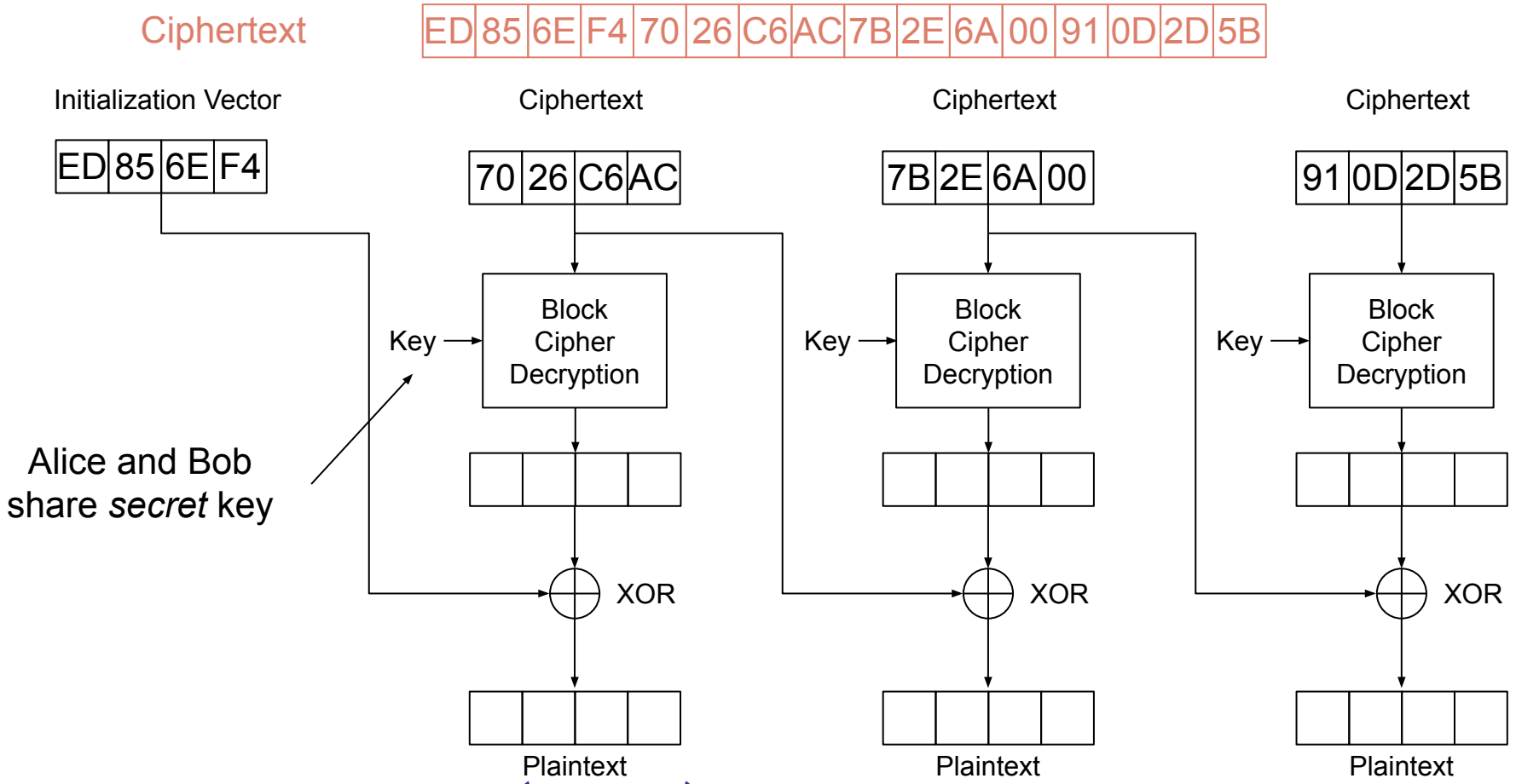




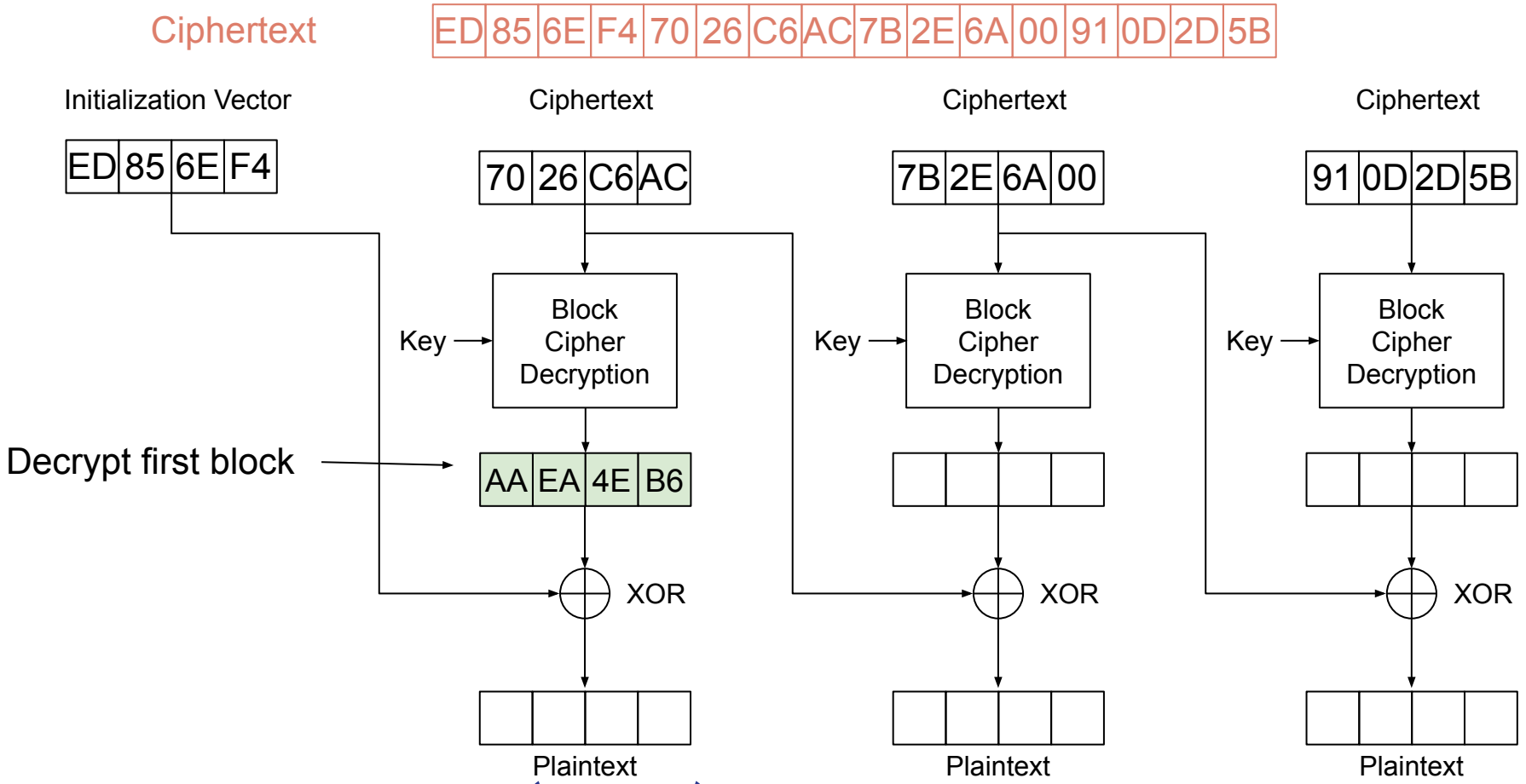
Bob's Decryption



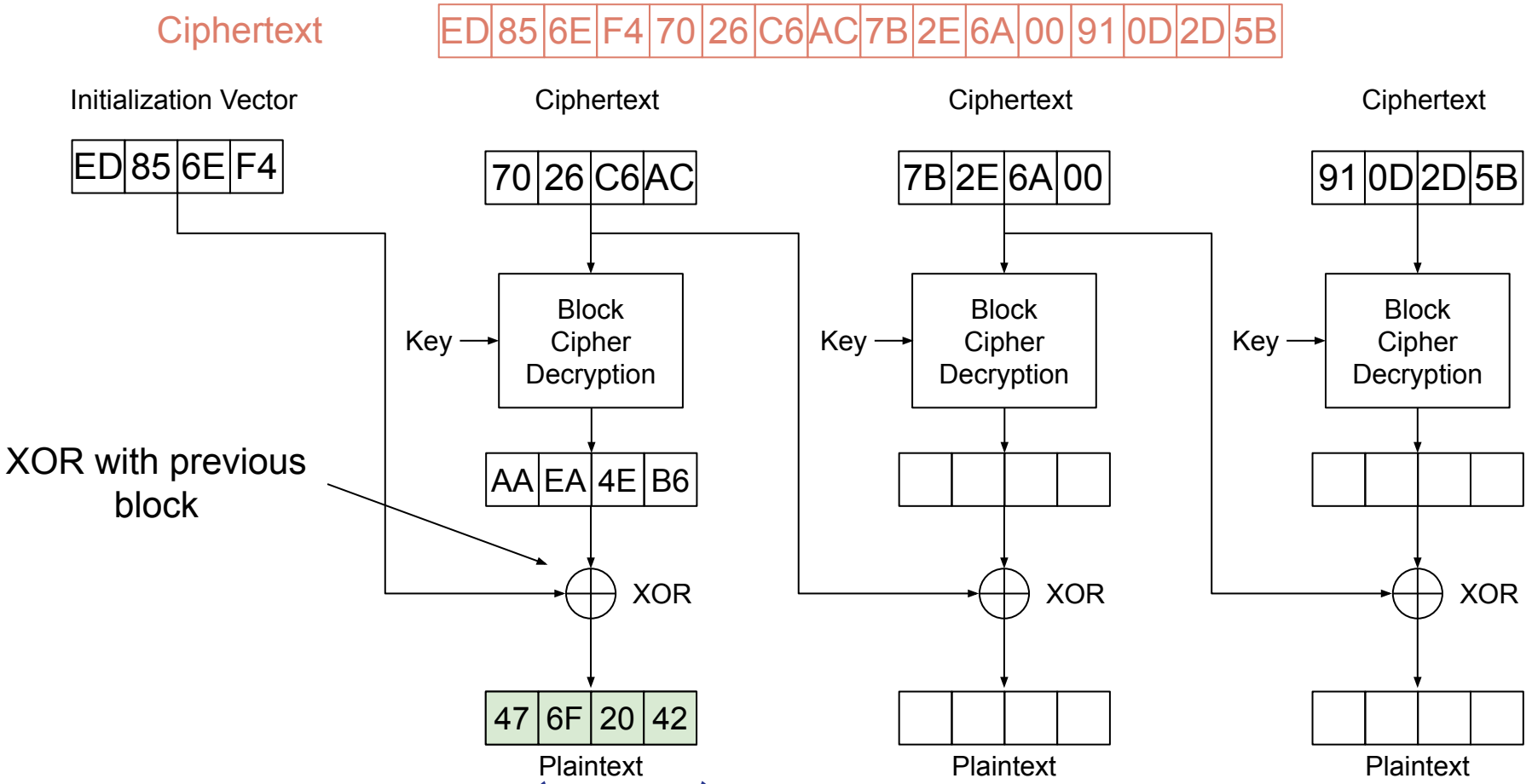
Bob’s Decryption (cont.)



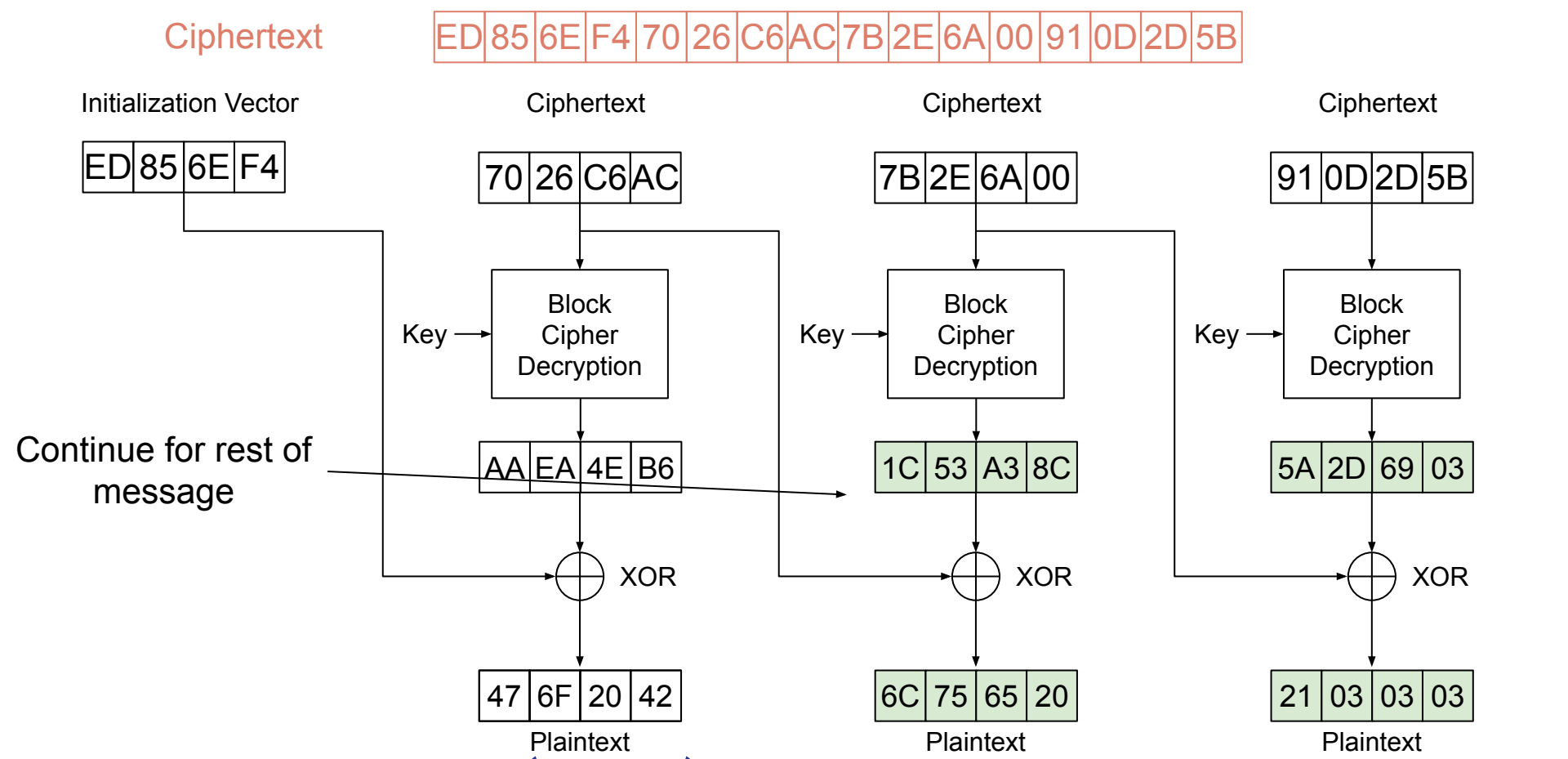
Bob's Decryption (cont.)



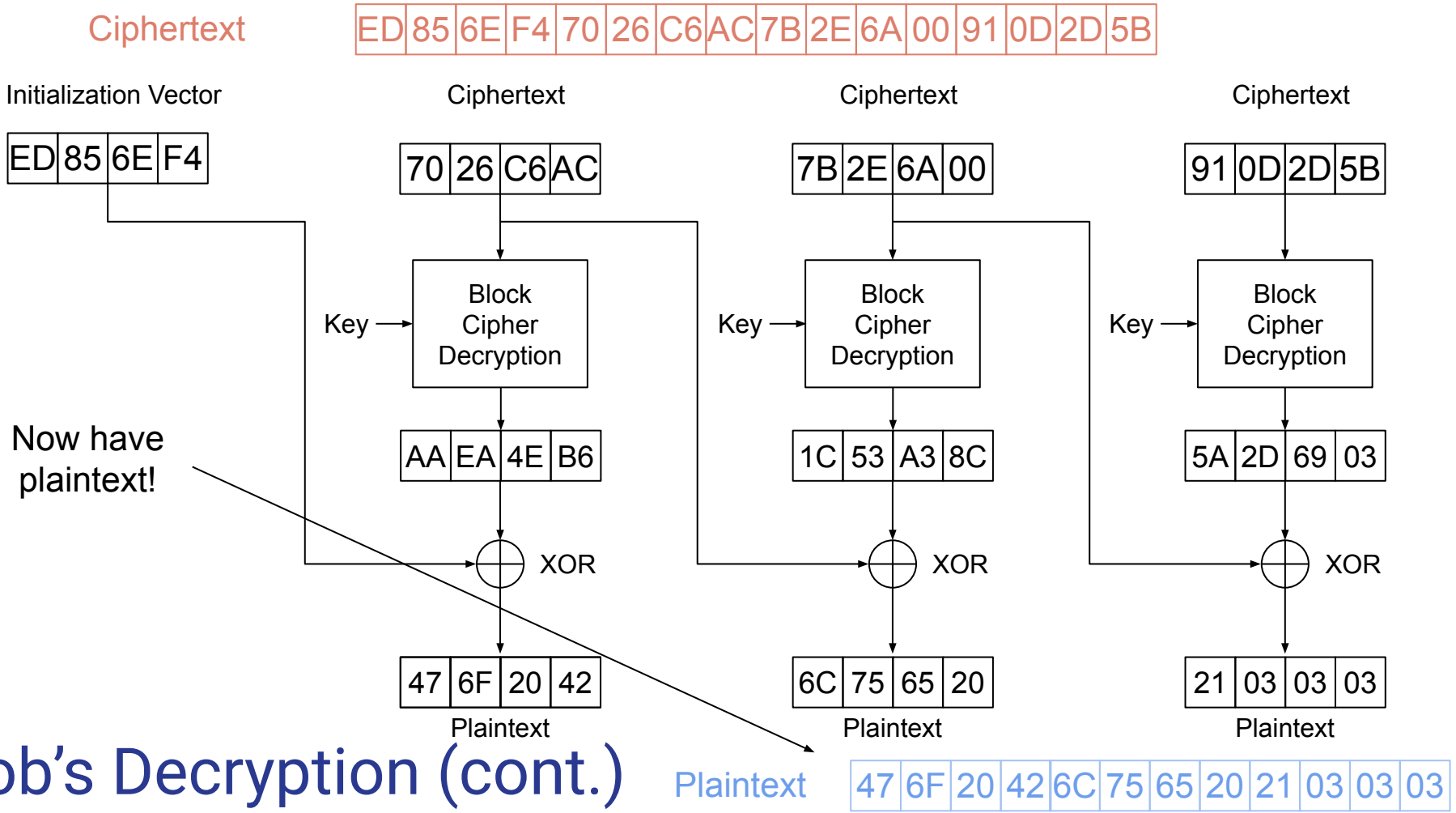
Bob's Decryption (cont.)



Bob's Decryption (cont.)

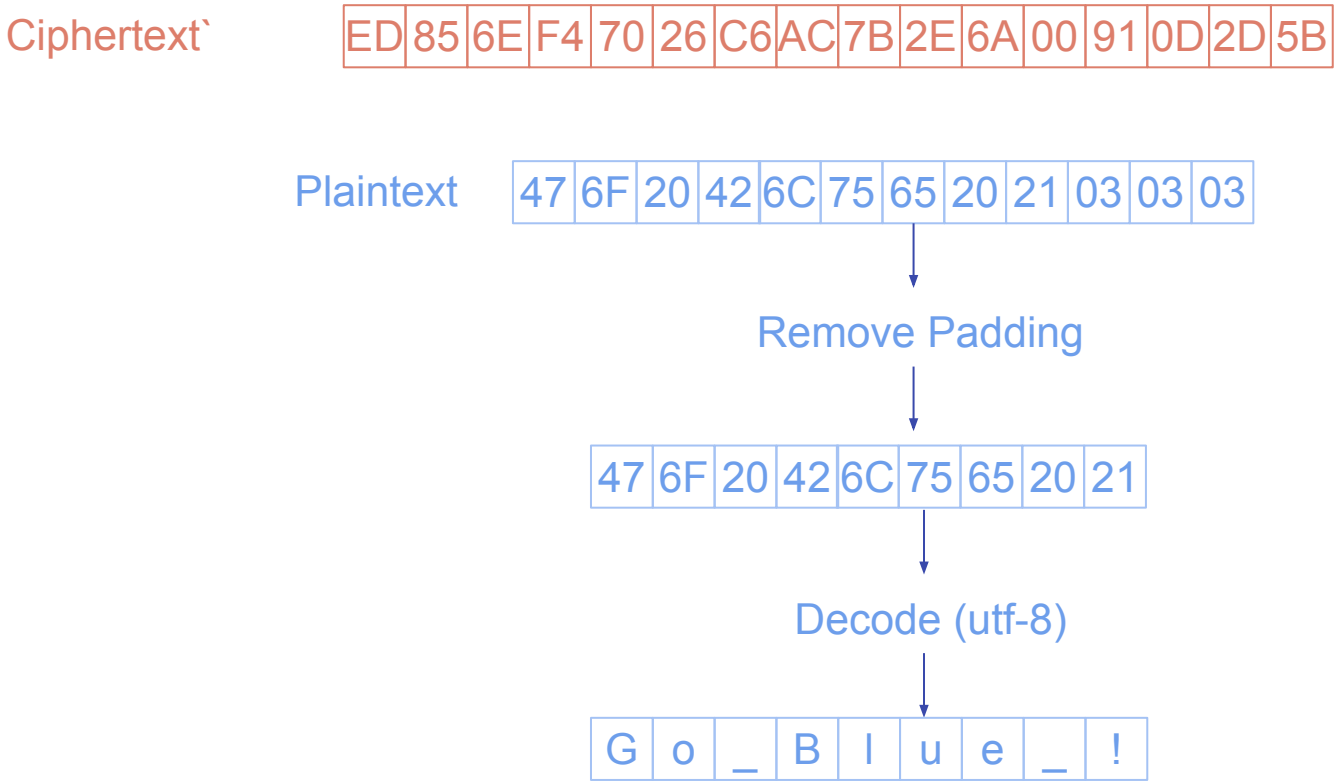


Bob's Decryption (cont.)

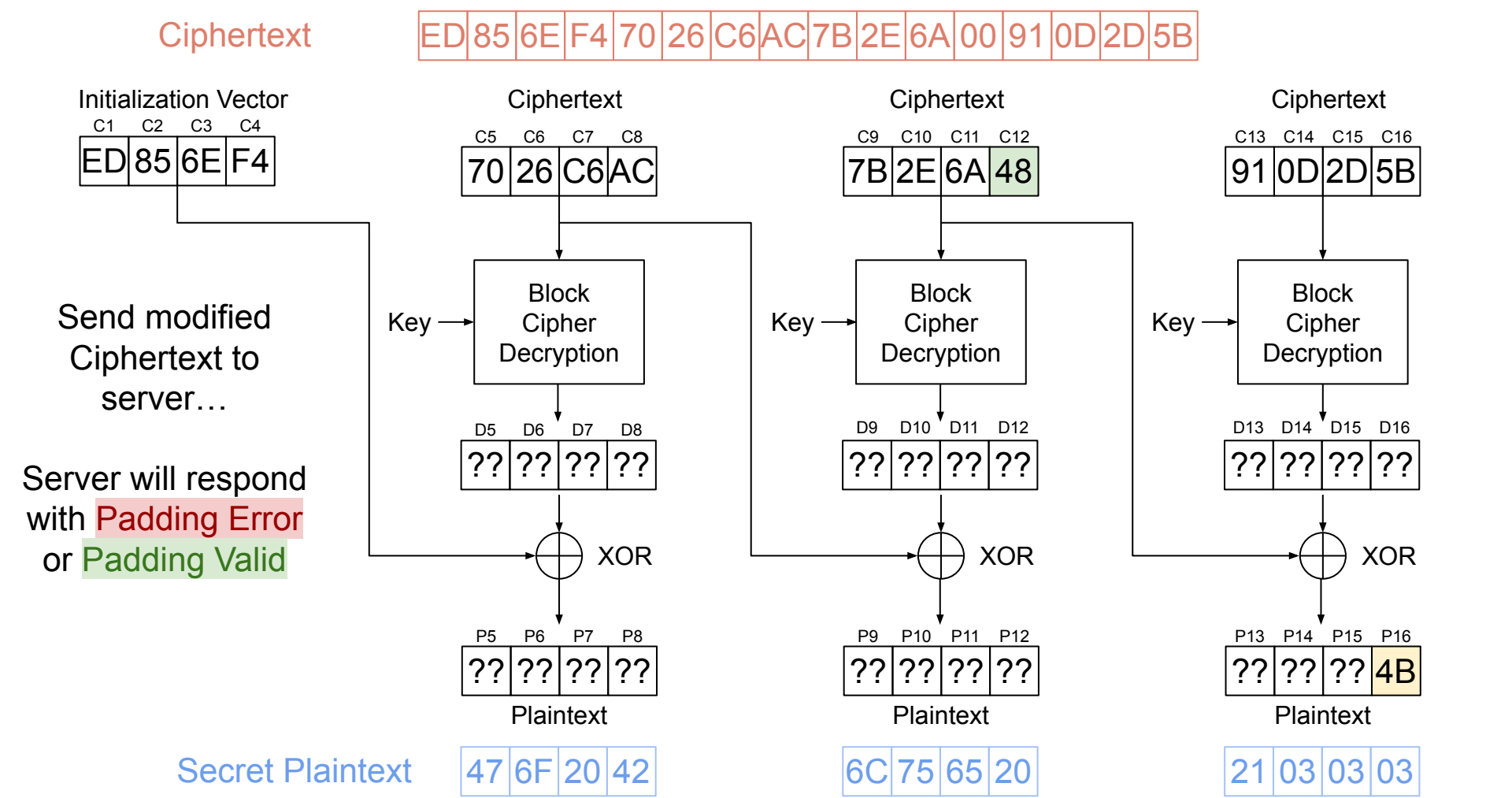


Bob's Decryption (cont.)

Plaintext: 47 6F 20 42 6C 75 65 20 21 03 03 03

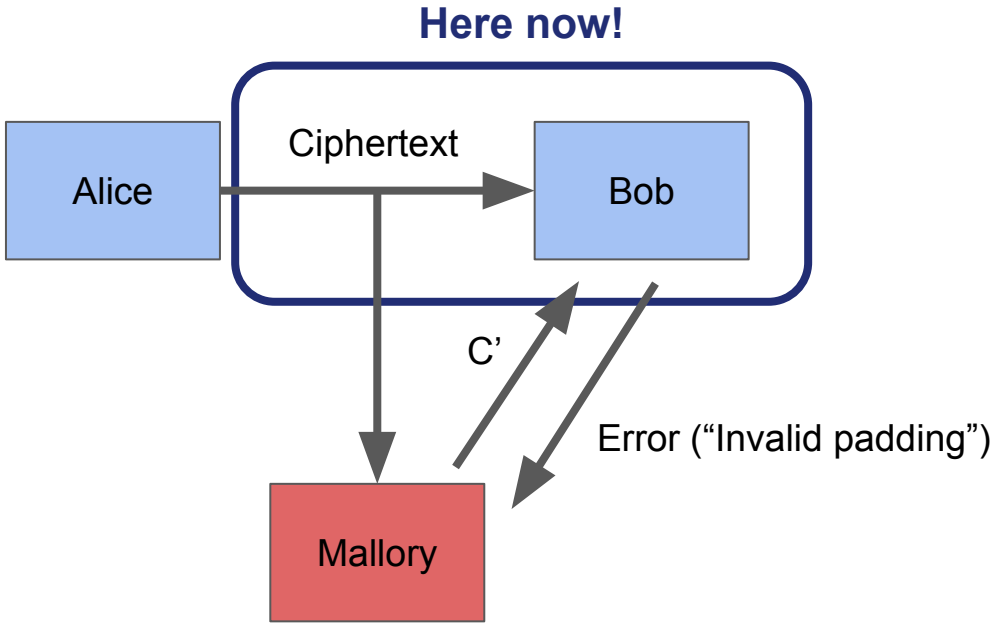


Bob’s Decryption (cont.)


Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 48
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Send modified Ciphertext to server…
Server will respond with Padding Error or Padding Valid
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? ??
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 4B
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

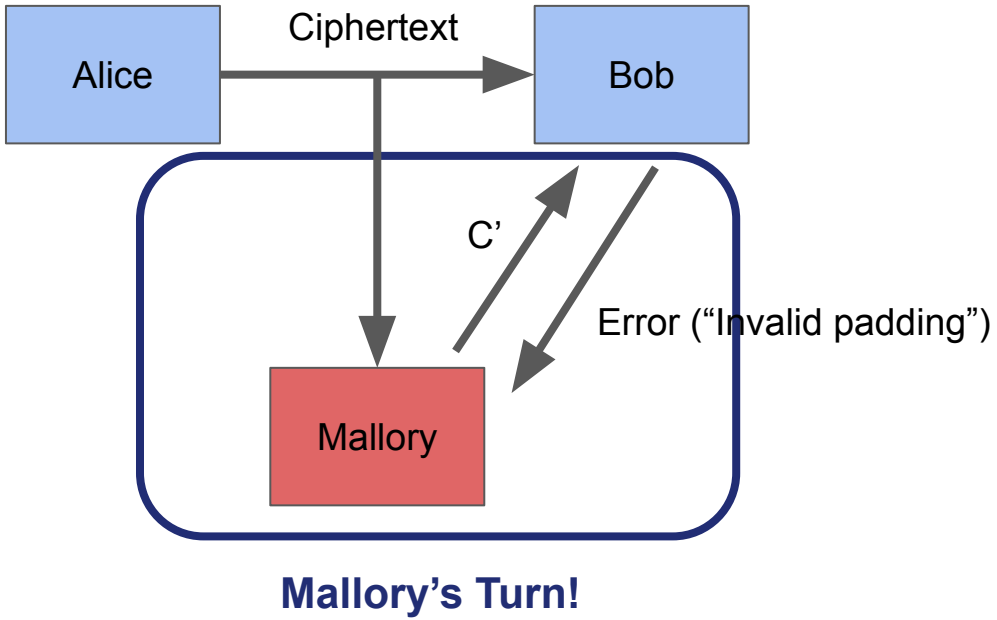
Premise

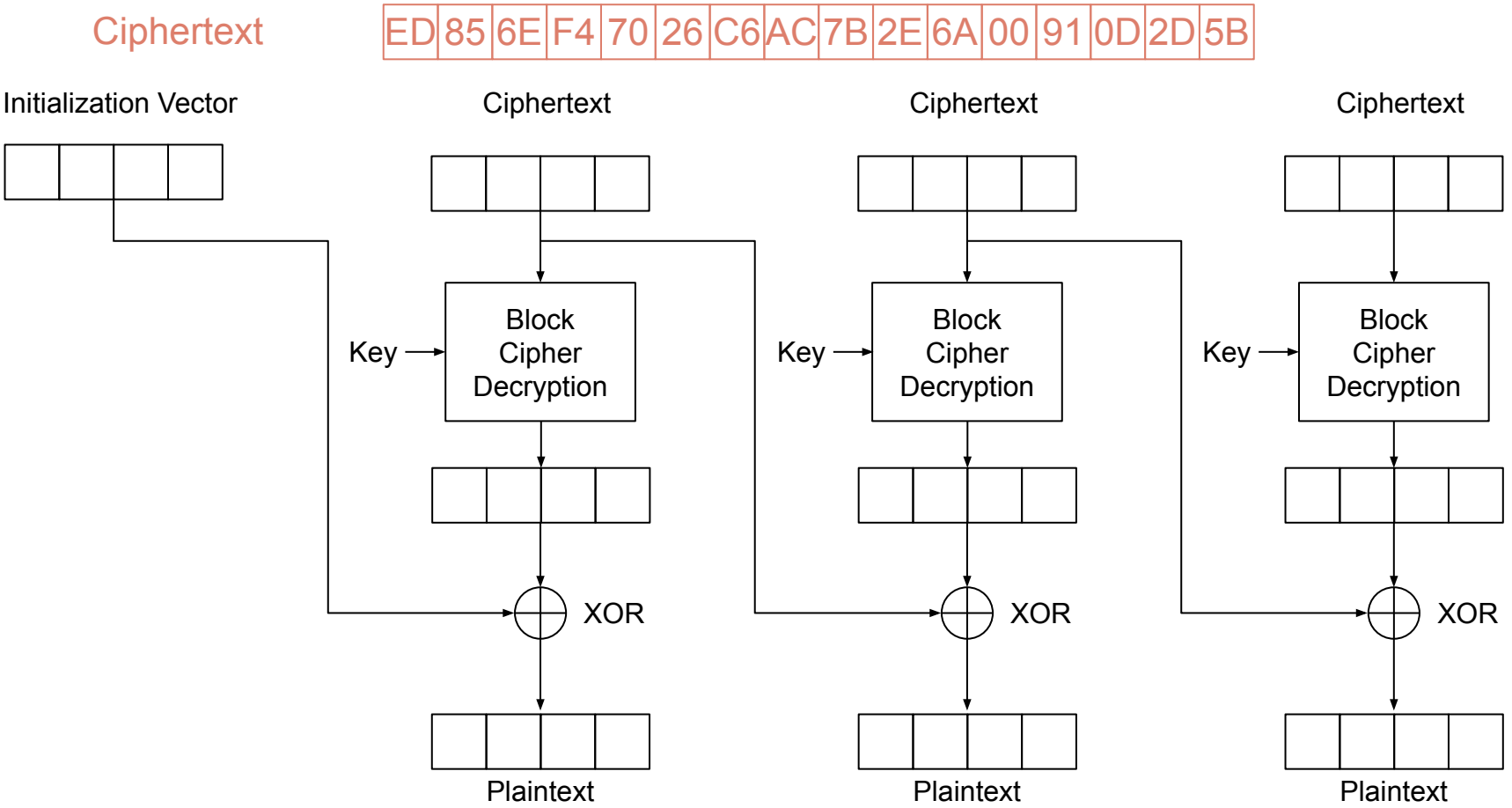
- Mallory initially only knows the ciphertext
- Mallory is able to query Bob to incrementally decrypt the ciphertext



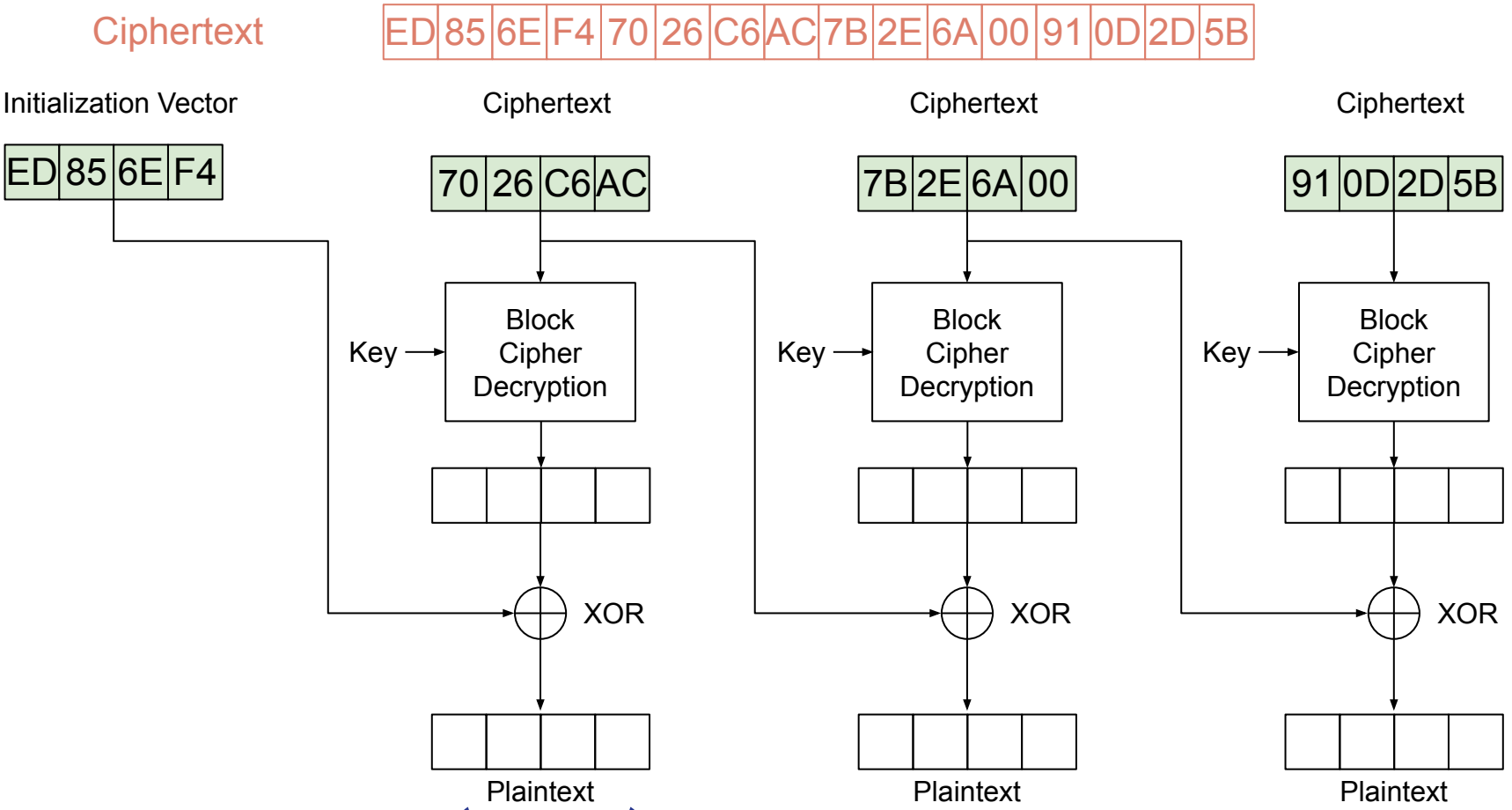
Premise

- Mallory initially only knows the ciphertext
- Mallory is able to query Bob to incrementally decrypt the ciphertext

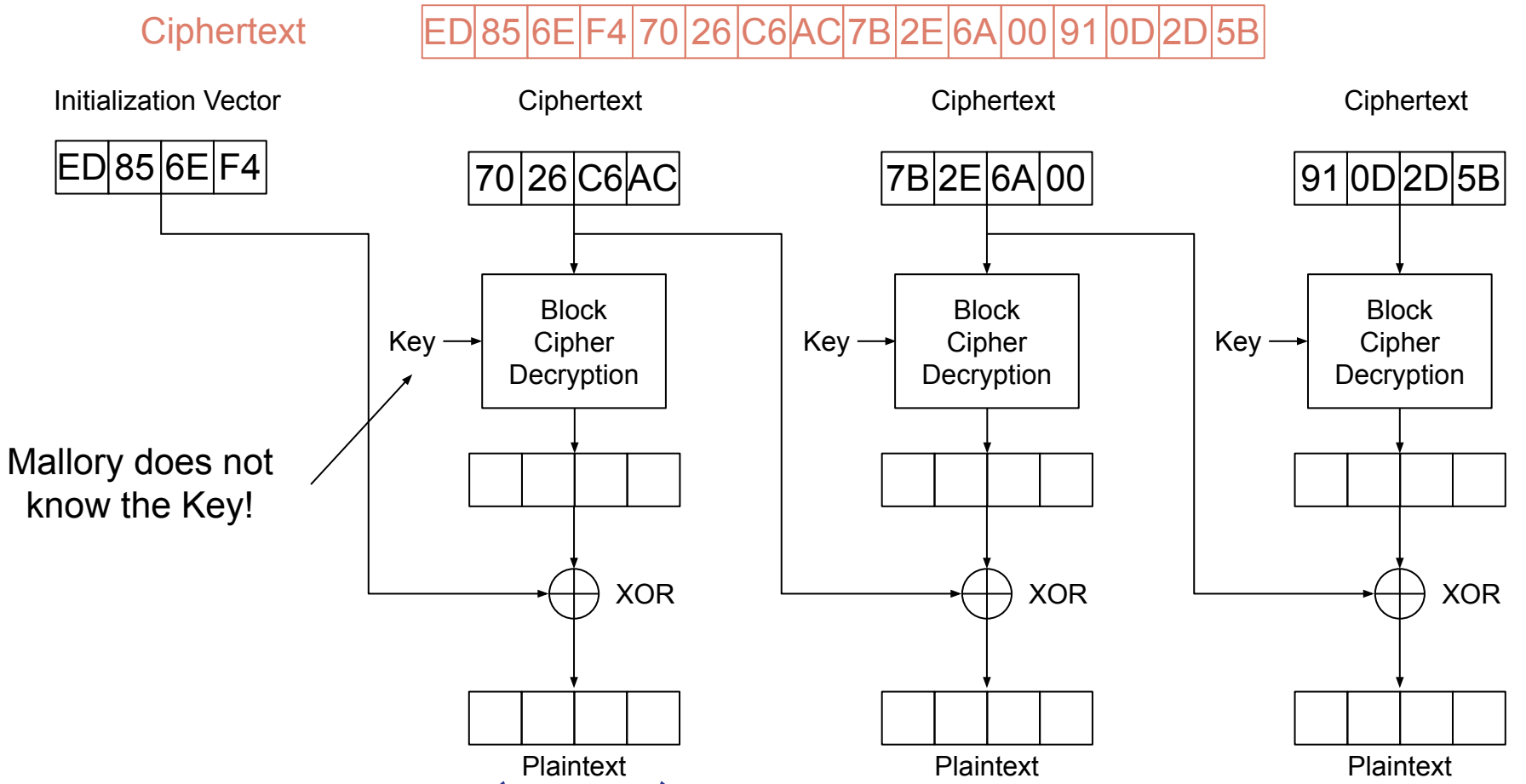




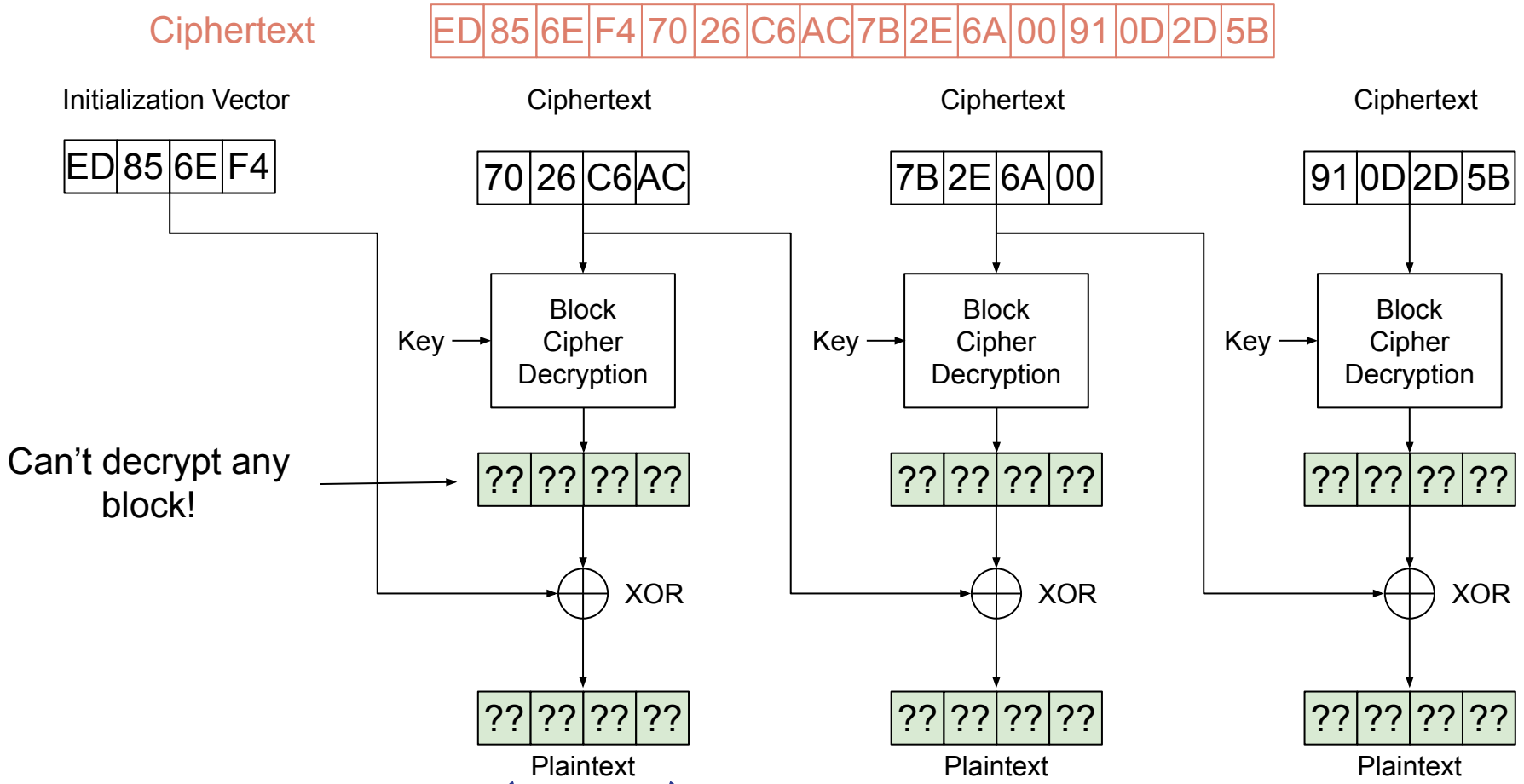
Mallory's Attack



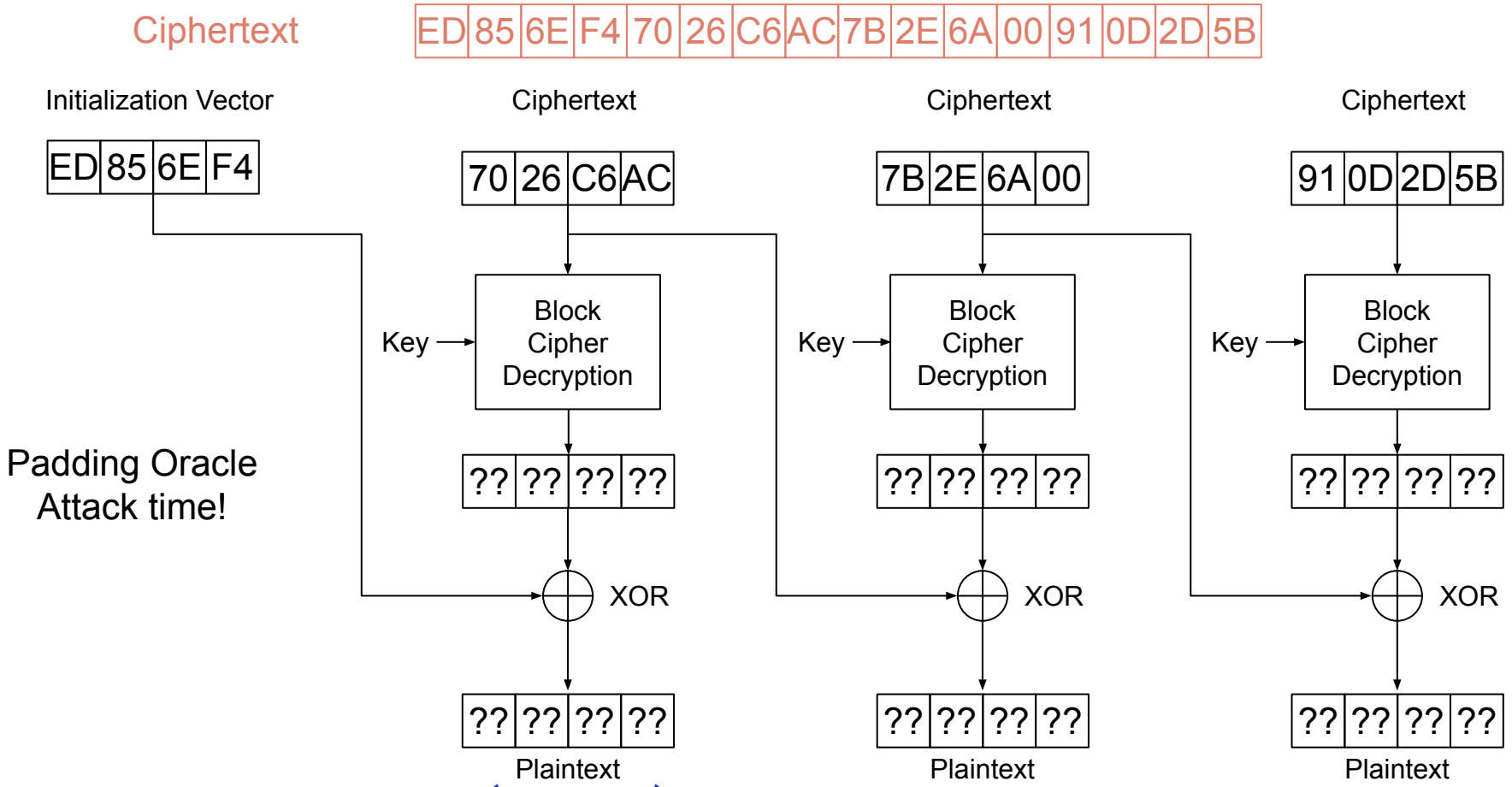
Mallory's Attack (cont.)



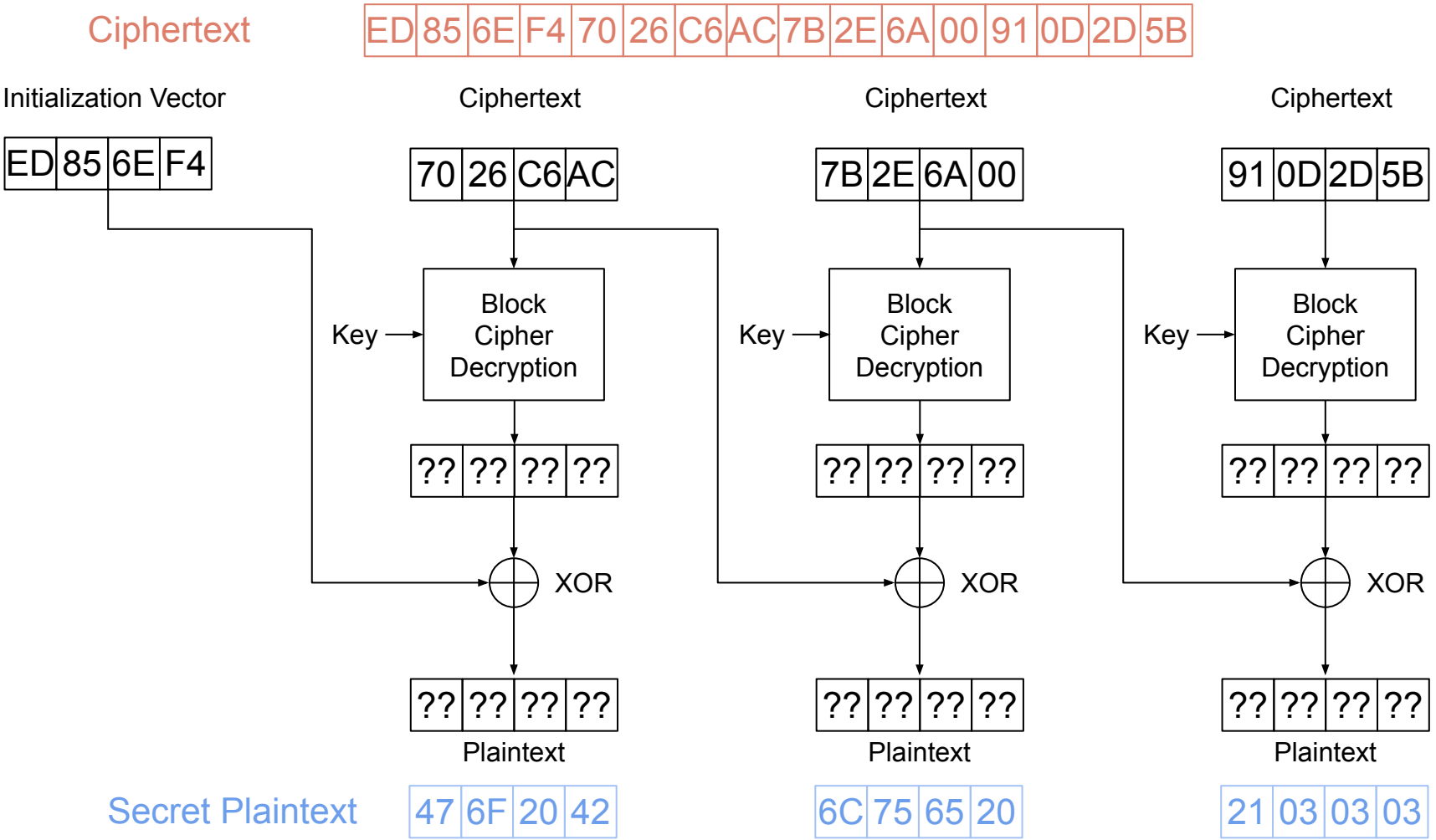
Mallory's Attack (cont.)

