

EECS 388: Lab 3

Padding Oracle Attack
Bleichenbacher Attack

Current Assignments

Reminder: Canvas quizzes due
the day before the next lecture

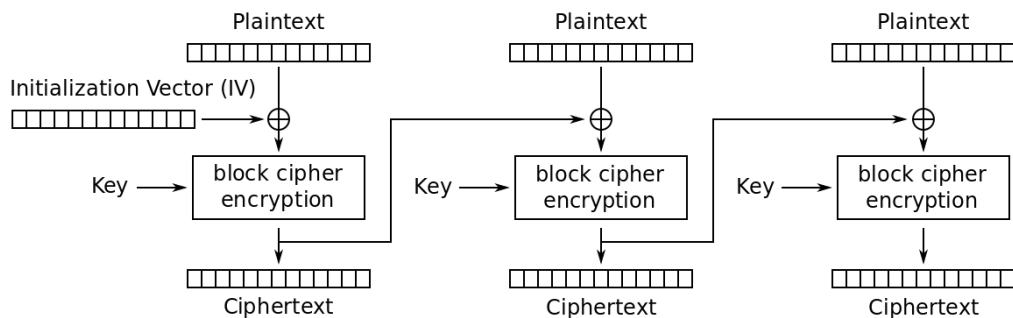
- Project 1 Part 2 due **Thursday, September 21 at 6 p.m.**
 - Padding Oracle Attack
 - Bleichenbacher Attack (RSA signature forgery)

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

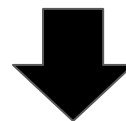
Padding

- 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

•	•	•		2A	FF	01	78	9A
---	---	---	--	----	----	----	----	----

XX	XX	XX	XX	XX	XX	XX	01
----	----	----	----	----	----	----	----

XX	XX	XX	XX	XX	XX	02	02
----	----	----	----	----	----	----	----



XX	07	07	07	07	07	07	07
----	----	----	----	----	----	----	----

08	08	08	08	08	08	08	08
----	----	----	----	----	----	----	----

XOR Properties

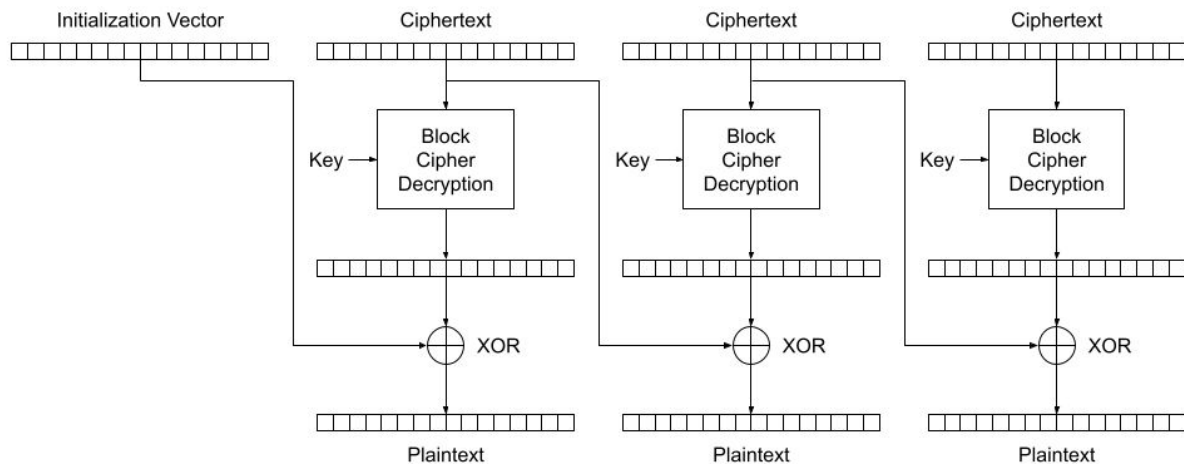
- $A \oplus A = 0$
- $A \oplus 0 = A$
- $A \oplus B = B \oplus A$
- If $A \oplus B = C$,
 then $C \oplus B = A$
 and $C \oplus A = B$