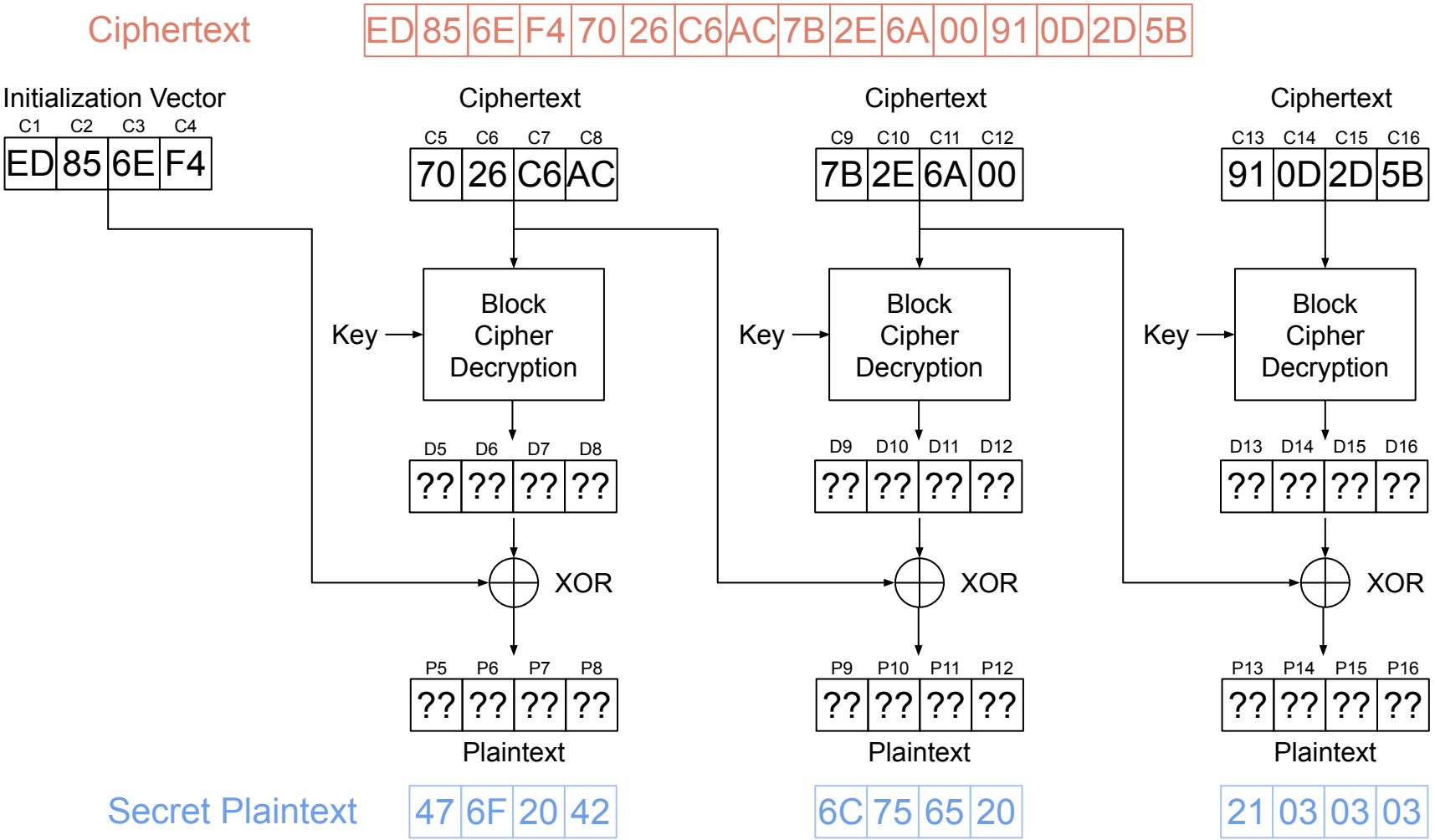


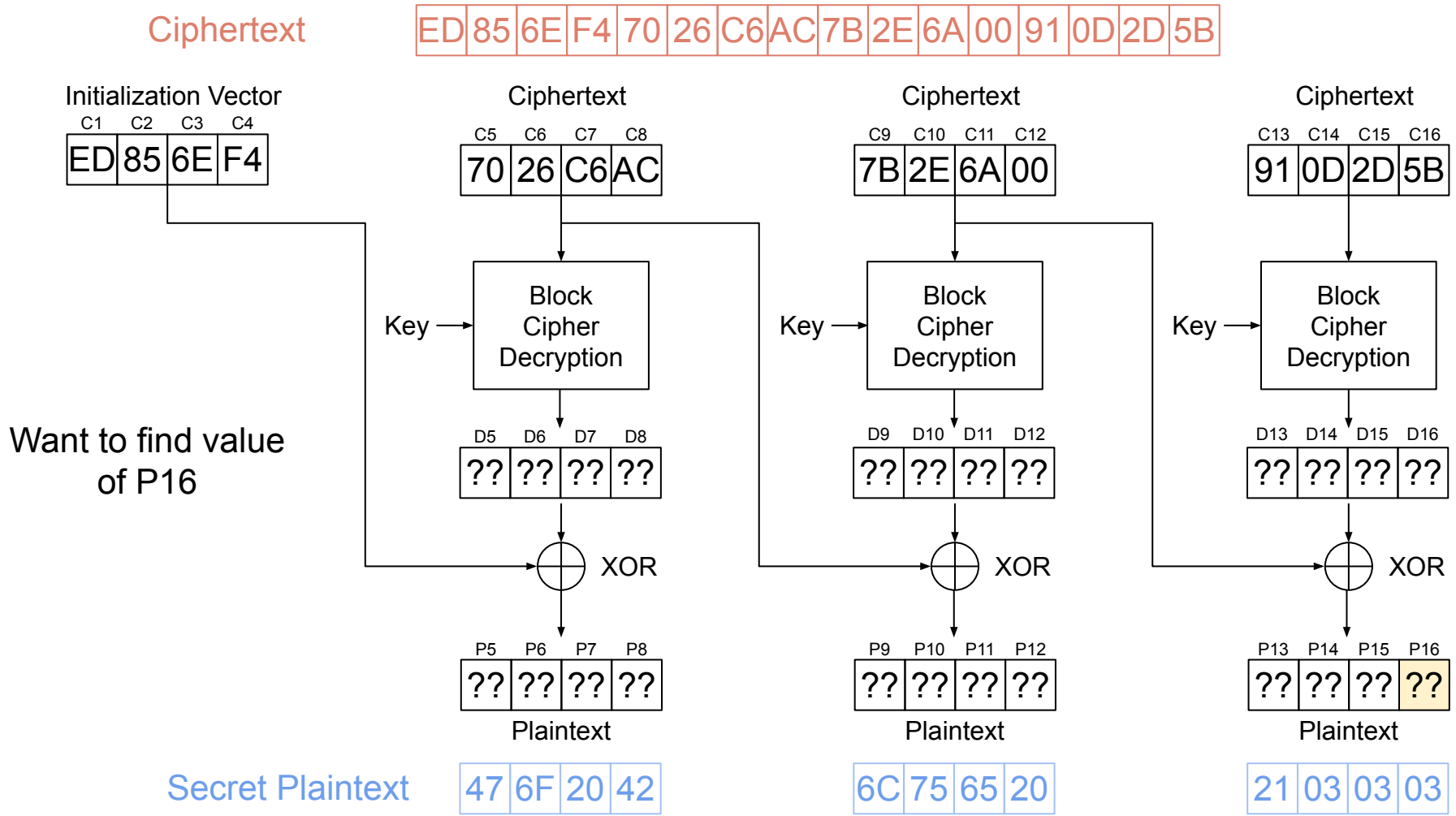
Mallory's Attack (cont.)

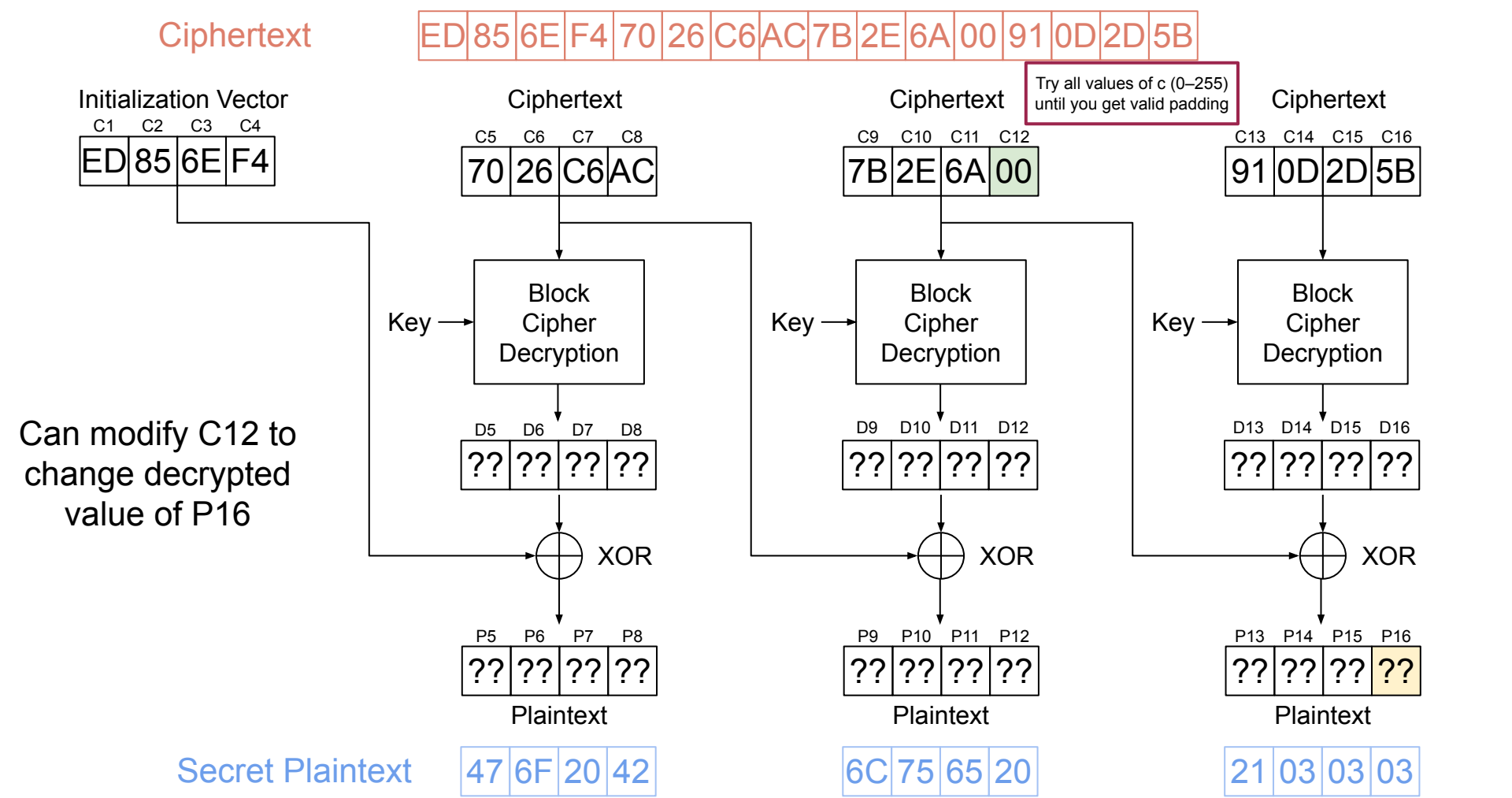


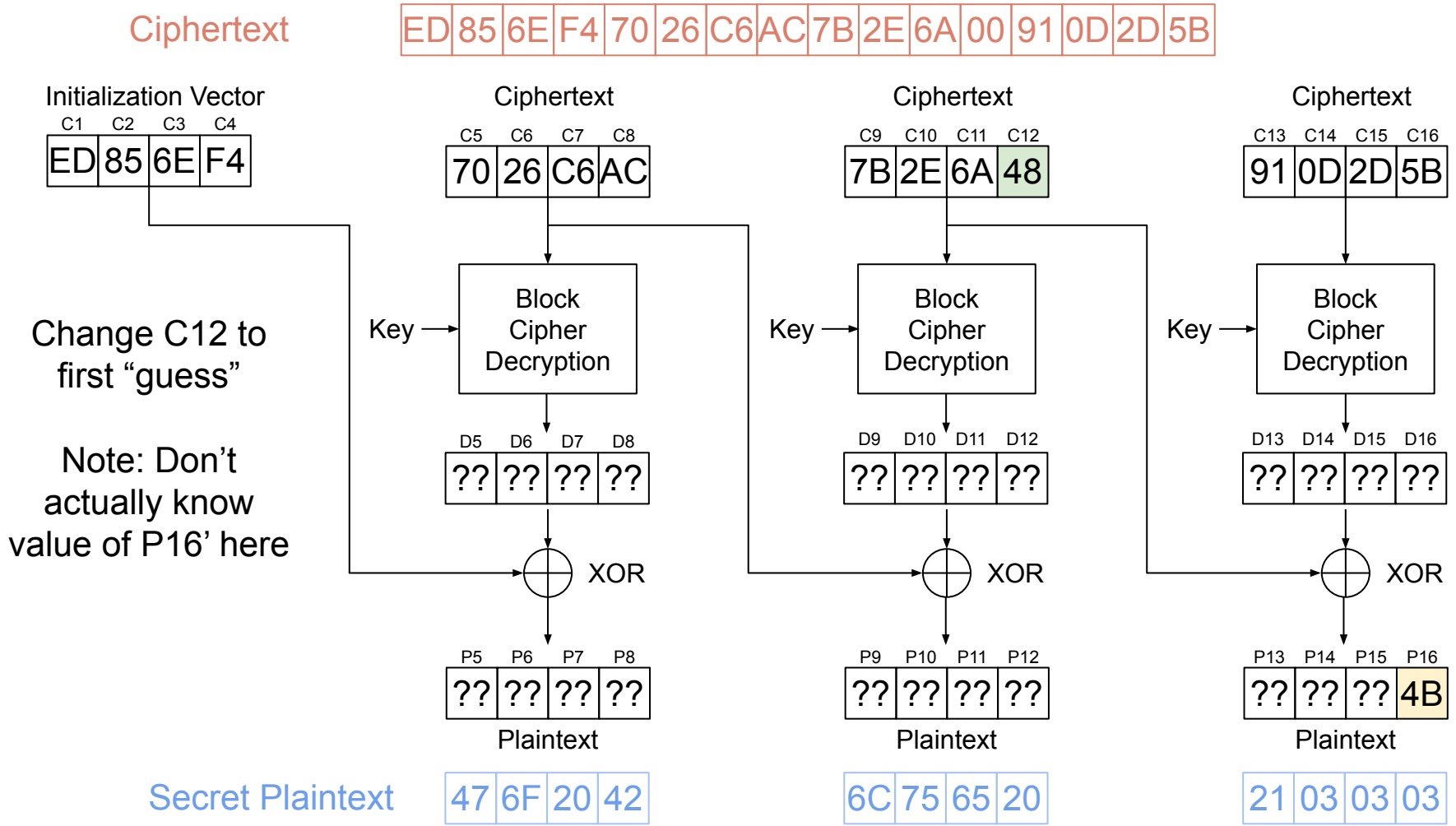
Mallory's Attack (cont.)

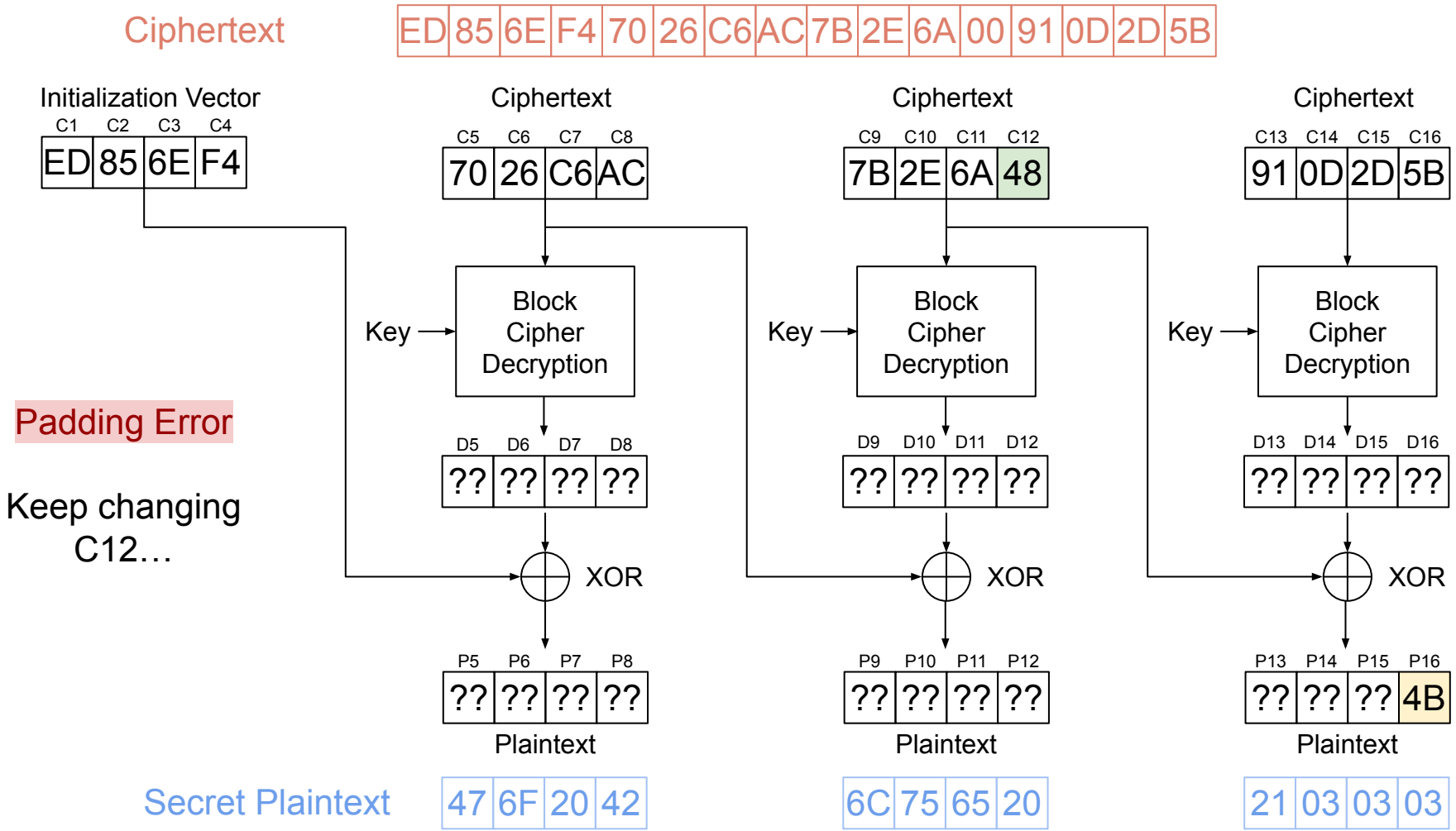

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
ED 85 6E F4
Ciphertext
70 26 C6 AC
Ciphertext
7B 2E 6A 00
Ciphertext
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
?? ?? ?? ??
?? ?? ?? ??
?? ?? ?? ??
XOR
XOR
XOR
?? ?? ?? ??
?? ?? ?? ??
?? ?? ?? ??
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

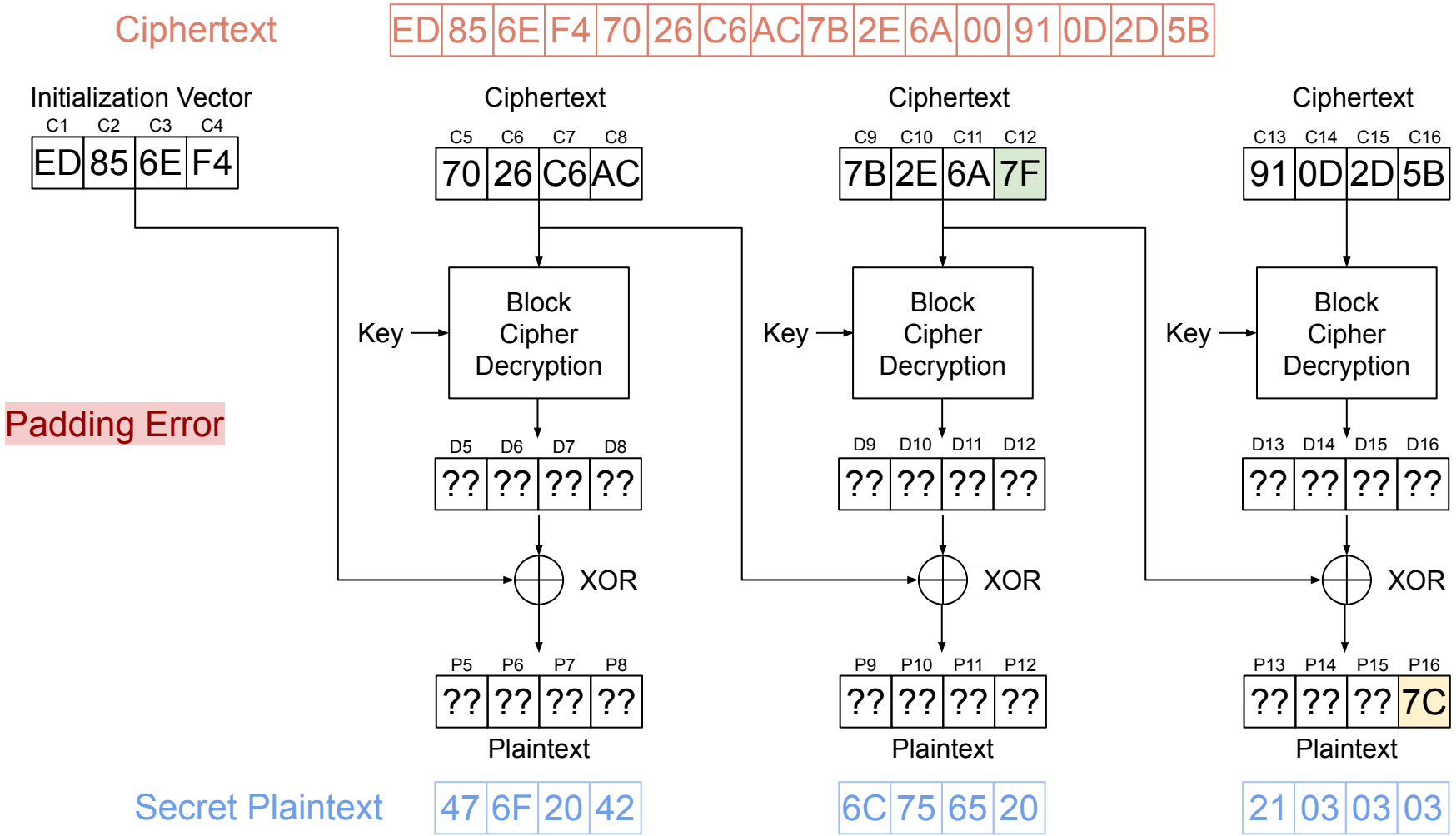

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? ??
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? ??
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

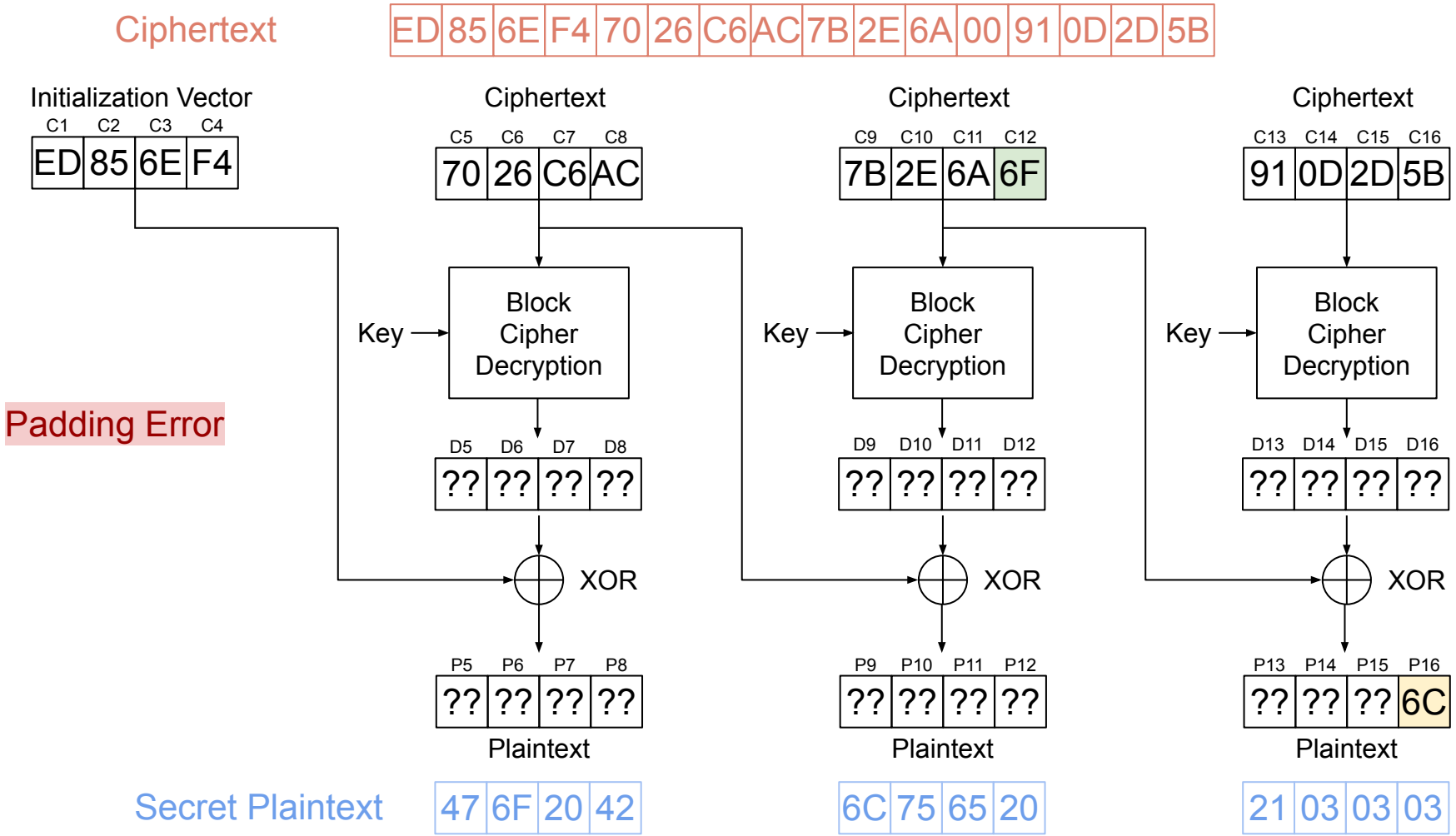

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Want to find value of P16
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? ??
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? ??
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