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

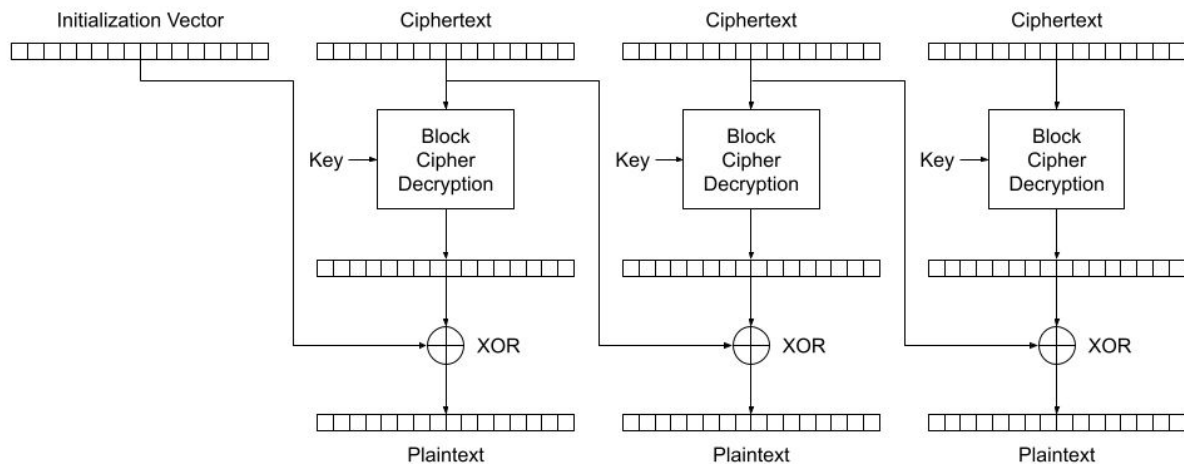


All Mallory has is ciphertext

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?

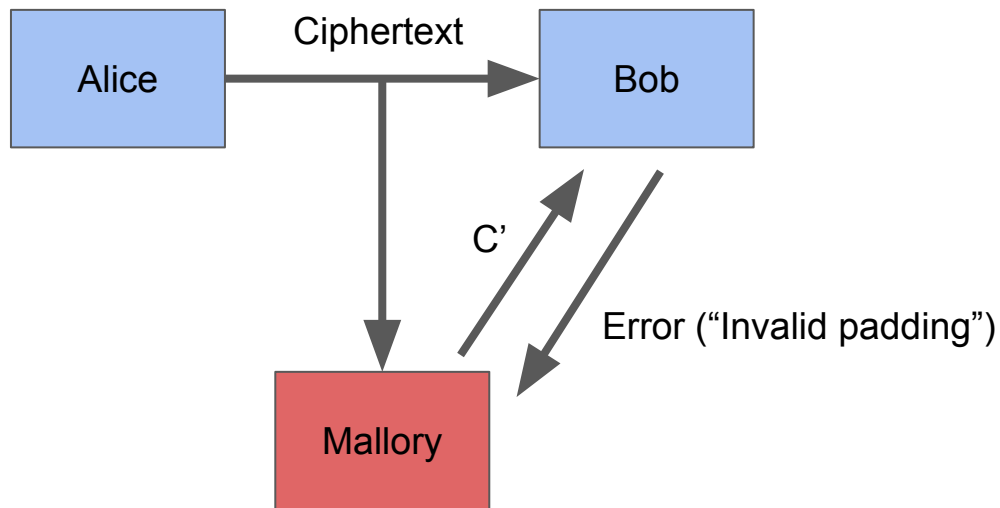


All Mallory has is ciphertext

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

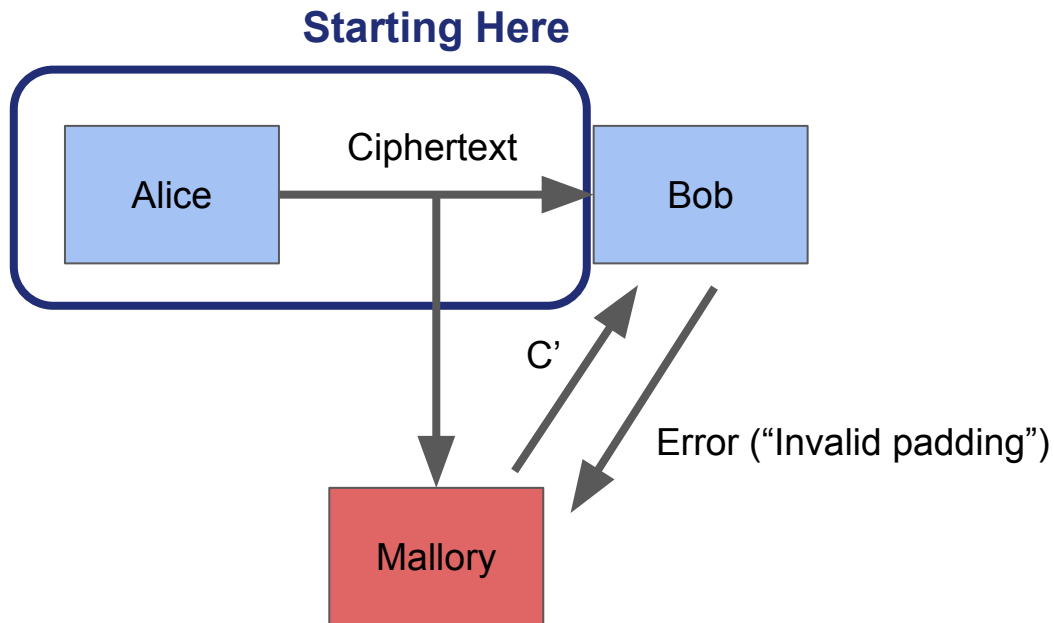
Premise

- 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

Secret Message

G	o	_	B	l	u	e	_	!
---	---	---	---	---	---	---	---	---

Encode (utf-8) & Add Padding

Secret Plaintext

47	6F	20	42	6C	75	65	20	21	03	03	03
----	----	----	----	----	----	----	----	----	----	----	----

Split into blocks (4 Bytes here)