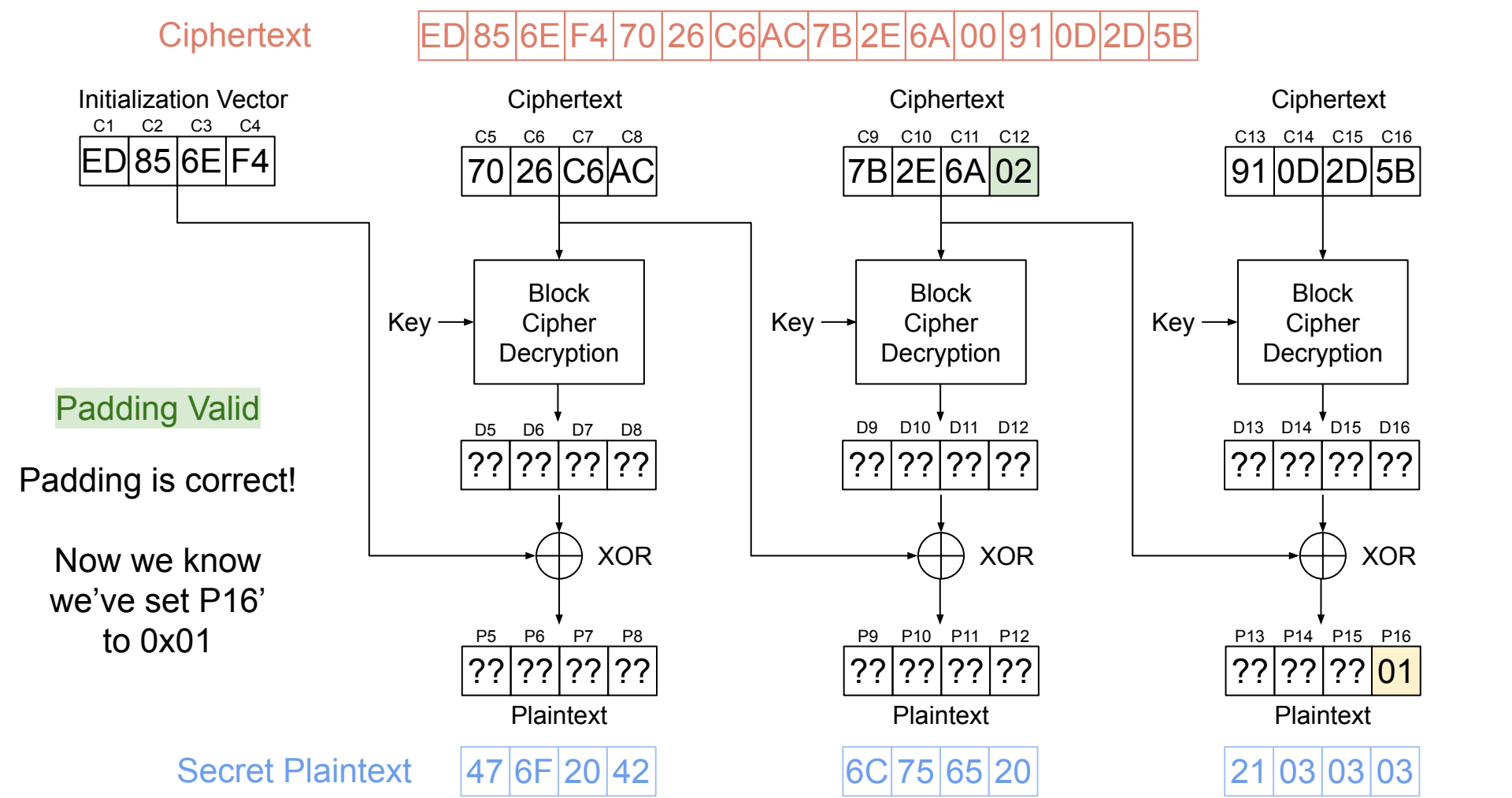

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Try all values of c (0–255) until you get valid padding
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? ??
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? ??
Plaintext
Plaintext
Plaintext
Can modify C12 to change decrypted value of P16
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03


Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 48
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Change C12 to first “guess”
Note: Don’t actually know value of P16’ here
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? ??
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 4B
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03


Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 48
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? ??
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 4B
Plaintext
Plaintext
Plaintext
Padding Error
Keep changing C12…
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03


Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 7F
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Padding Error
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? ??
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 7C
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

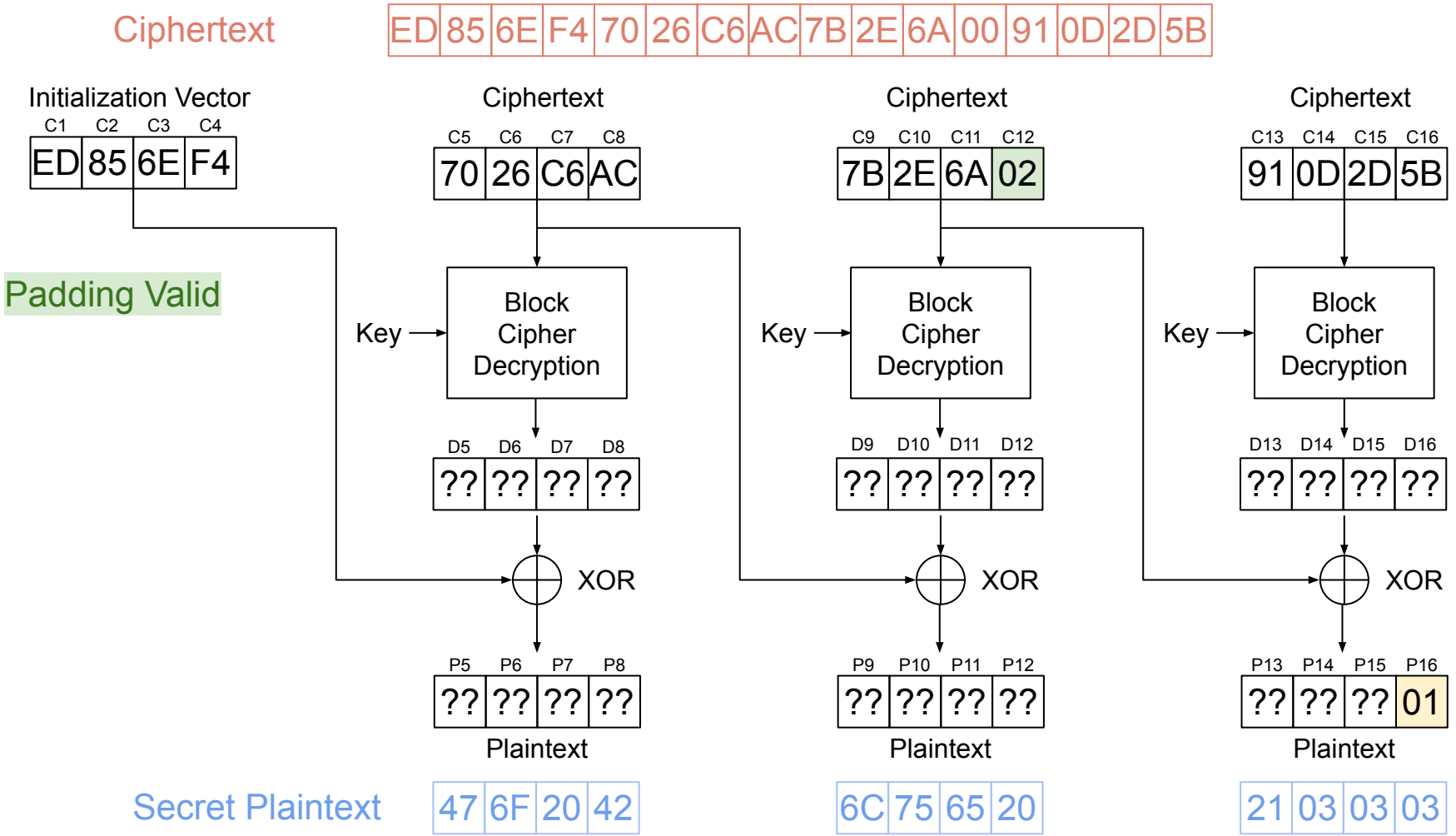

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 6F
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Padding Error
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? ??
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 6C
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

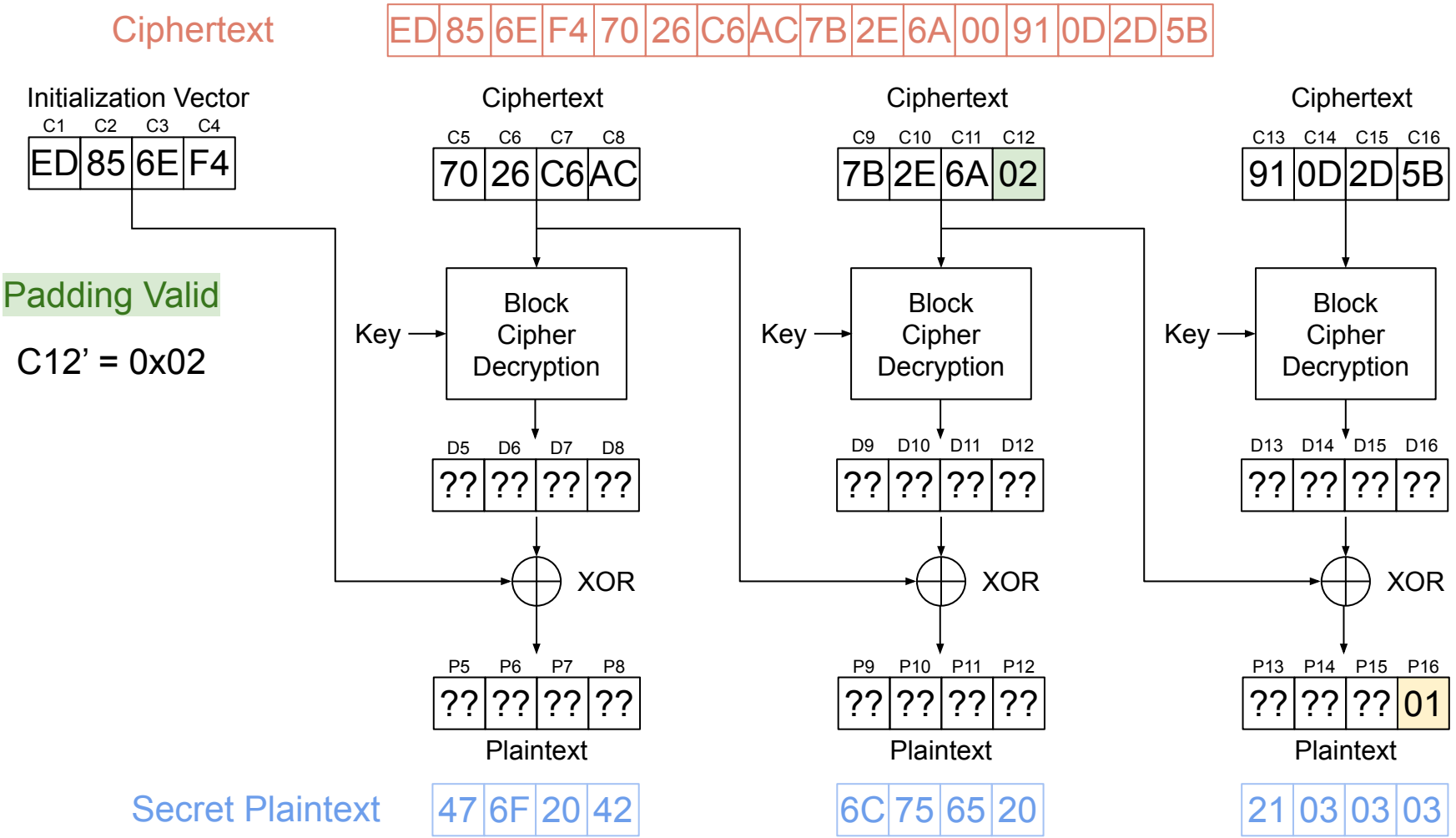


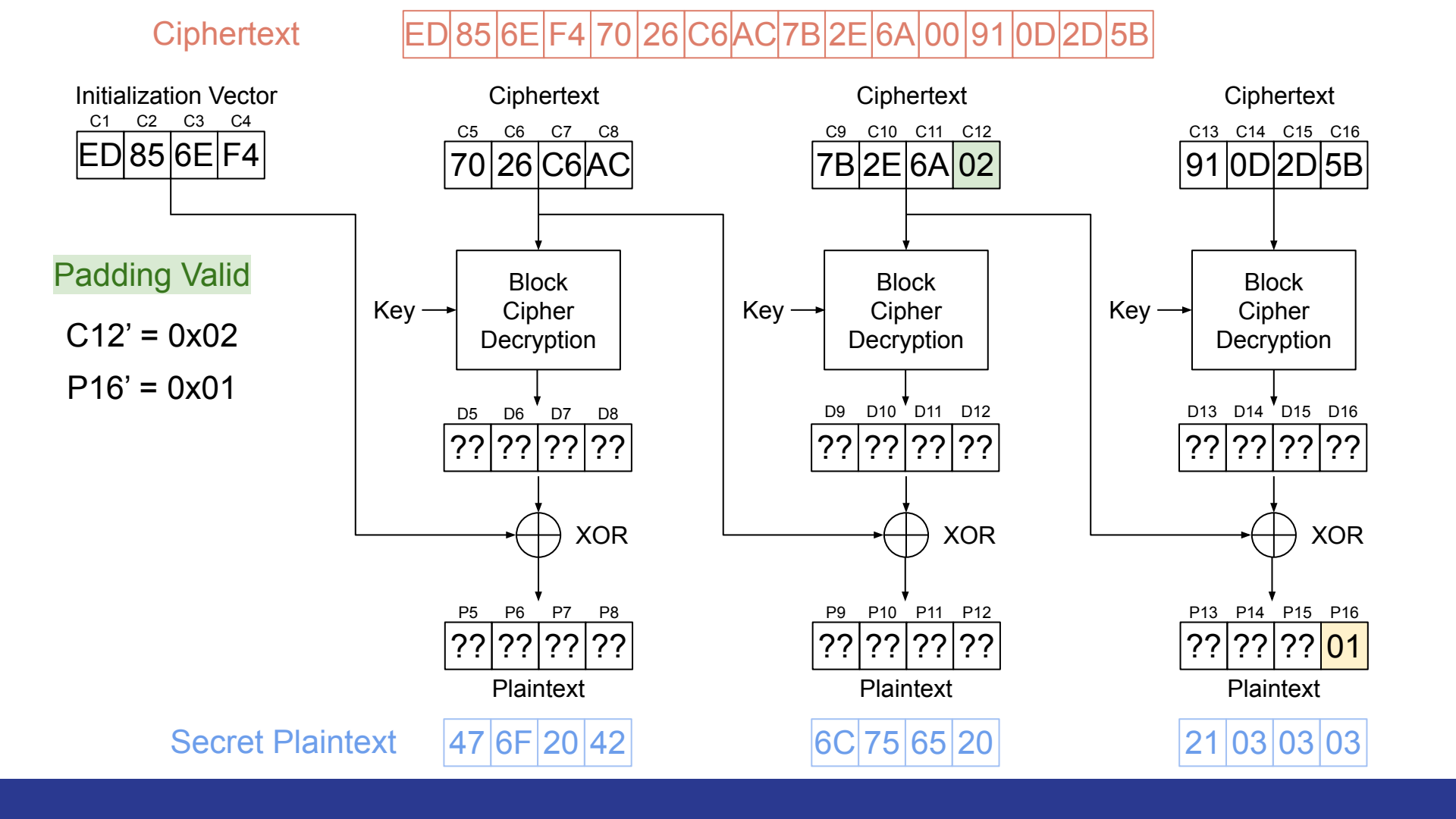
Padding Valid

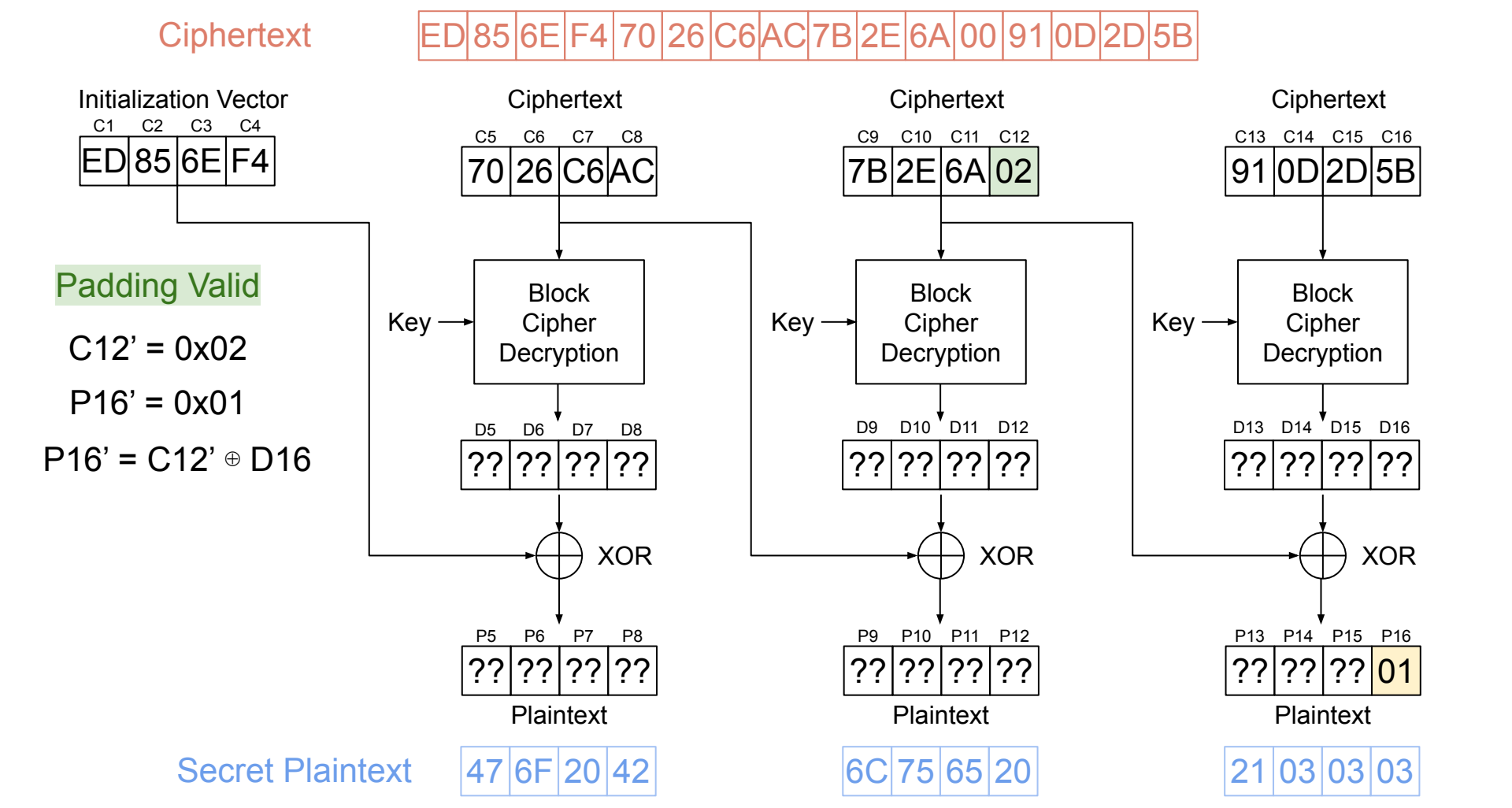
Padding is correct!

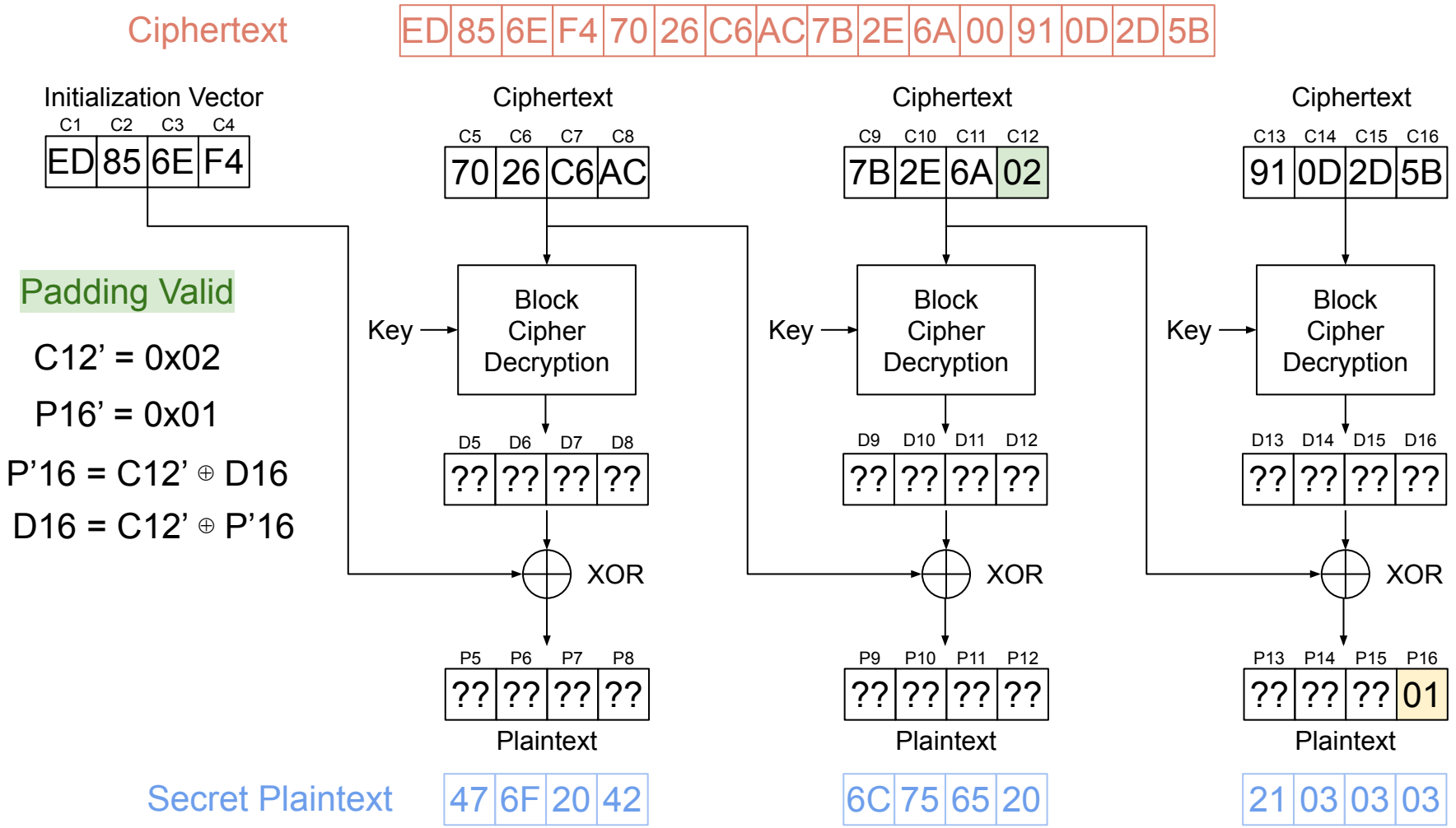
Now we know we've set P16' to 0x01

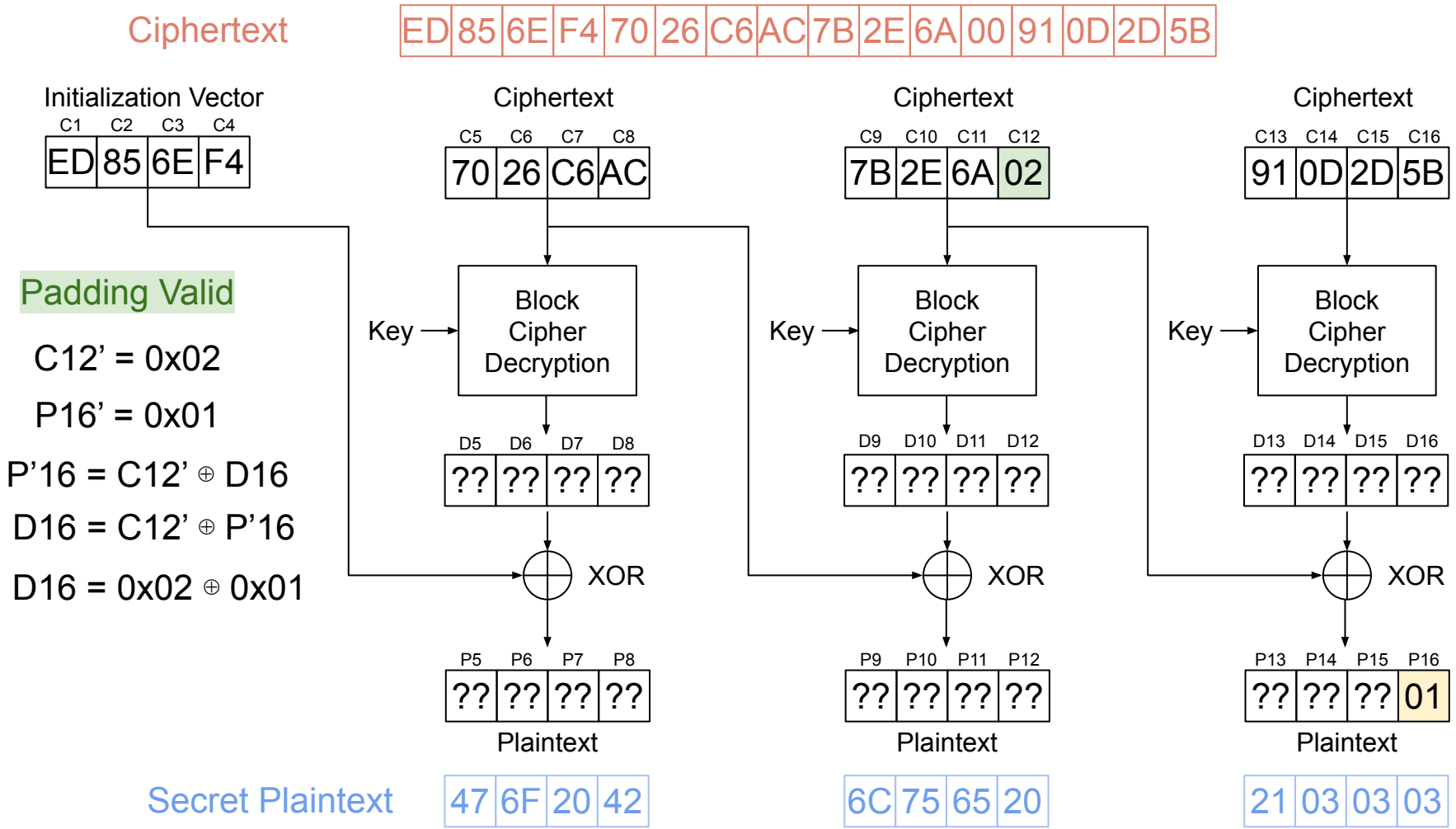

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Padding Valid
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 02
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? ??
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
Plaintext
P9 P10 P11 P12
?? ?? ?? ??
Plaintext
P13 P14 P15 P16
?? ?? ?? 01
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

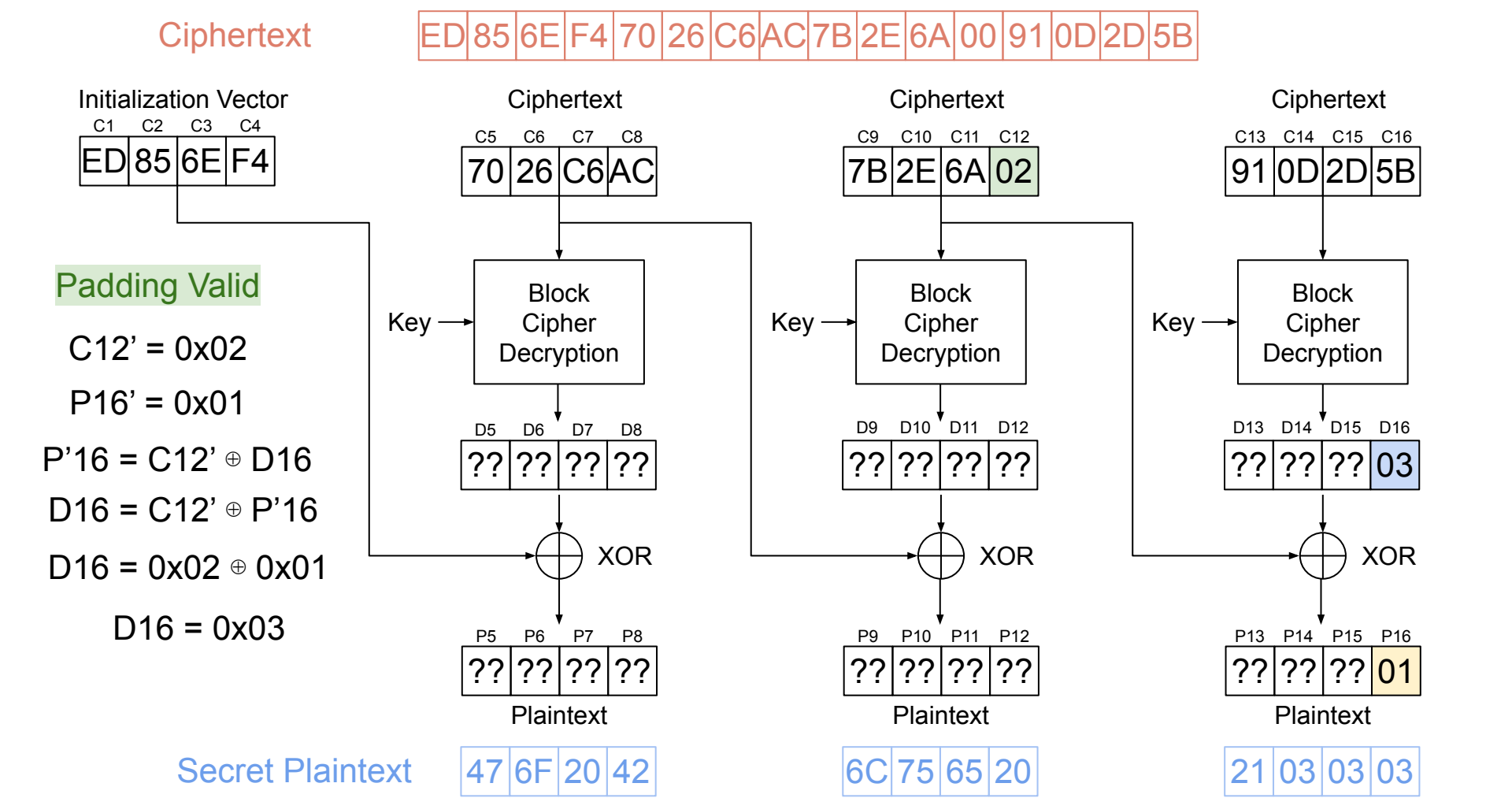

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Padding Valid
C12' = 0x02
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 02
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? ??
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 01
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

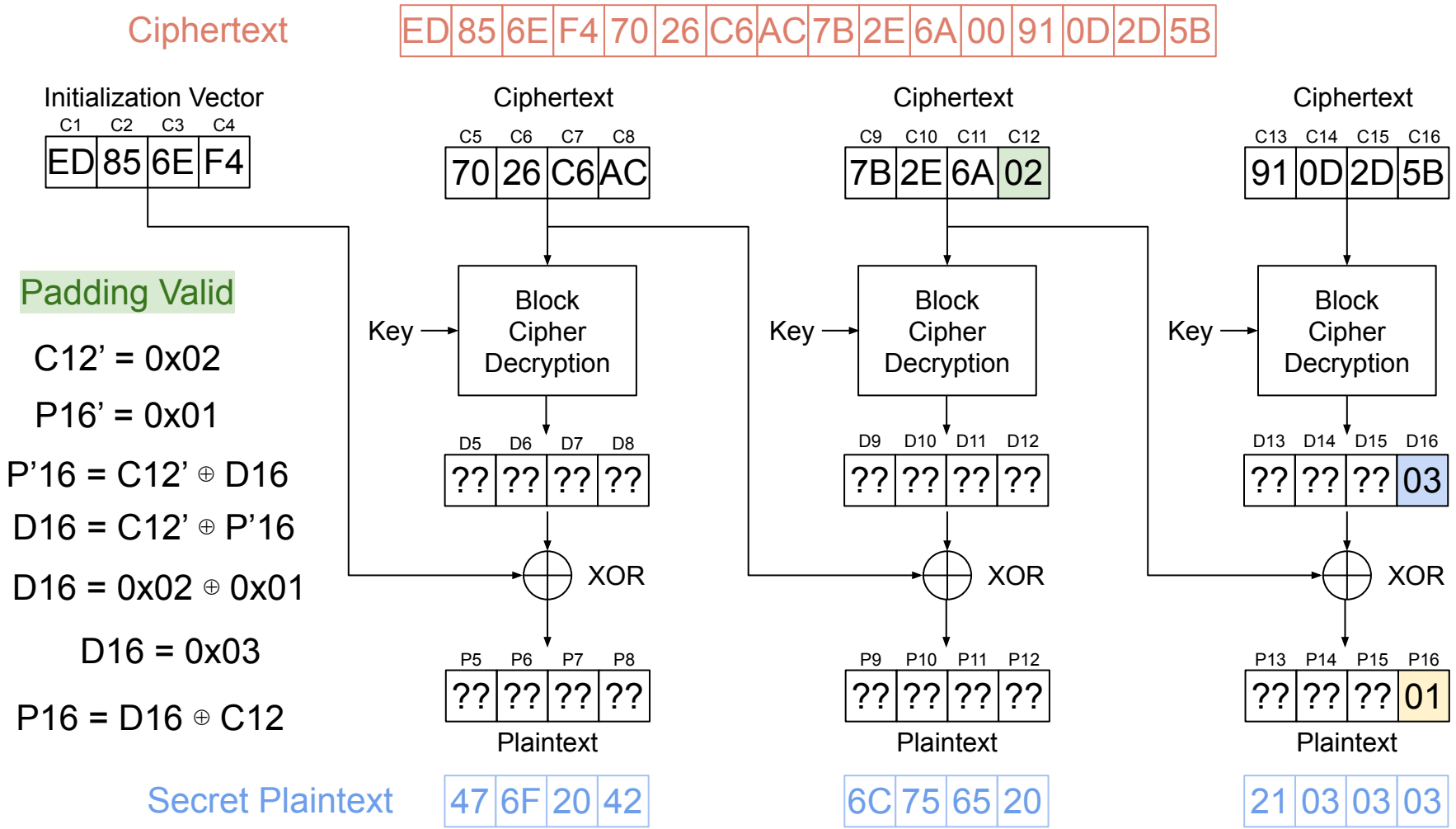

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 02
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Padding Valid
C12' = 0x02
P16' = 0x01
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? ??
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 01
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

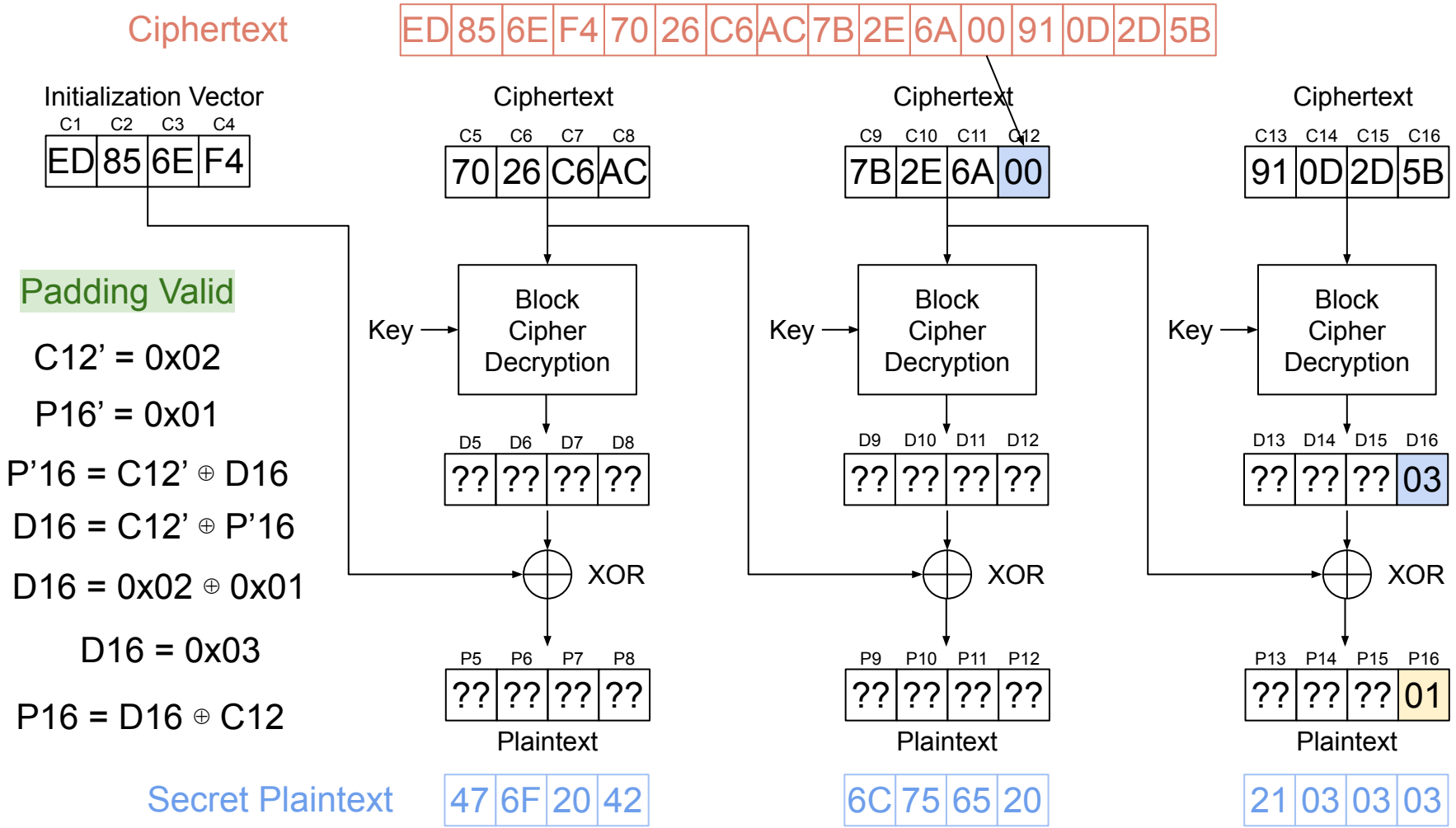

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 02
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Padding Valid
C12' = 0x02
P16' = 0x01
P16' = C12' ⊕ D16
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? ??
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 01
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

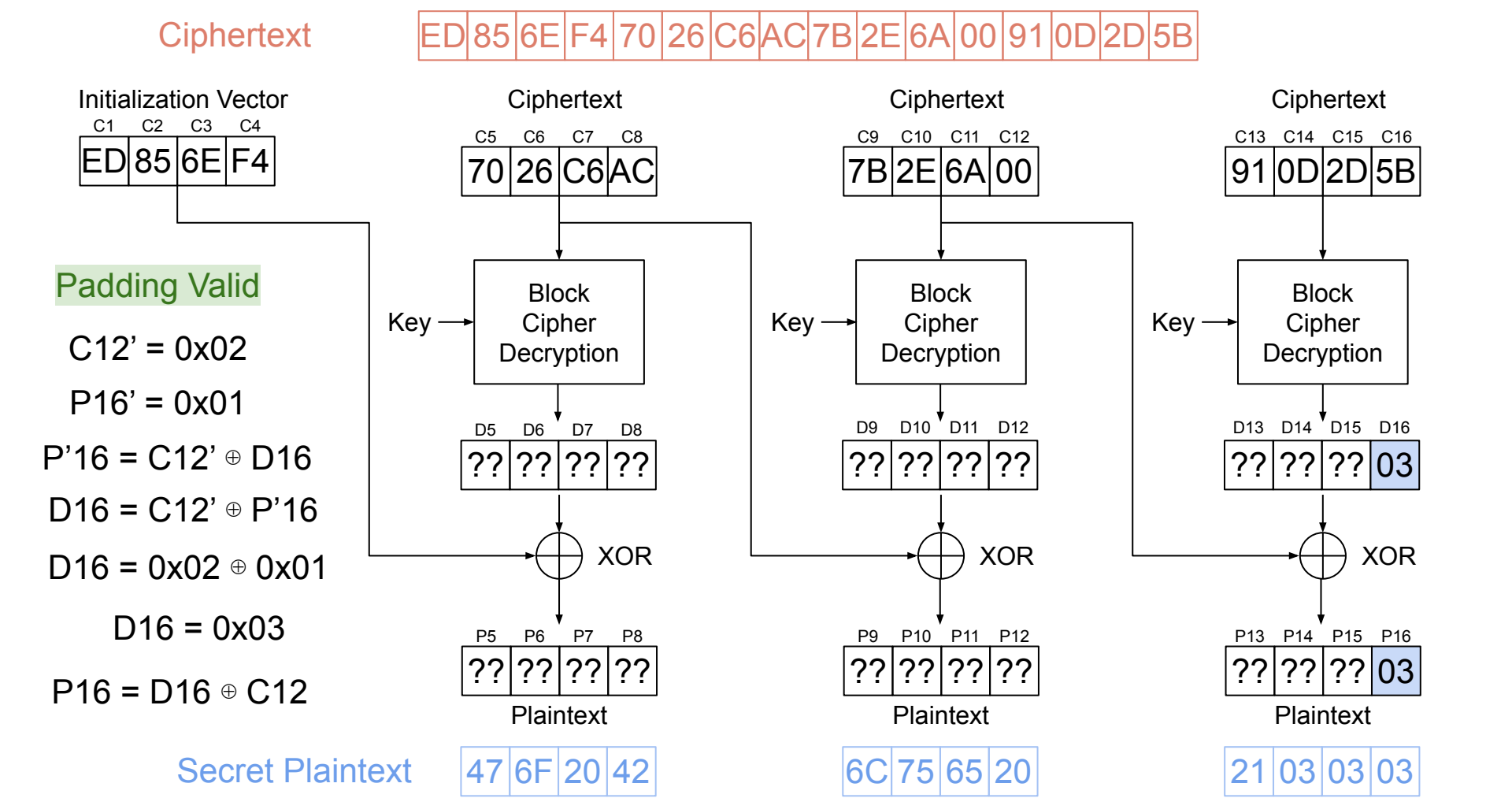

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 02
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Padding Valid
C12' = 0x02
P16' = 0x01
P'16 = C12' ⊕ D16
D16 = C12' ⊕ P'16
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? ??
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 01
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

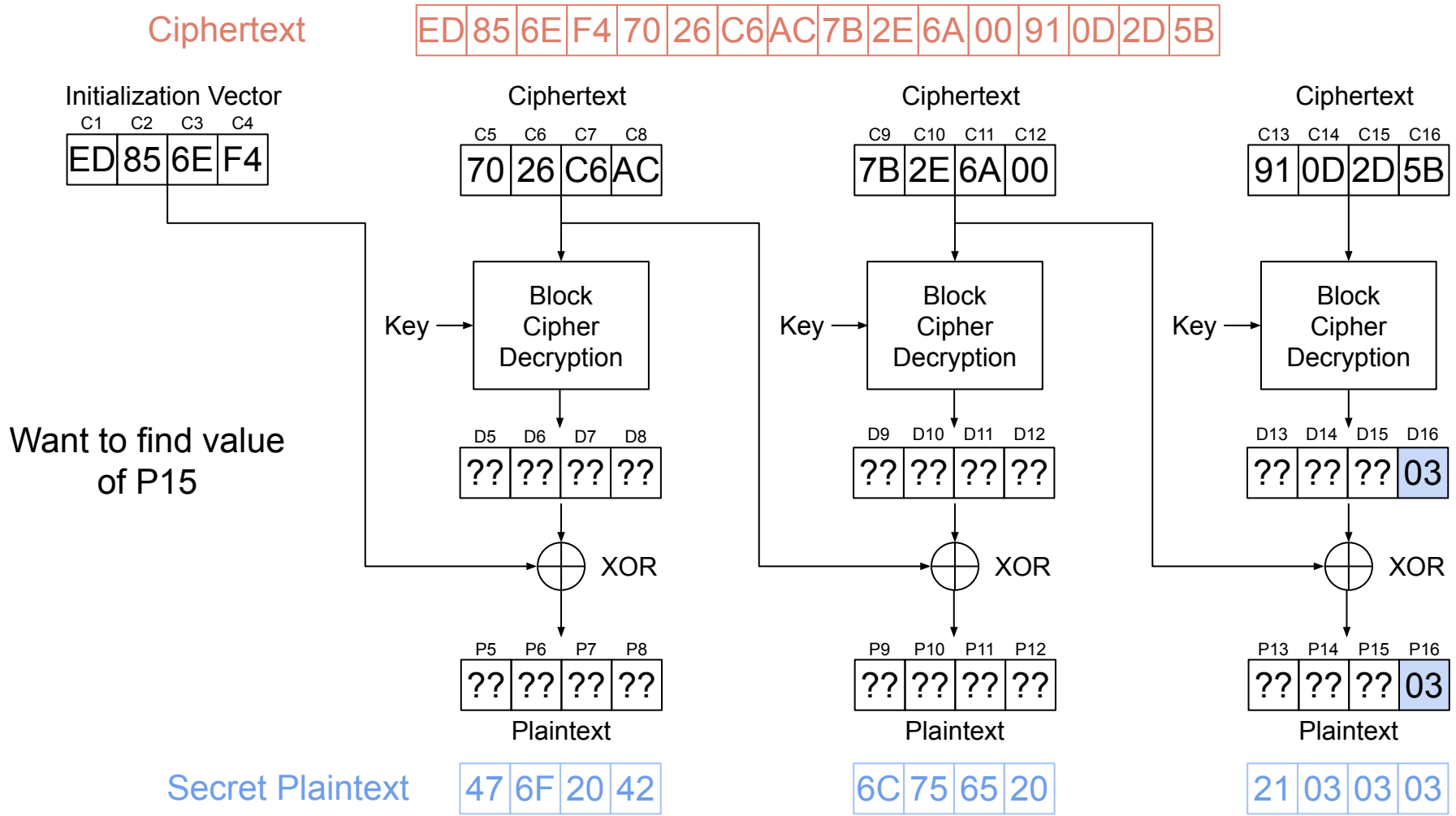

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 02
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Padding Valid
C12' = 0x02
P16' = 0x01
P'16 = C12' ⊕ D16
D16 = C12' ⊕ P'16
D16 = 0x02 ⊕ 0x01
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? ??
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 01
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

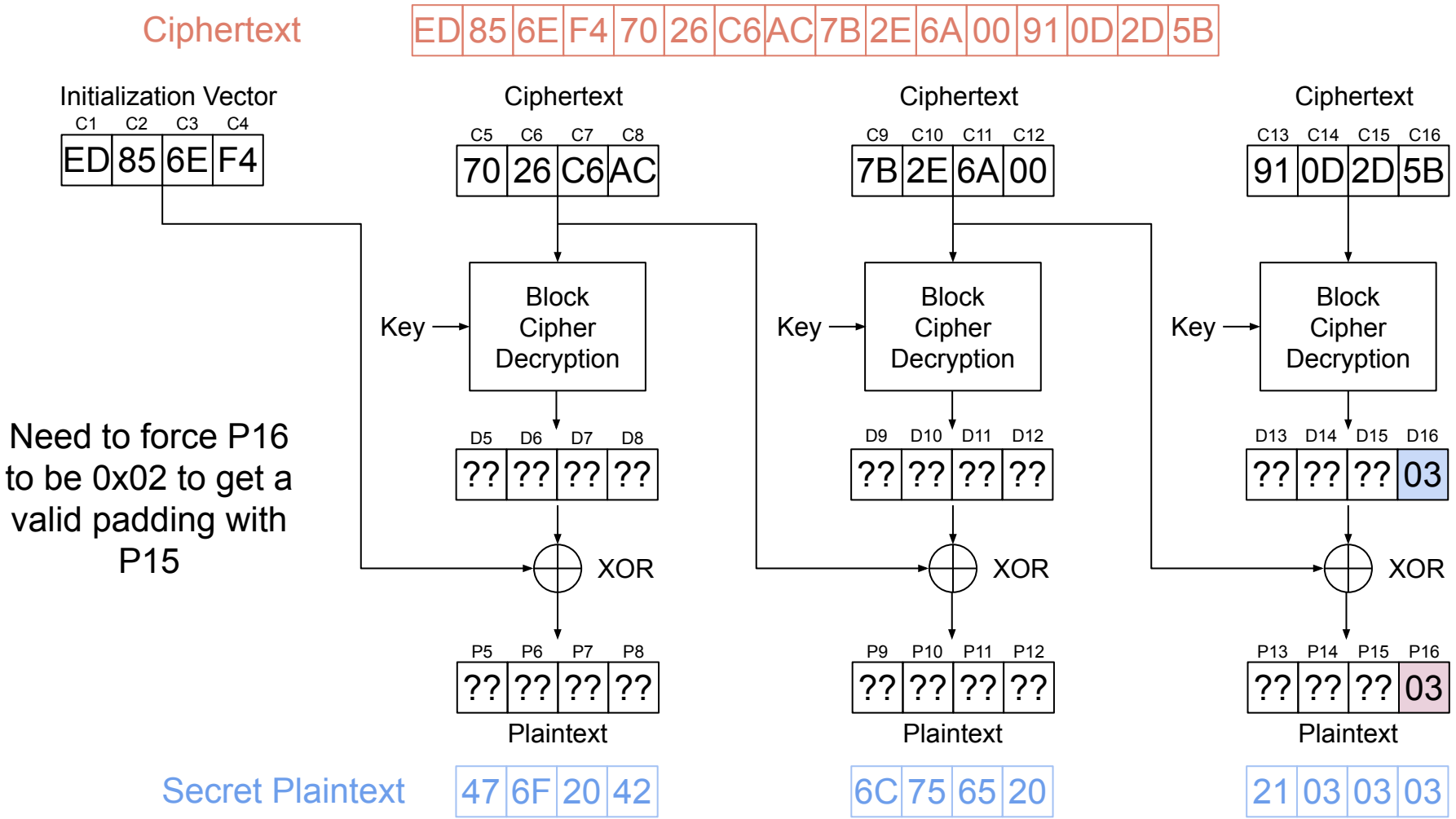

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 02
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Padding Valid
C12' = 0x02
P16' = 0x01
P'16 = C12' ⊕ D16
D16 = C12' ⊕ P'16
D16 = 0x02 ⊕ 0x01
D16 = 0x03
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 01
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

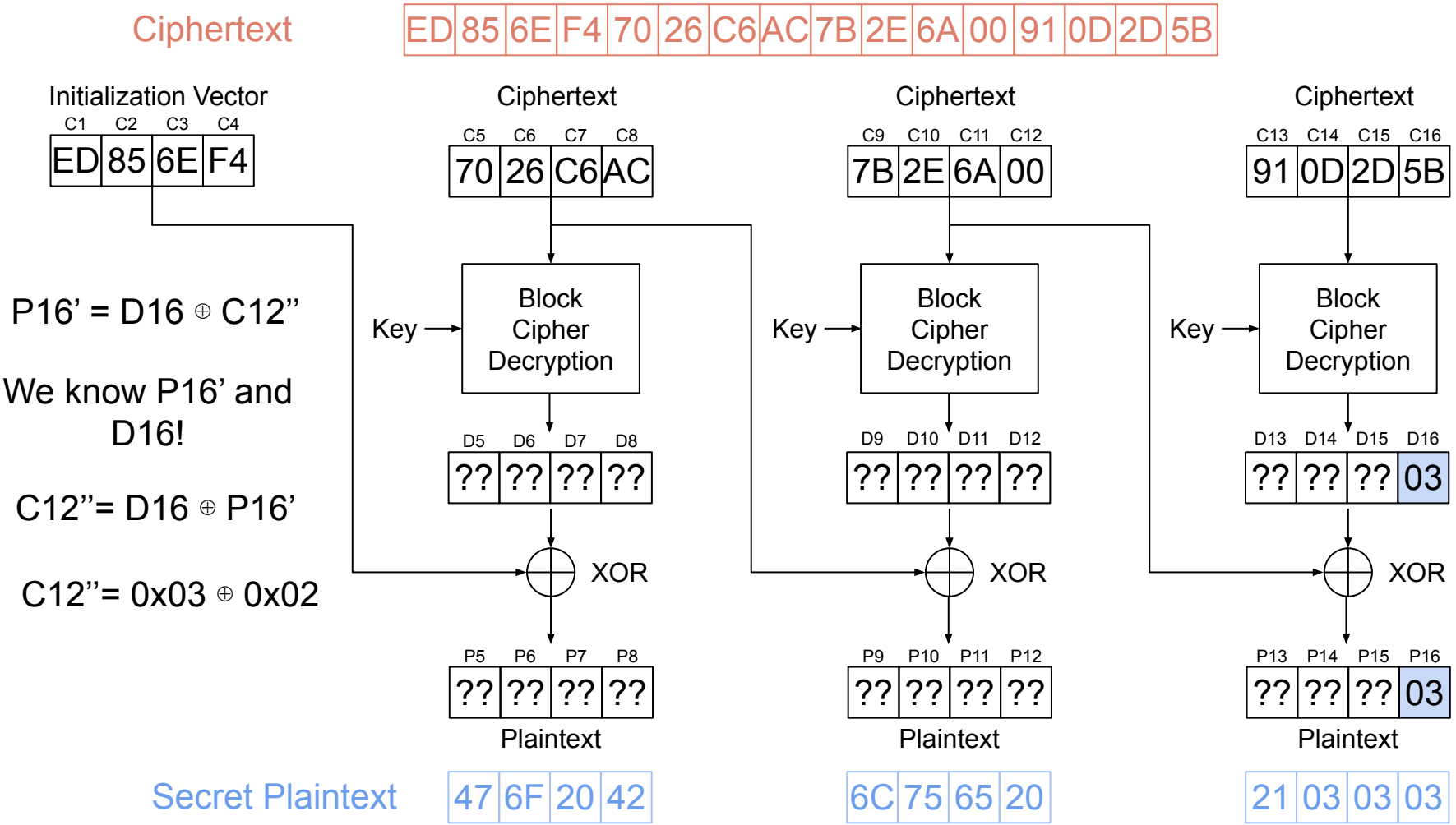

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 02
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Padding Valid
C12' = 0x02
P16' = 0x01
P'16 = C12' ⊕ D16
D16 = C12' ⊕ P'16
D16 = 0x02 ⊕ 0x01
D16 = 0x03
P16 = D16 ⊕ C12
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 01
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

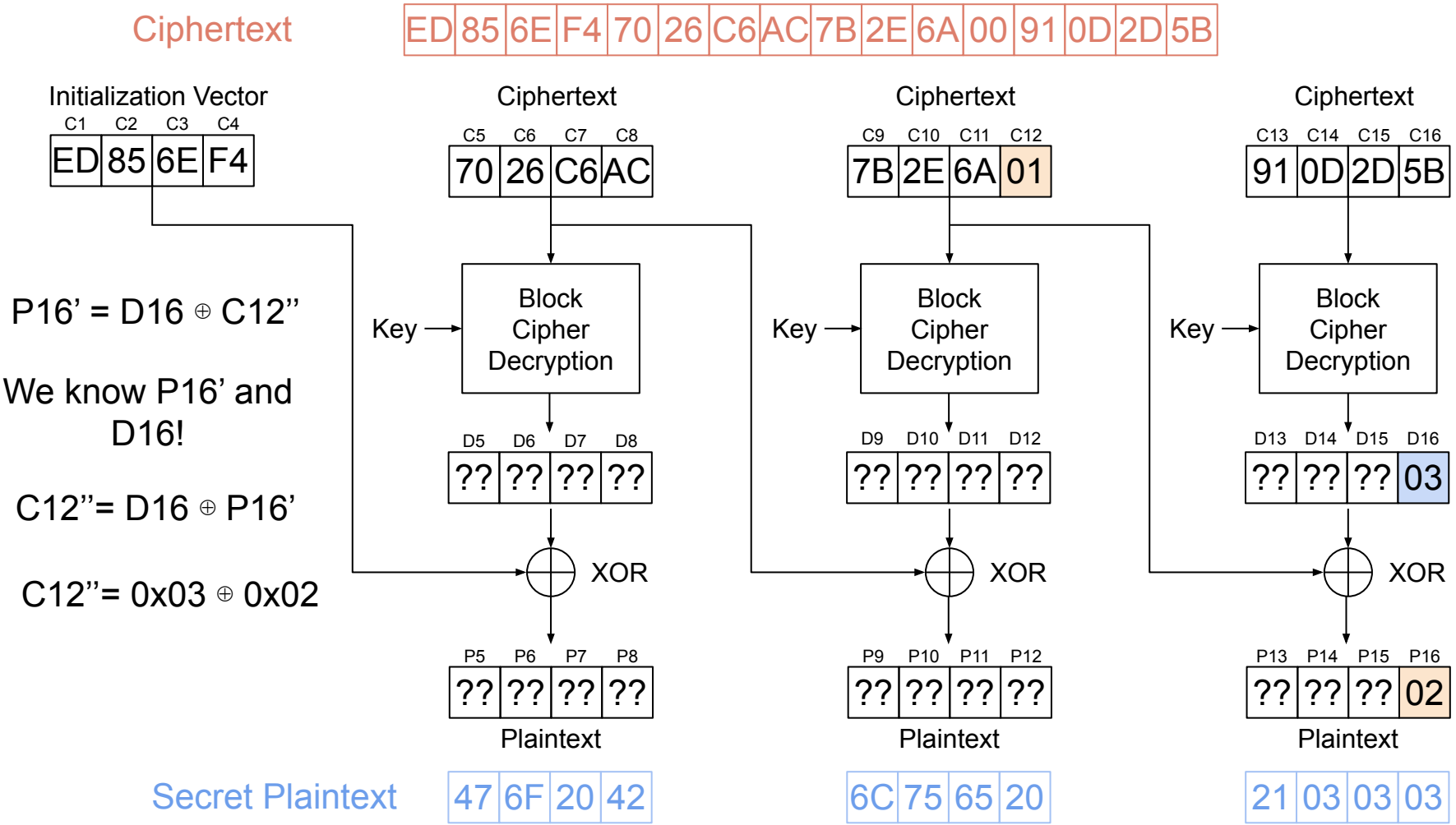

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Padding Valid
C12' = 0x02
P16' = 0x01
P'16 = C12' ⊕ D16
D16 = C12' ⊕ P'16
D16 = 0x02 ⊕ 0x01
D16 = 0x03
P16 = D16 ⊕ C12
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 01
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

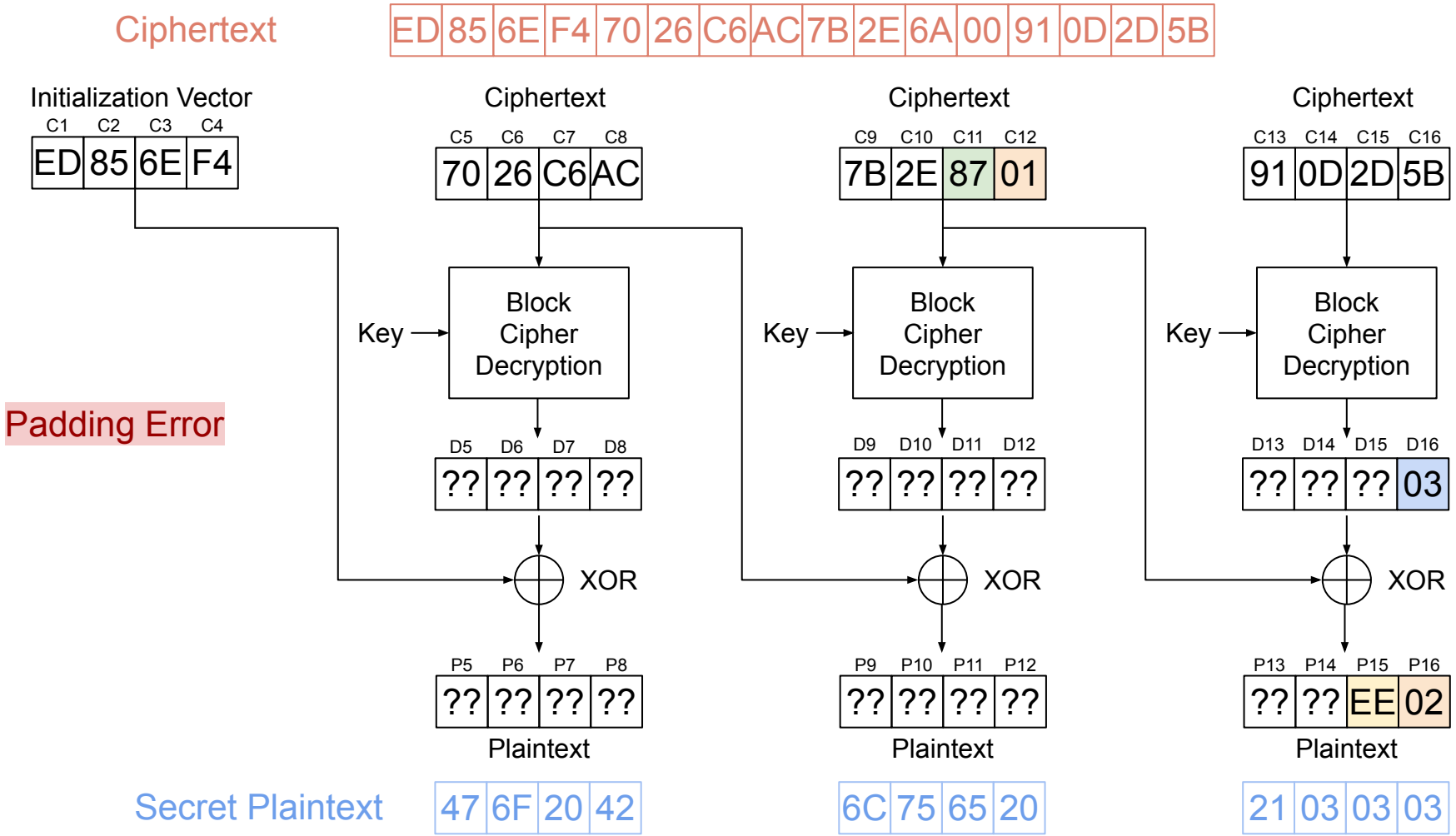

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Padding Valid
C12' = 0x02
P16' = 0x01
P'16 = C12' ⊕ D16
D16 = C12' ⊕ P'16
D16 = 0x02 ⊕ 0x01
D16 = 0x03
P16 = D16 ⊕ C12
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 03
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

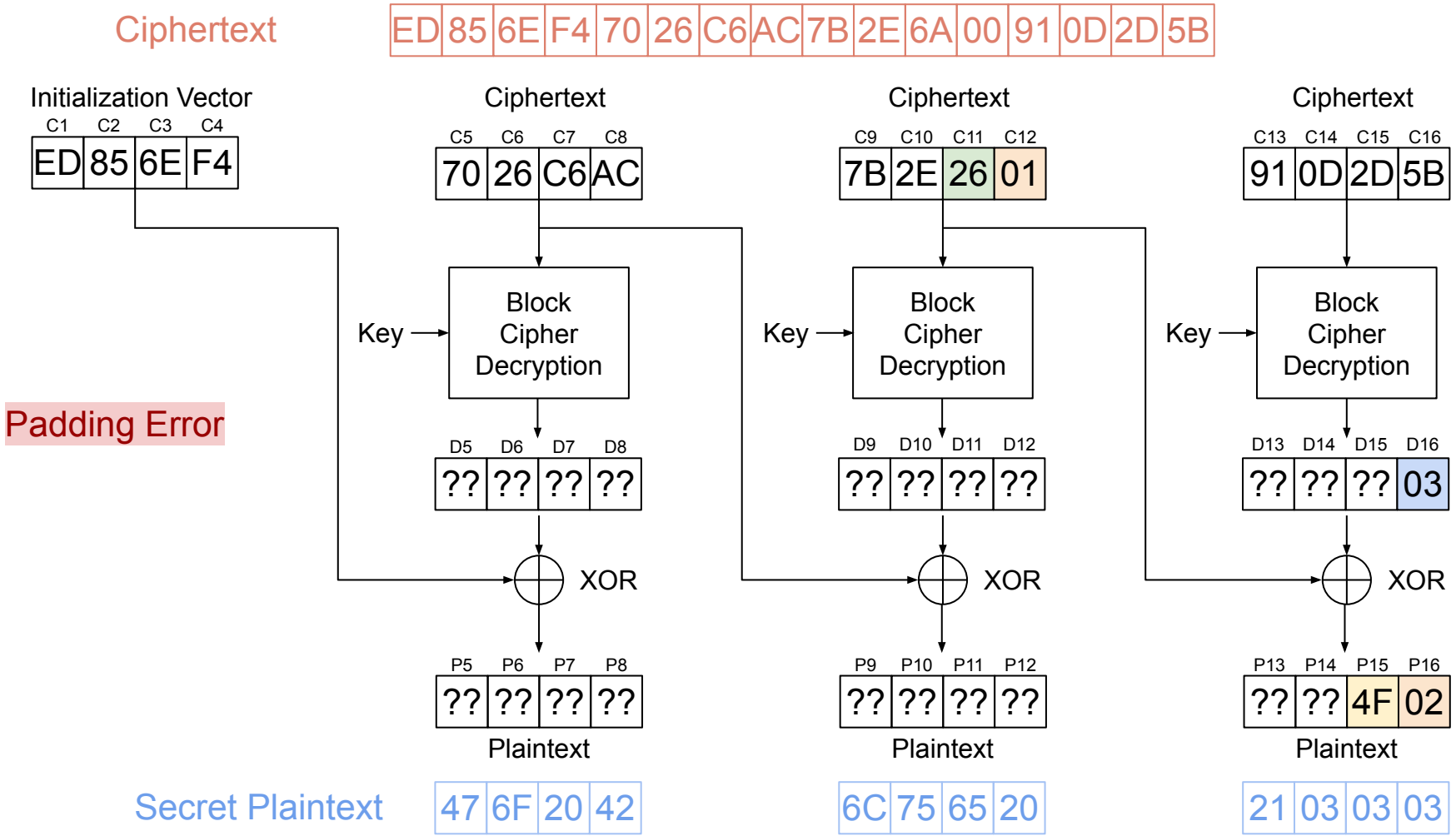

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Want to find value of P15
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 03
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

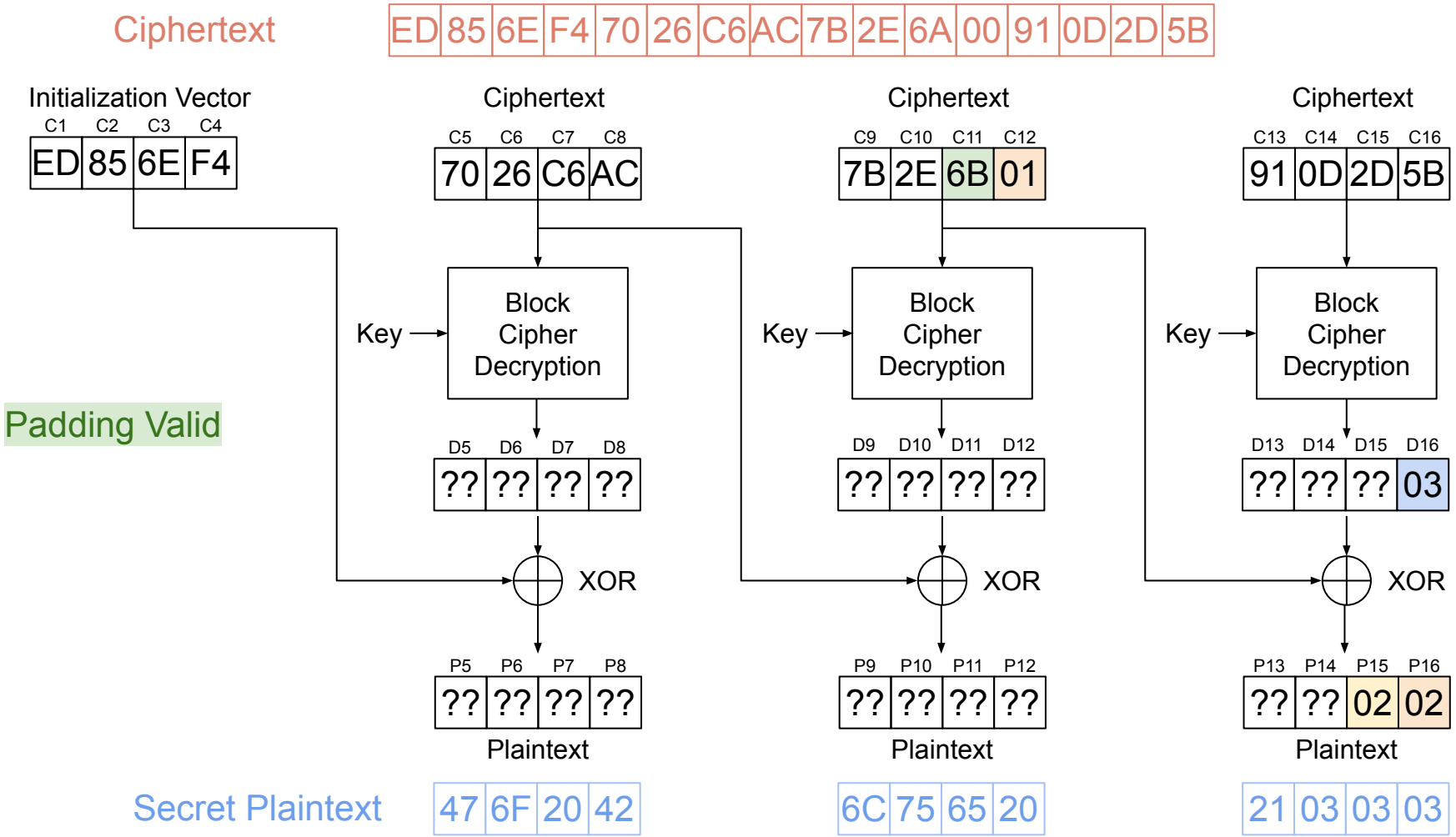

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 03
Plaintext
Plaintext
Plaintext
Need to force P16 to be 0x02 to get a valid padding with P15
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

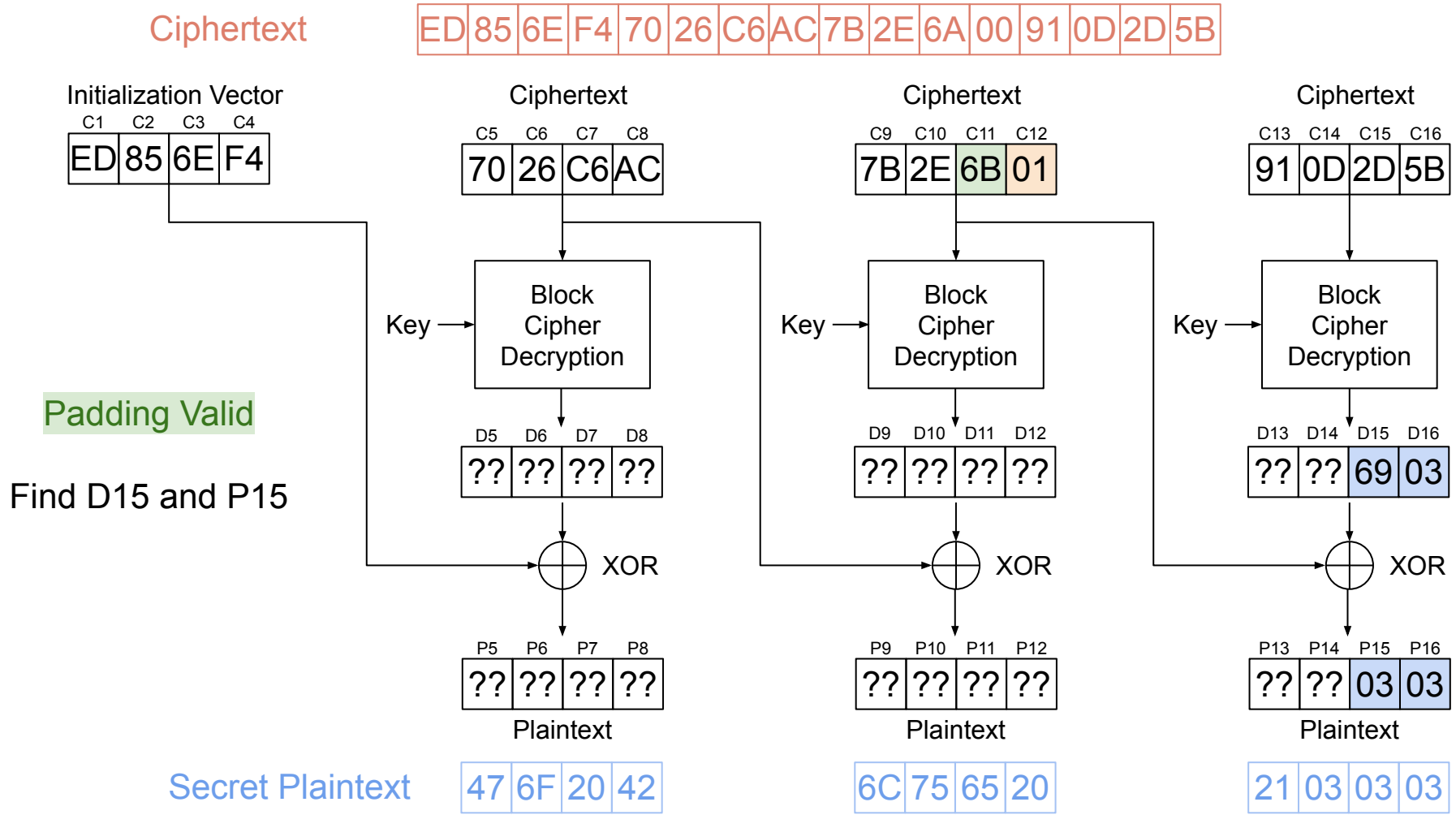

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
P16' = D16 ⊕ C12"
We know P16' and D16!
C12"= D16 ⊕ P16'
C12"= 0x03 ⊕ 0x02
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 03
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

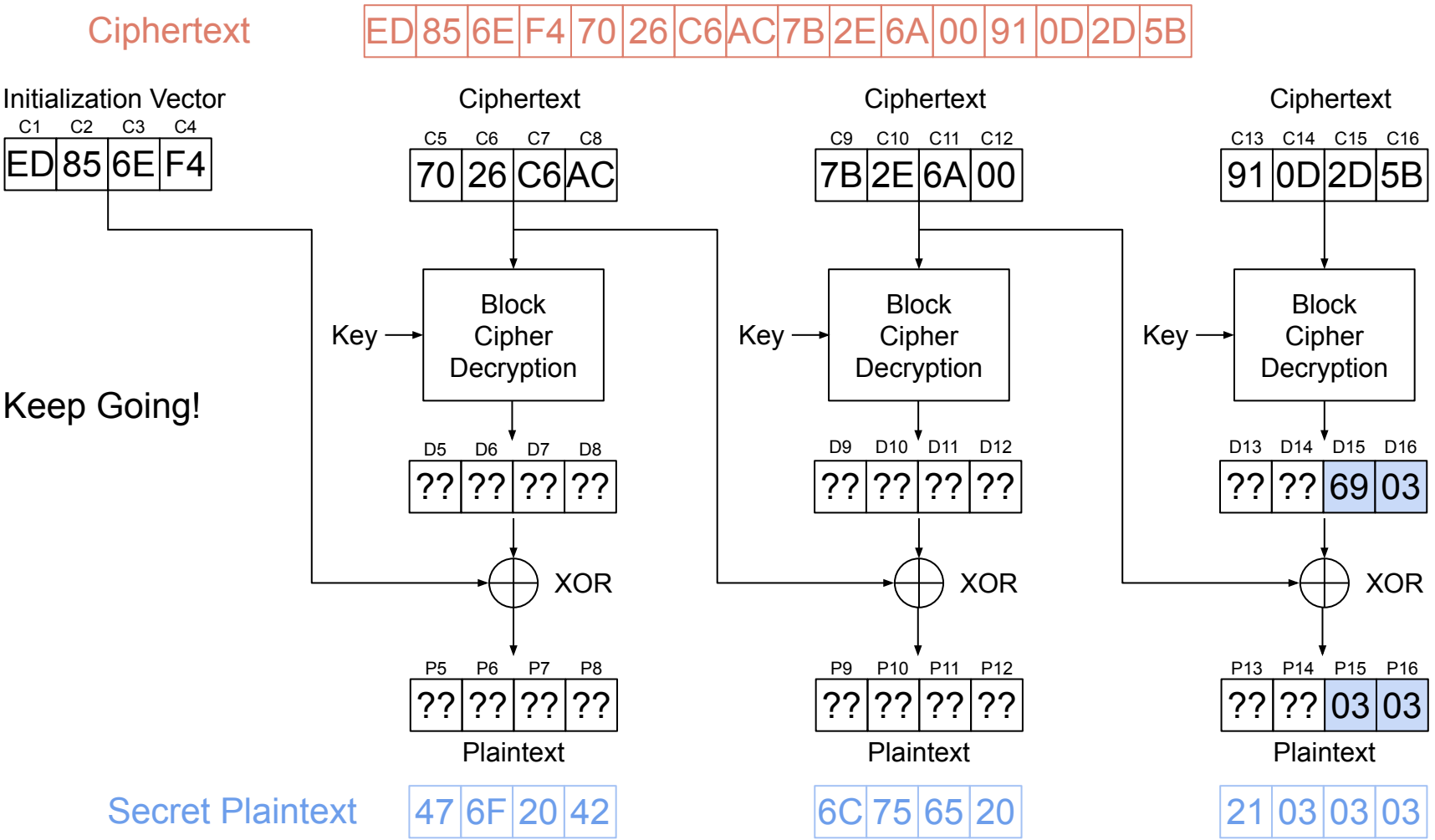

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 01
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
P16' = D16 ⊕ C12"
We know P16' and D16!
C12"= D16 ⊕ P16'
C12"= 0x03 ⊕ 0x02
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? ?? 02
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

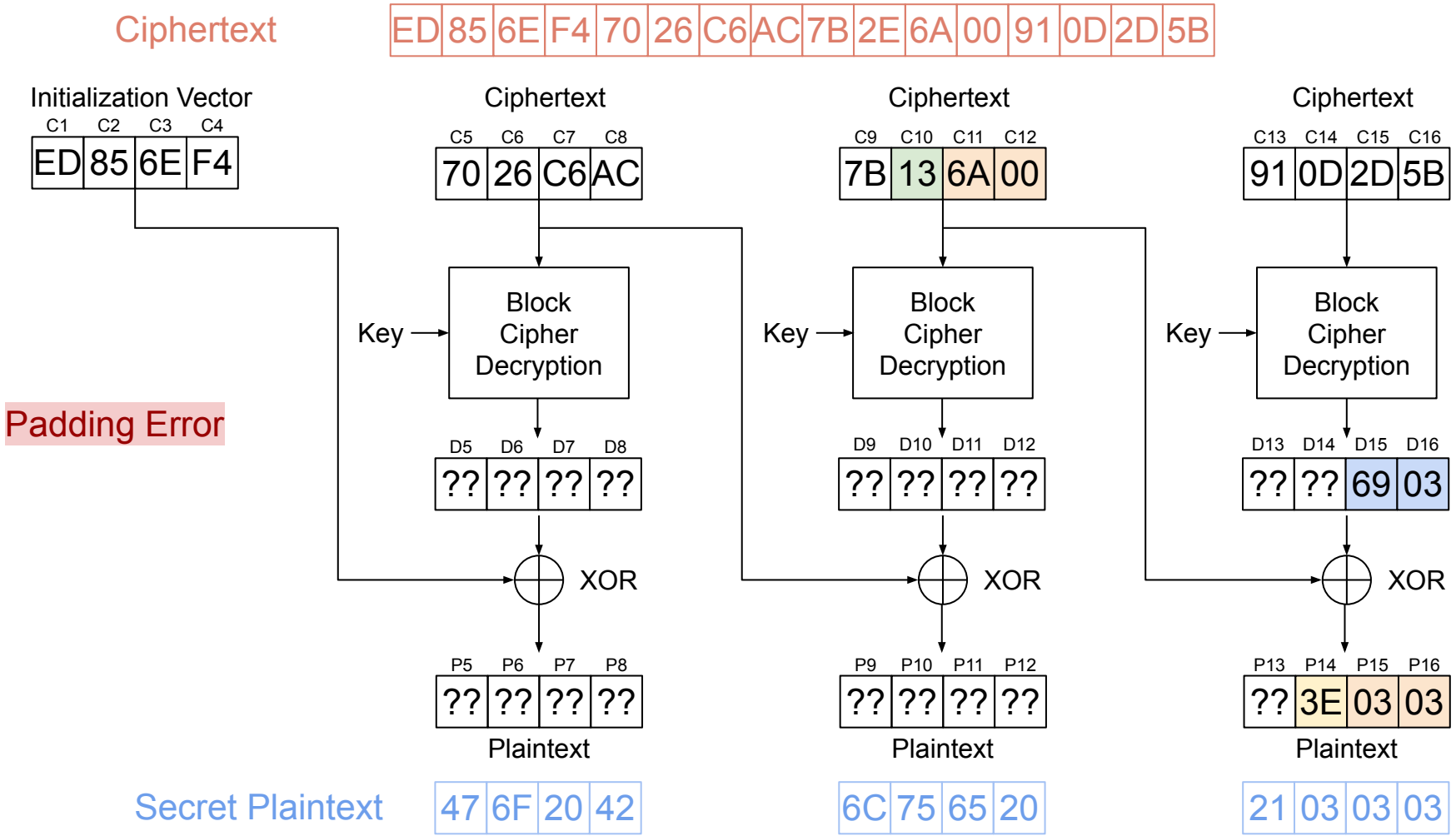

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 87 01
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Padding Error
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? EE 02
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

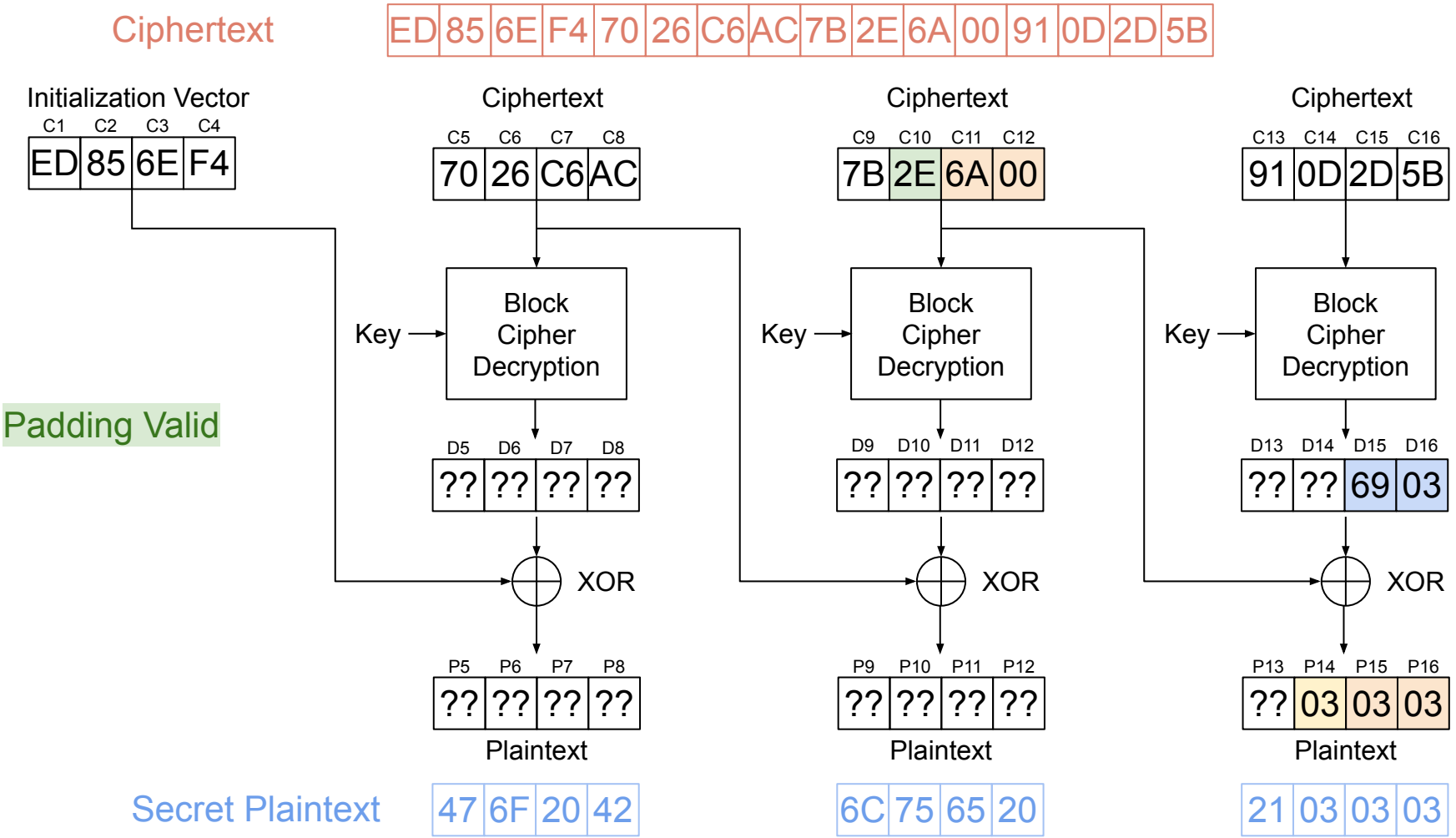

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 26 01
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Padding Error
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? 4F 02
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

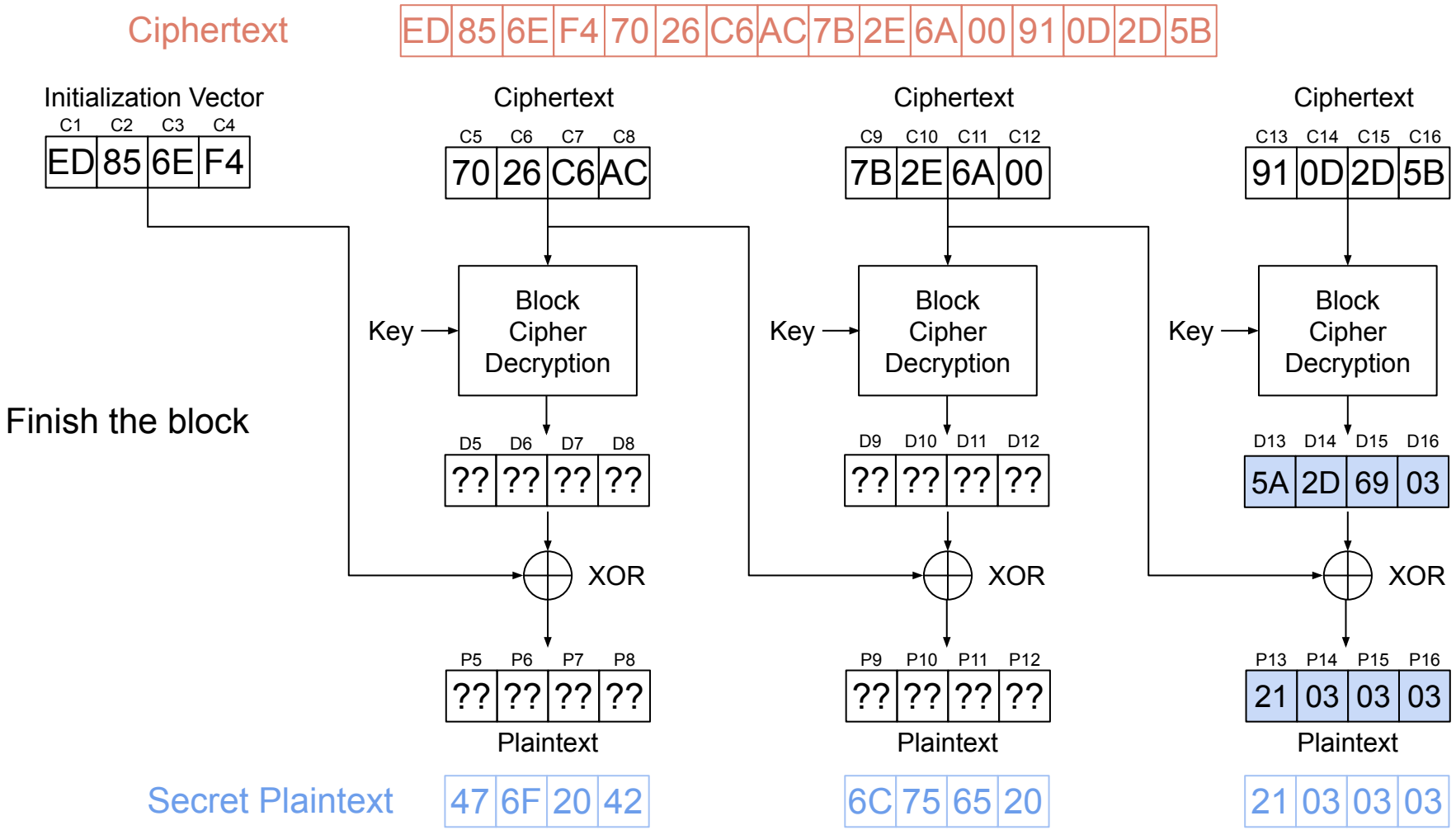

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6B 01
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Padding Valid
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? ?? 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
Plaintext
P9 P10 P11 P12
?? ?? ?? ??
Plaintext
P13 P14 P15 P16
?? ?? 02 02
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

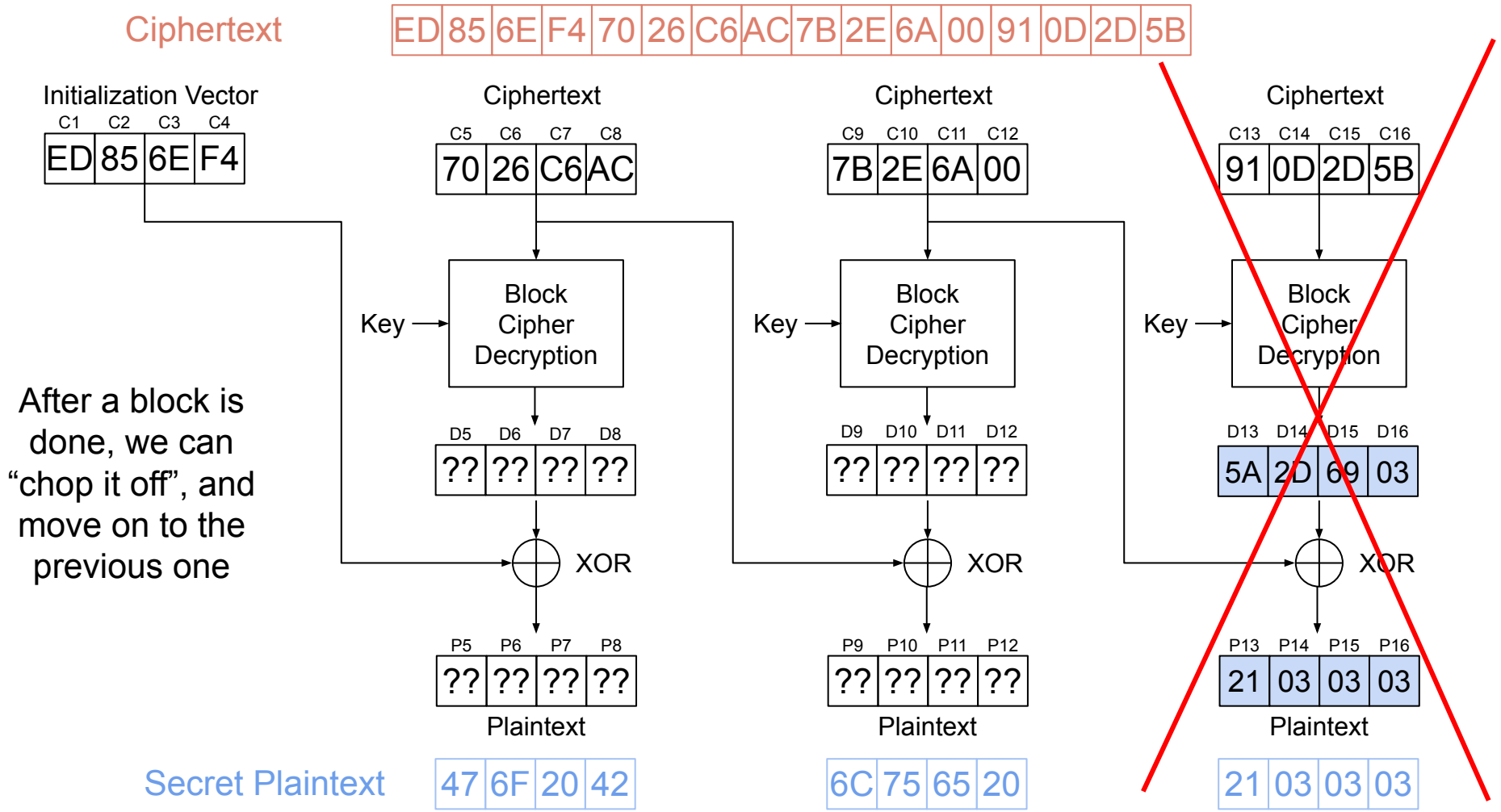

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6B 01
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Padding Valid
Find D15 and P15
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? 69 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
?? ?? 03 03
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

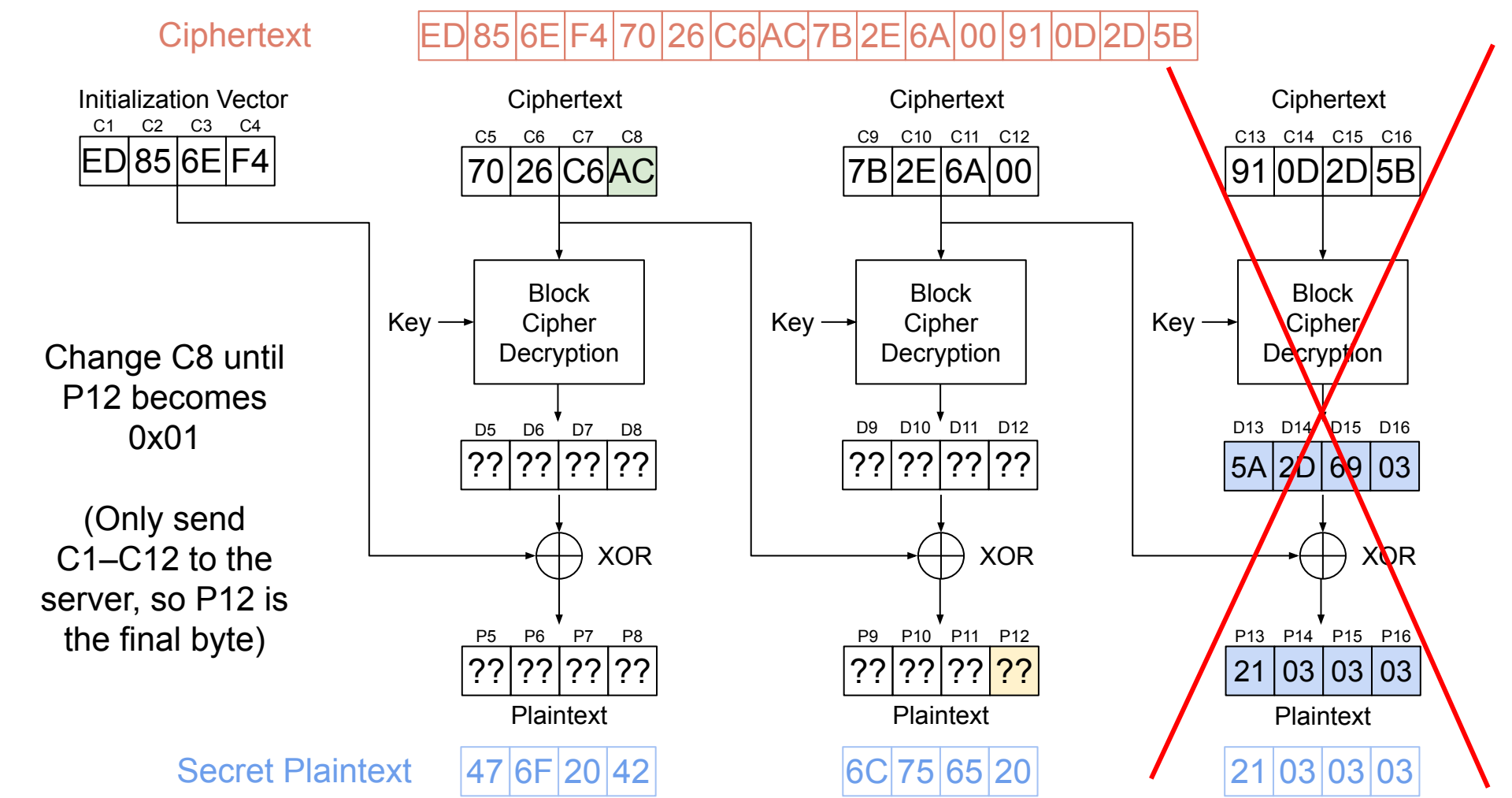

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Keep Going!
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
XOR
P5 P6 P7 P8
?? ?? ?? ??
Plaintext
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Key
Block Cipher Decryption
D9 D10 D11 D12
?? ?? ?? ??
XOR
P9 P10 P11 P12
?? ?? ?? ??
Plaintext
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
D13 D14 D15 D16
?? ?? 69 03
XOR
P13 P14 P15 P16
?? ?? 03 03
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

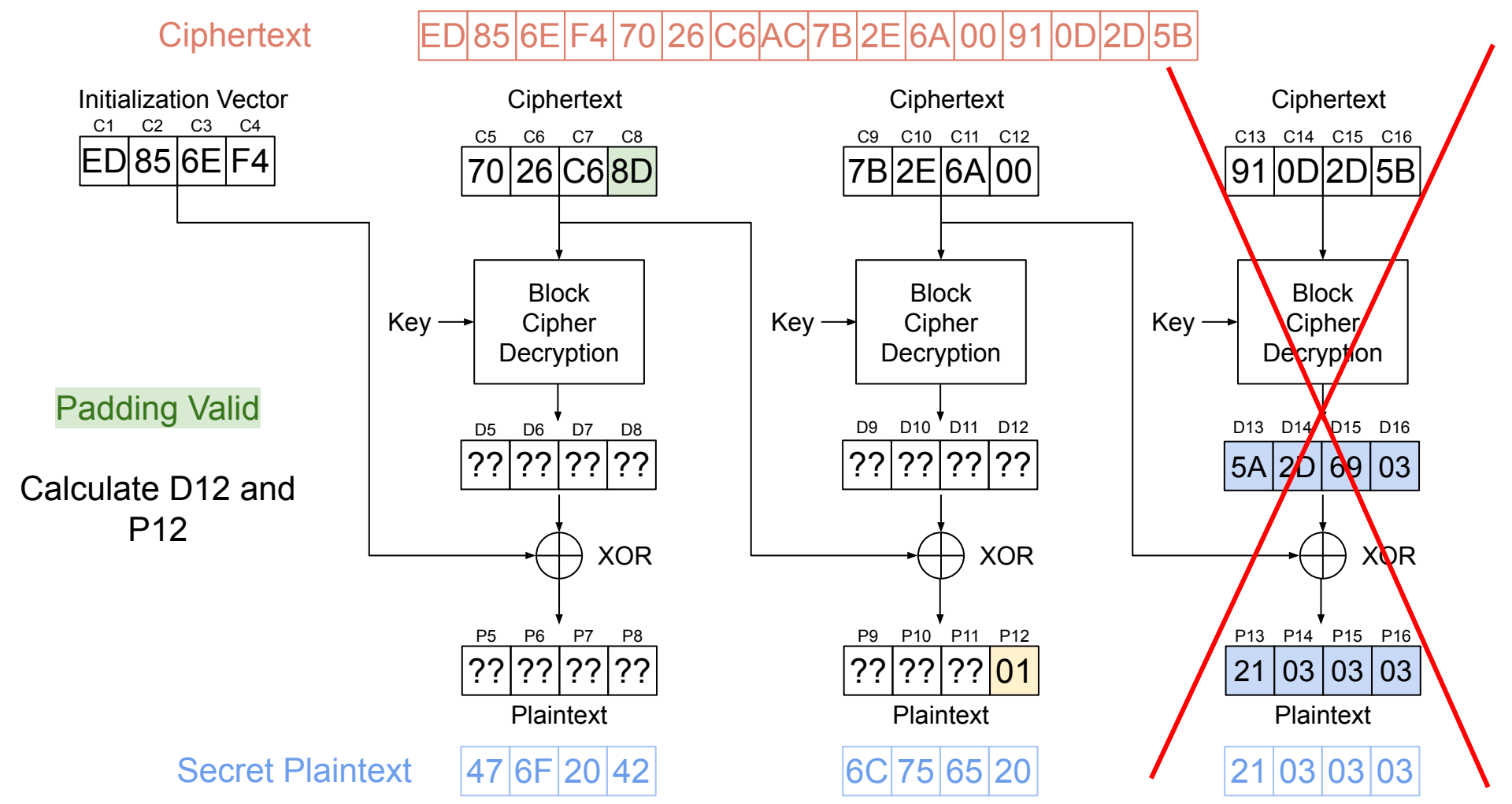

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 13 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Padding Error
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? 69 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
Plaintext
P9 P10 P11 P12
?? ?? ?? ??
Plaintext
P13 P14 P15 P16
?? 3E 03 03
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

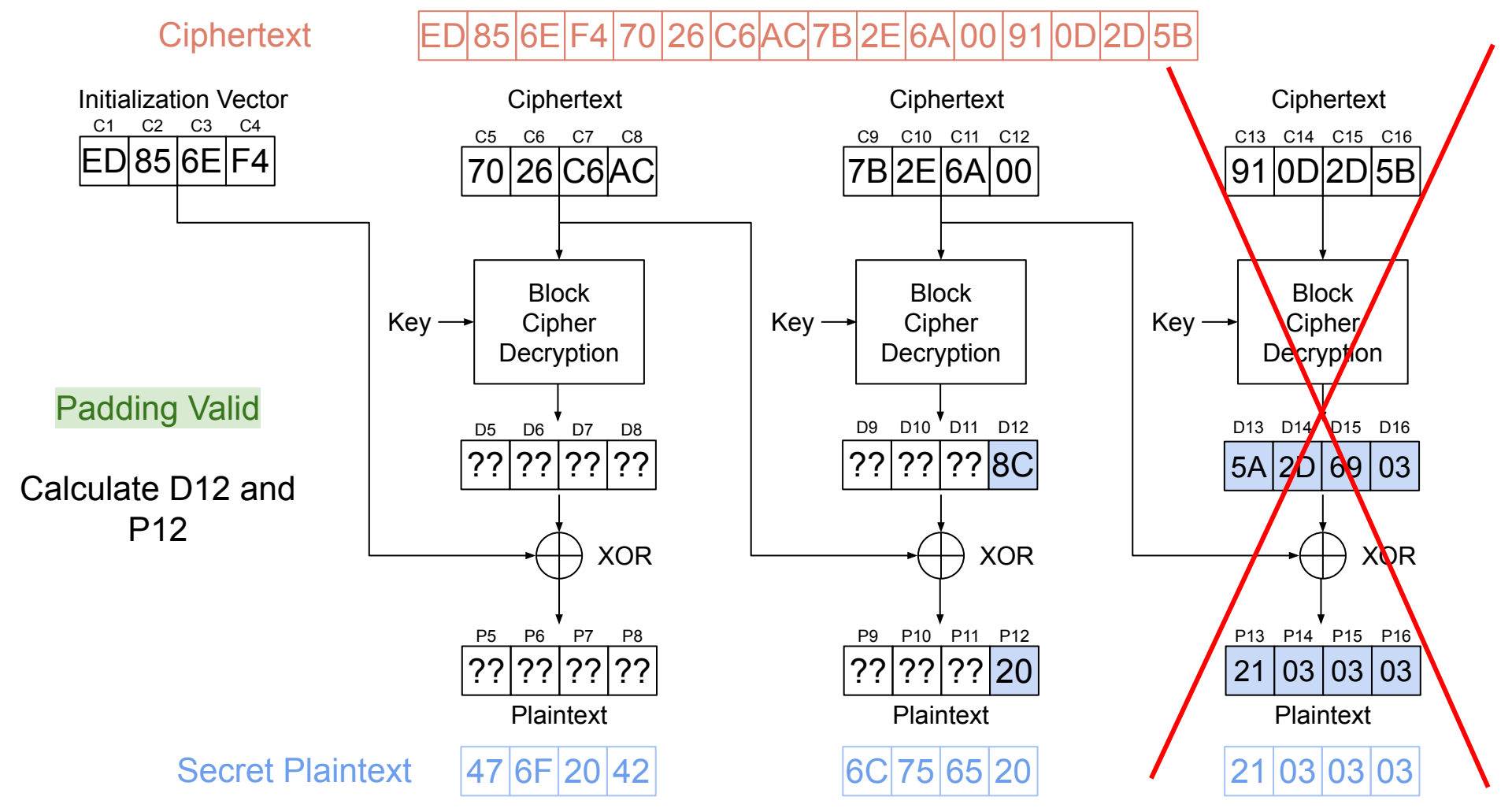

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Padding Valid
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
?? ?? 69 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
Plaintext
P9 P10 P11 P12
?? ?? ?? ??
Plaintext
P13 P14 P15 P16
?? 03 03 03
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

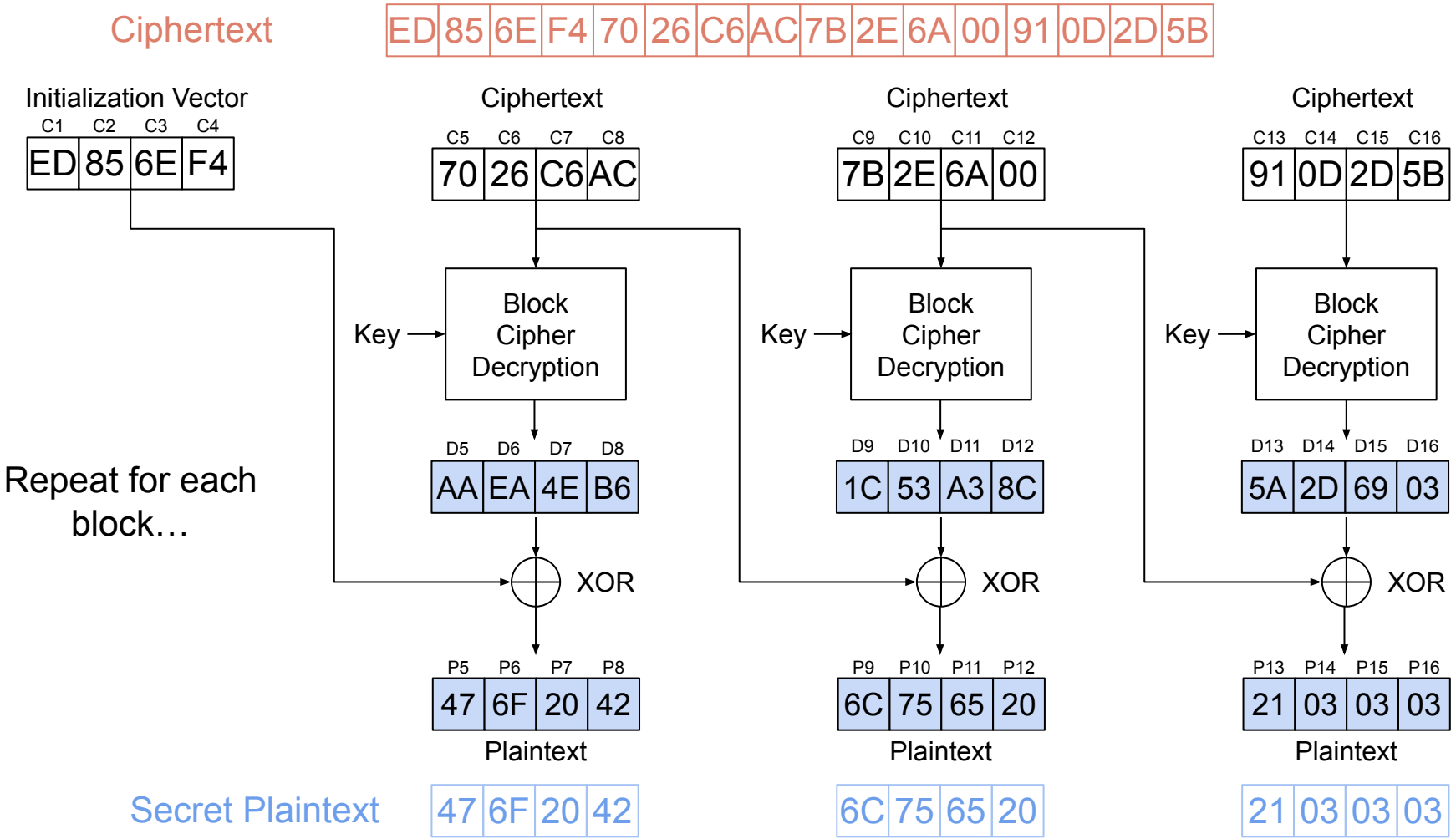

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Finish the block
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
5A 2D 69 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
21 03 03 03
Plaintext
Plaintext
Plaintext
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

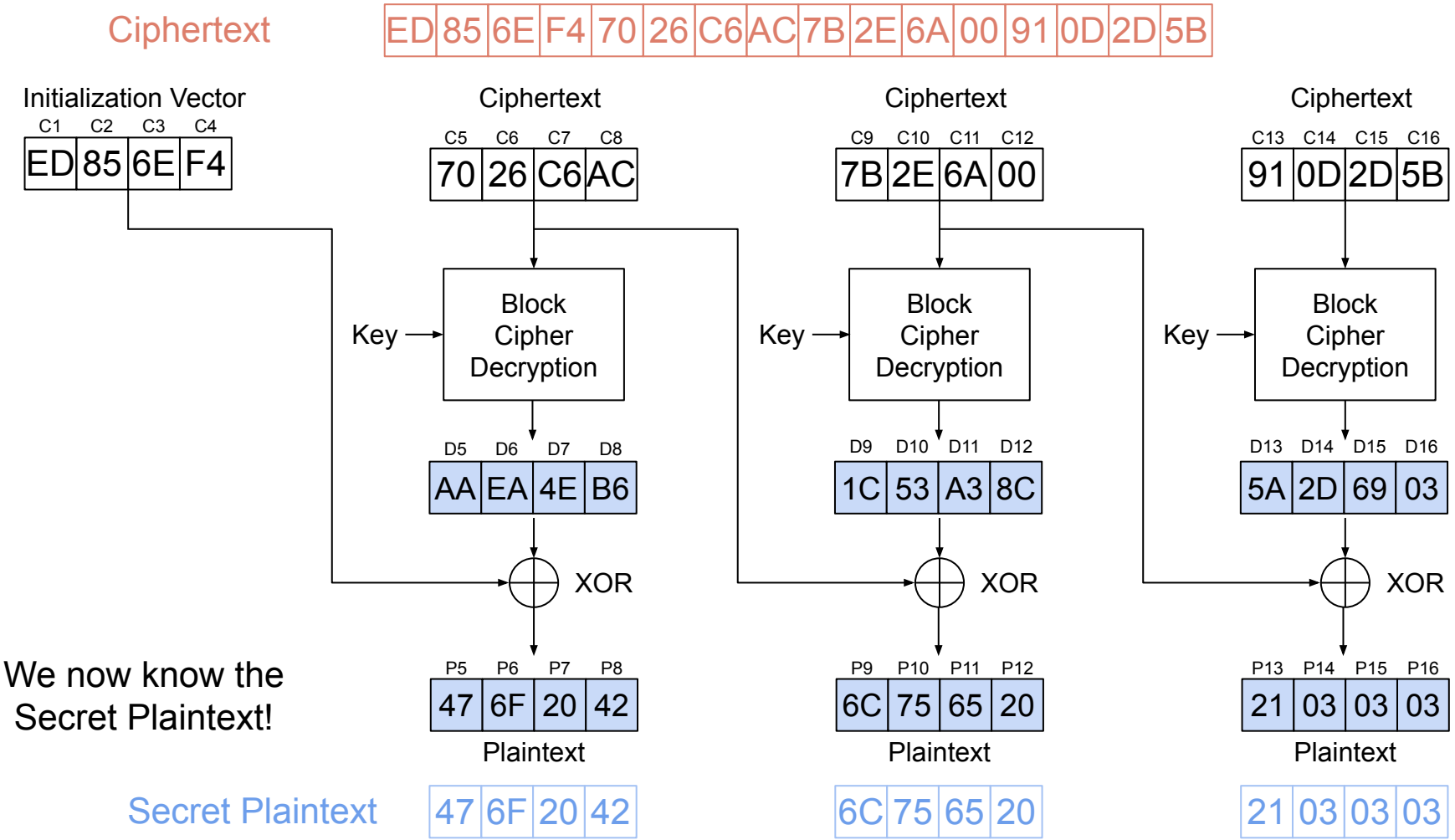

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
5A 2D 69 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
21 03 03 03
Plaintext
Plaintext
Plaintext
After a block is done, we can “chop it off”, and move on to the previous one
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03


Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
5A 2D 69 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
21 03 03 03
Plaintext
Plaintext
Plaintext
Change C8 until P12 becomes 0x01
(Only send C1–C12 to the server, so P12 is the final byte)
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

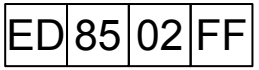

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 8D
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
5A 2D 69 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? 01
P13 P14 P15 P16
21 03 03 03
Plaintext
Plaintext
Plaintext
Padding Valid
Calculate D12 and P12
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03


Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? 8C
D13 D14 D15 D16
5A 2D 69 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? 20
P13 P14 P15 P16
21 03 03 03
Plaintext
Plaintext
Plaintext
Padding Valid
Calculate D12 and P12
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03


Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
AA EA 4E B6
D9 D10 D11 D12
1C 53 A3 8C
D13 D14 D15 D16
5A 2D 69 03
XOR
XOR
XOR
P5 P6 P7 P8
47 6F 20 42
Plaintext
P9 P10 P11 P12
6C 75 65 20
Plaintext
P13 P14 P15 P16
21 03 03 03
Plaintext
Repeat for each block…
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

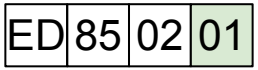

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
AA EA 4E B6
D9 D10 D11 D12
1C 53 A3 8C
D13 D14 D15 D16
5A 2D 69 03
XOR
XOR
XOR
P5 P6 P7 P8
47 6F 20 42
Plaintext
P9 P10 P11 P12
6C 75 65 20
Plaintext
P13 P14 P15 P16
21 03 03 03
Plaintext
We now know the Secret Plaintext!
Secret Plaintext
47 6F 20 42
6C 75 65 20
21 03 03 03

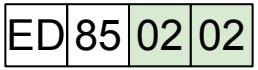
Tricky Edge Cases

- What if one of the blocks of Plaintext is 

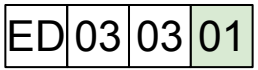
?

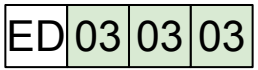
- When the last byte is **0x01** OR **0x02**, the block can have valid padding!

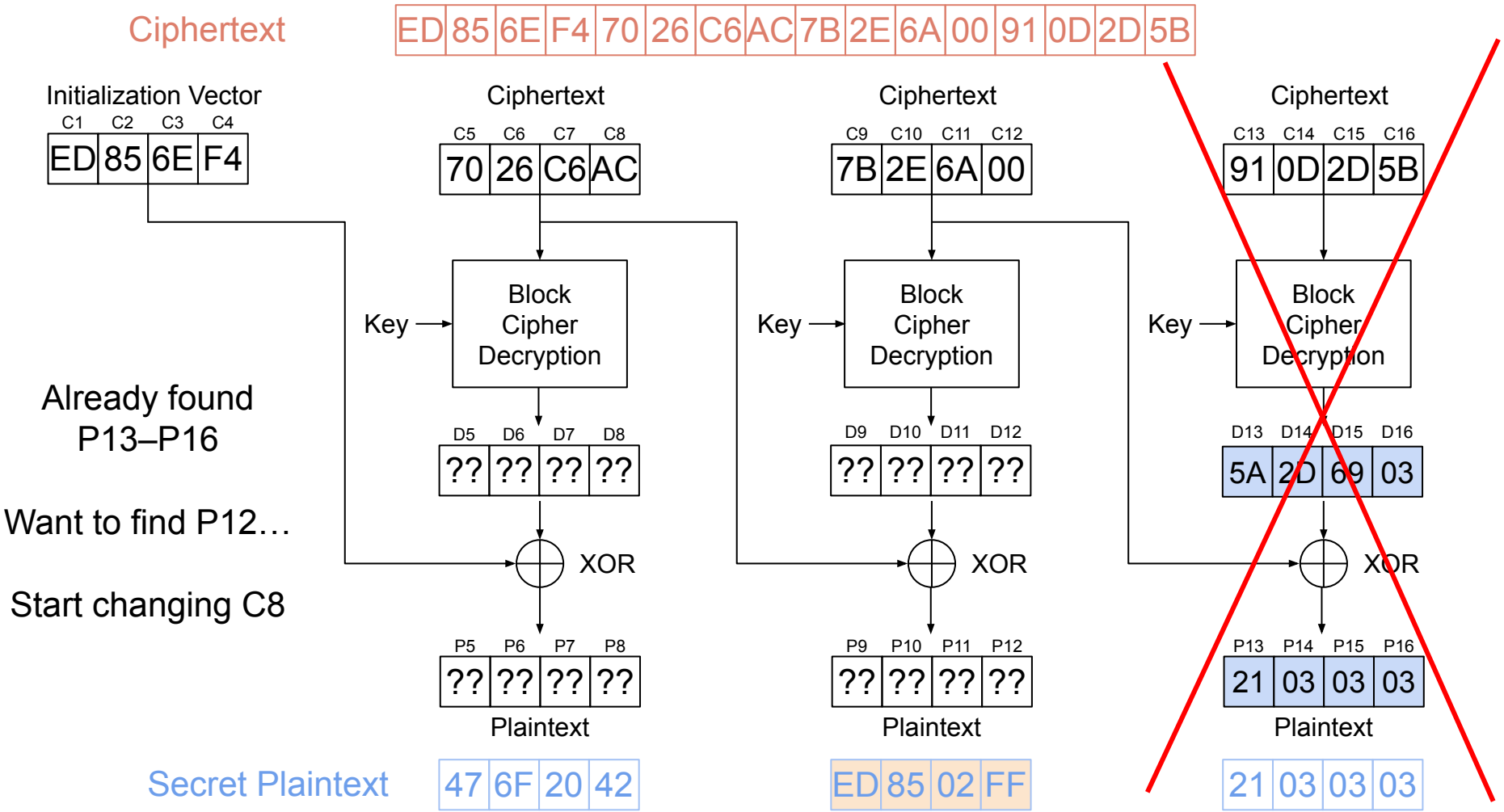


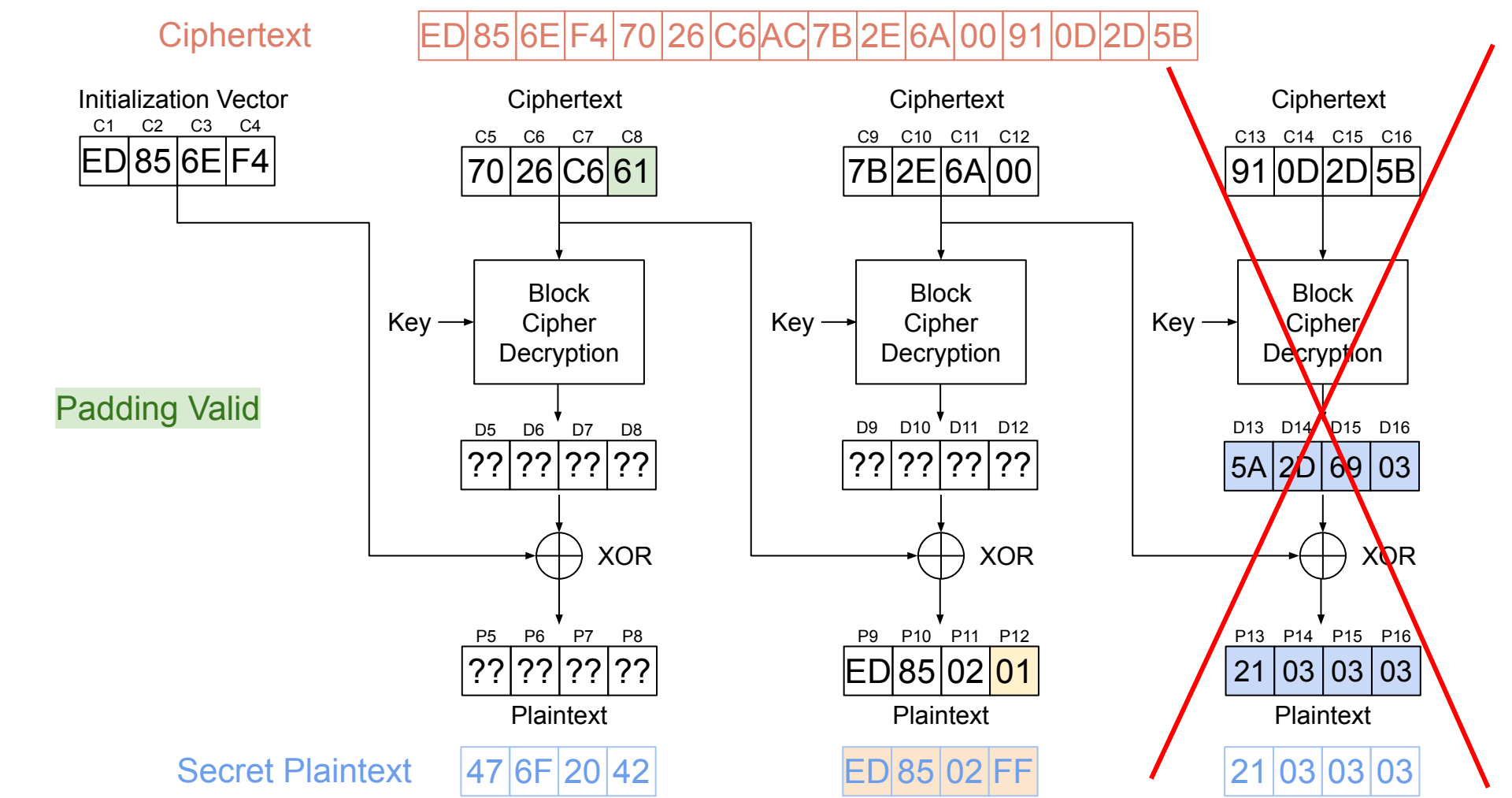


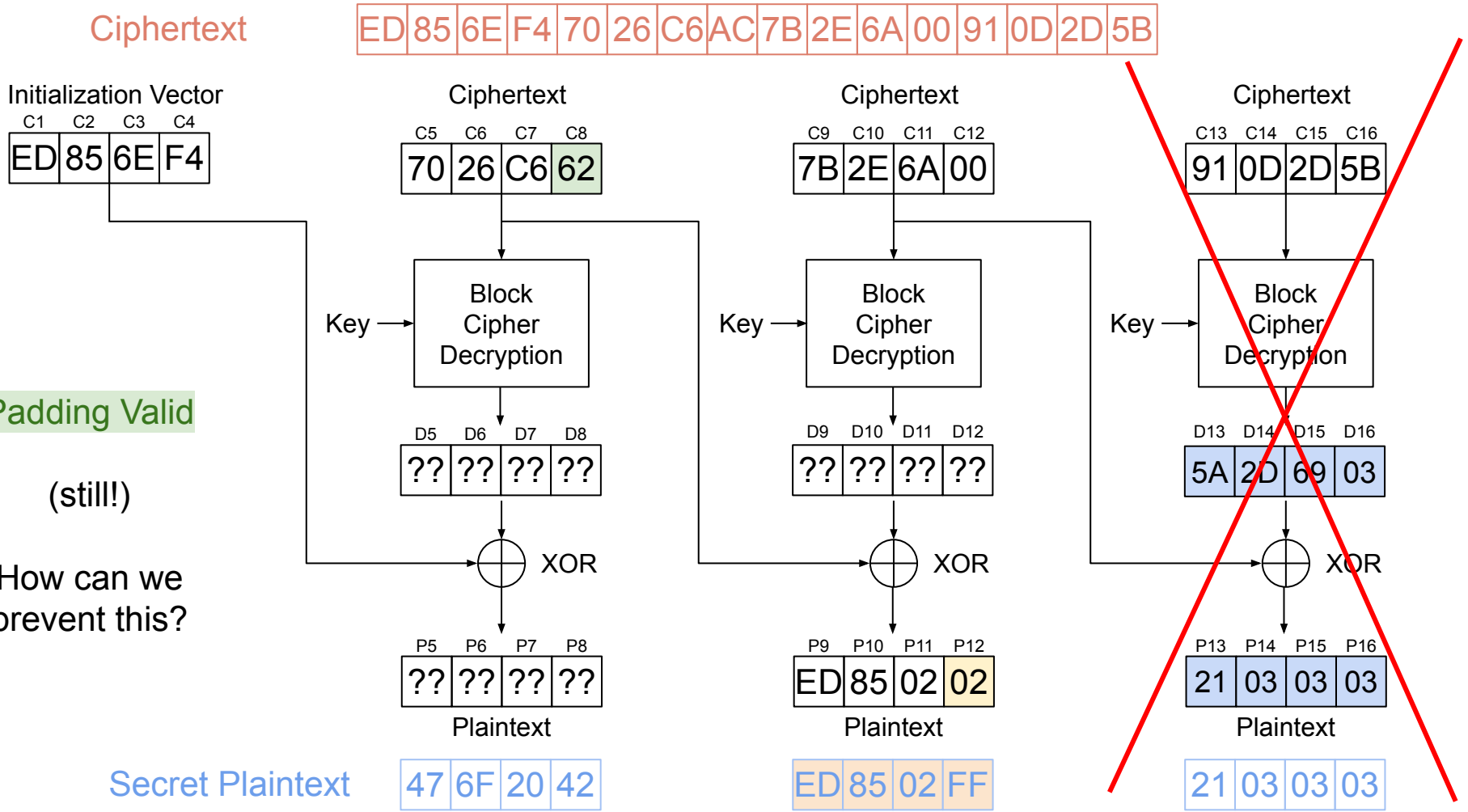
- Other edge cases as well, imagine:






Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 AC
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
5A 2D 69 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
?? ?? ?? ??
P13 P14 P15 P16
21 03 03 03
Plaintext
Plaintext
Plaintext
Already found P13–P16
Want to find P12…
Start changing C8
Secret Plaintext
47 6F 20 42
ED 85 02 FF
21 03 03 03


Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 61
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Padding Valid
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
5A 2D 69 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
Plaintext
P9 P10 P11 P12
ED 85 02 01
Plaintext
P13 P14 P15 P16
21 03 03 03
Plaintext
Secret Plaintext
47 6F 20 42
ED 85 02 FF
21 03 03 03

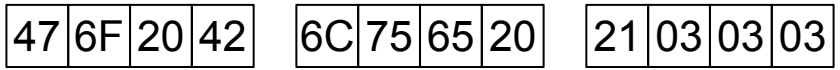

Ciphertext
ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B
Initialization Vector
C1 C2 C3 C4
ED 85 6E F4
Ciphertext
C5 C6 C7 C8
70 26 C6 62
Ciphertext
C9 C10 C11 C12
7B 2E 6A 00
Ciphertext
C13 C14 C15 C16
91 0D 2D 5B
Key
Block Cipher Decryption
Key
Block Cipher Decryption
Key
Block Cipher Decryption
D5 D6 D7 D8
?? ?? ?? ??
D9 D10 D11 D12
?? ?? ?? ??
D13 D14 D15 D16
5A 2D 69 03
XOR
XOR
XOR
P5 P6 P7 P8
?? ?? ?? ??
P9 P10 P11 P12
ED 85 02 02
P13 P14 P15 P16
21 03 03 03
Plaintext
Plaintext
Plaintext
Padding Valid
(still!)
How can we prevent this?
Secret Plaintext
47 6F 20 42
ED 85 02 FF
21 03 03 03

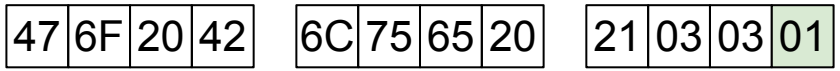
Project Differences

- 16 byte blocks (4 byte blocks in this example)
- MAC appended to plaintext before padding and block encryption
- New error message from server: Invalid Mac
    - Padding is correct, but the MAC is not valid for the message

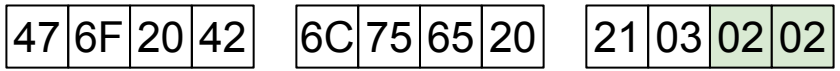
Another Edge Case

- Plaintext looks like this ➡️

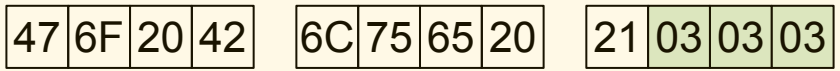




- How will the server respond to the bottom case?



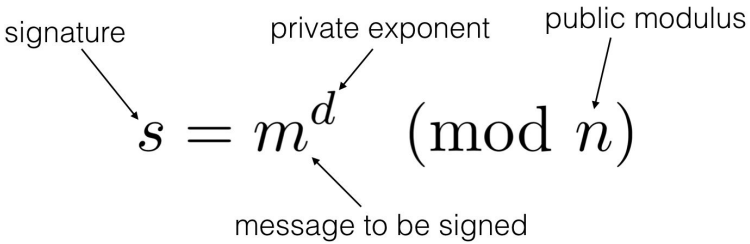
?



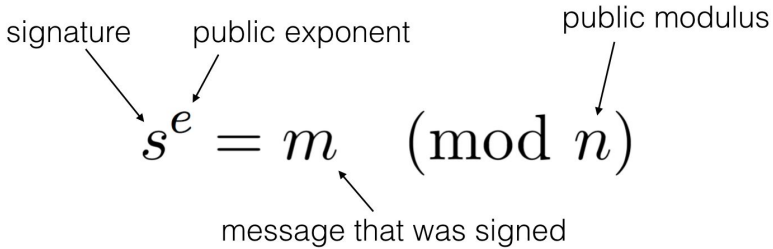
Bleichenbacher Attack (RSA Signature Forgery)

Textbook RSA Signatures

Signing



Verifying



See the guts of your own key:

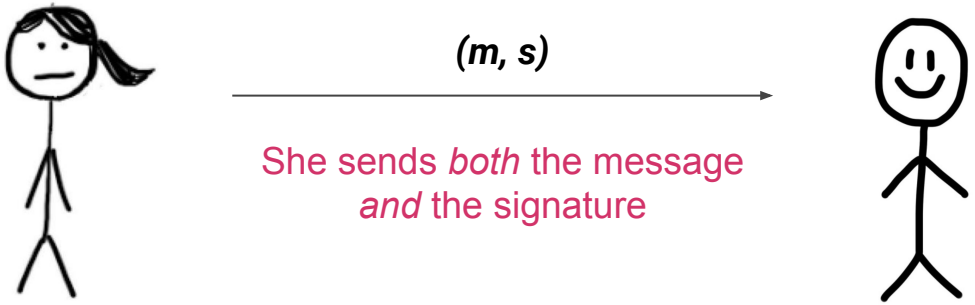
```
$ openssl genrsa -out private.key 4096
$ openssl rsa -in private.key -pubout -out public.key
$ openssl rsa -in private.key -text -noout
$ openssl rsa -in public.key -pubin -text -noout
```

generate private
…and public key

print private
…and public key info

Textbook RSA Signatures

- Our good friends Alice and Bob want to communicate with sender authenticity using RSA



Public: ***(e, N)***
Private: ***d***

Message: ***m***
Signature: $s = m^d \bmod N$

Verify: $s^e \bmod N == m$

A Problem With Textbook RSA

- It's really easy for Mallory to generate a valid ***(m, s)*** pair
- Instead of starting with ***m*** and generating ***s***, they start with ***s*** and generate ***m***:

$$m = s^e \bmod N$$

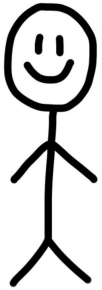
- Fix: Instead of signing ***m***, we sign ***PKCS-PAD(m)***
  - The output of PKCS-PAD follows a very specific format
  - It's infeasible for Mallory to find a value of ***s*** such that $s^e \bmod N$ will follow this format
  - The PKCS-PAD digest will be the same length for any message

Bleichenbacher Attack: Vulnerability 1

- So what's Bleichenbacher got to do with it?

(m, s)

She sends *both* the message *and* the signature



If e is small enough, we can forge a signature that Bob will verify is correct *without needing to know Alice's private key.* How?

Public: ***(e, N)***
Private: ***d***

Message: ***m***
Signature: $s = (PKCS\text{-}PAD(m))^d \bmod N$ Verify: $s^e \bmod N == PKCS\text{-}PAD(m)$

What if e is really small, like, 3?

Bleichenbacher Attack: Vulnerability 2

- **How *<u>should</u>* a secure bank's operations work?**

m = *"gimme some $$$"*

$$s = (PKCS\text{-}PAD(m))^d \bmod N$$

1. Admin sends the bank's server the ***(m, s)*** pair
2. Bank recreates the ***PKCS-PAD(m)*** using what Admin sent: ***x = PKCS-PAD(m)***
3. Bank raises ***s*** to Admin's public exponent ***e***: $y = s^e \bmod N$
4. If ***x == y***, Admin is authenticated

Bleichenbacher Attack: Vulnerability 2

- **How do the bank's operations actually work?**

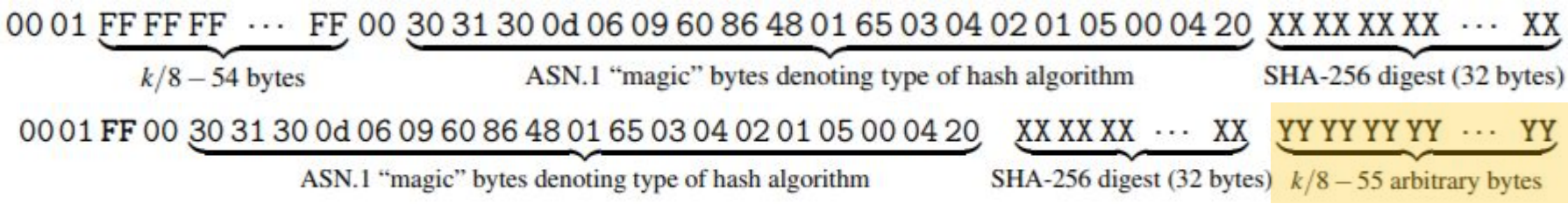
m = *"gimme some $$$"*

$$s = (PKCS\text{-}PAD(m))^d \bmod N$$

1. Admin sends the bank's server the ***(m, s)*** pair
2. Bank raises ***s*** to Admin's public exponent ***e***: $y = s^e \bmod N$
3. Bank parses the SHA-256 digest, ***h***, from ***y***
4. If ***h*** == SHA-256(***m***), Admin is authenticated

Bleichenbacher Attack

What the result of the signature verification should look like ***(s^e mod N)***



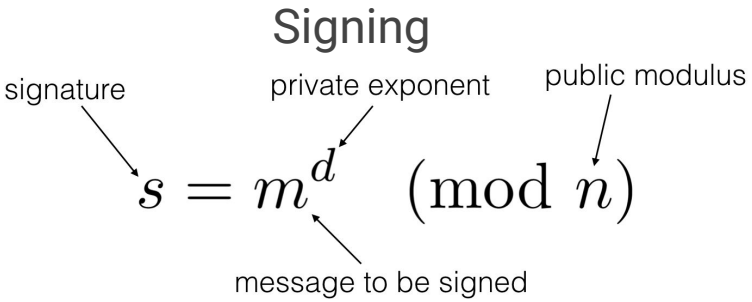
Format of PKCS-PAD(***m***) above.

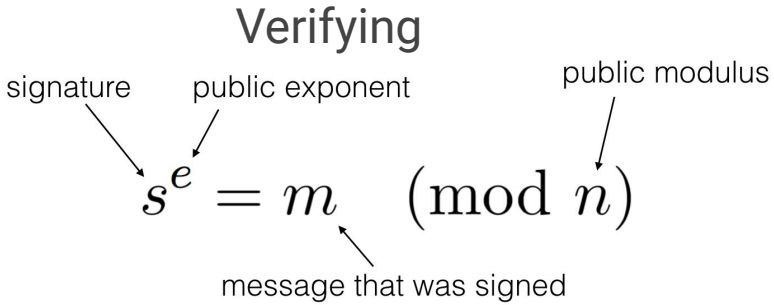
Accepted due to poor implementation

- Lazy implementation
  - Does not count FF bytes; also does not verify hash is in rightmost bytes
- How can we forge something such that (***s^e mod N***) gives us the 2nd message seen above?
  - What if **e** just so happens to be very small?

When it doesn’t wrap around...

- Let’s forge a signature for message m with e = 3
  - How do we make it so that verifying the message gives us m (mod n)?
  - How does the “lazy implementation” of checking signatures help with this?





See you next week!