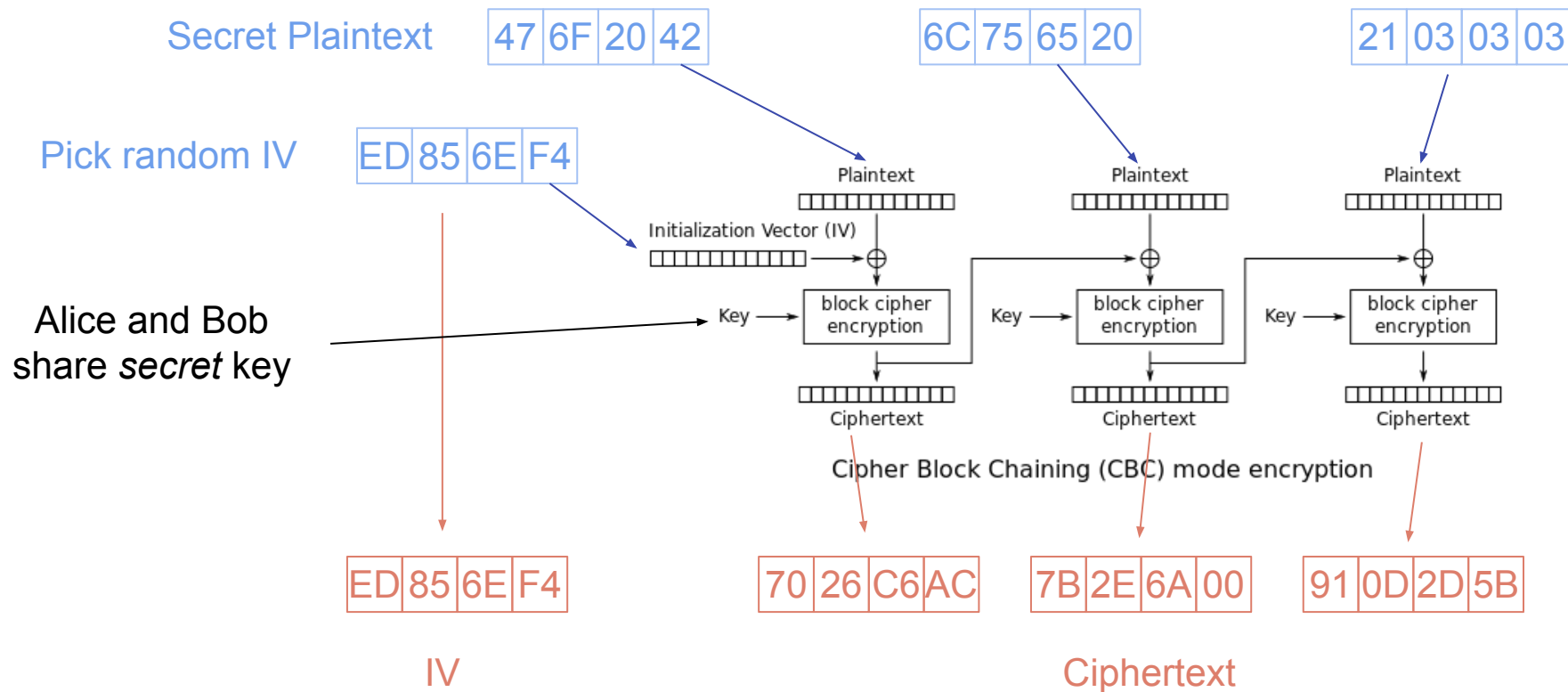
Secret Plaintext

47	6F	20	42
----	----	----	----

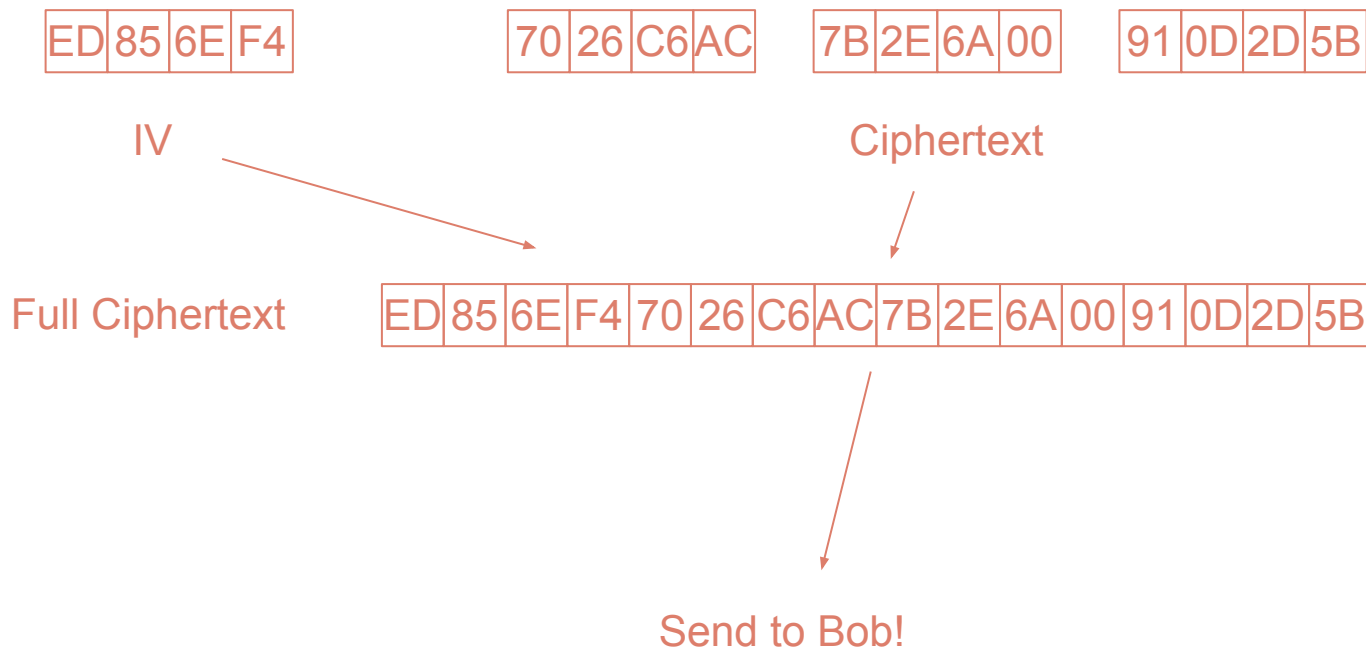
6C	75	65	20
----	----	----	----

21	03	03	03
----	----	----	----

Alice's Encryption (cont.)

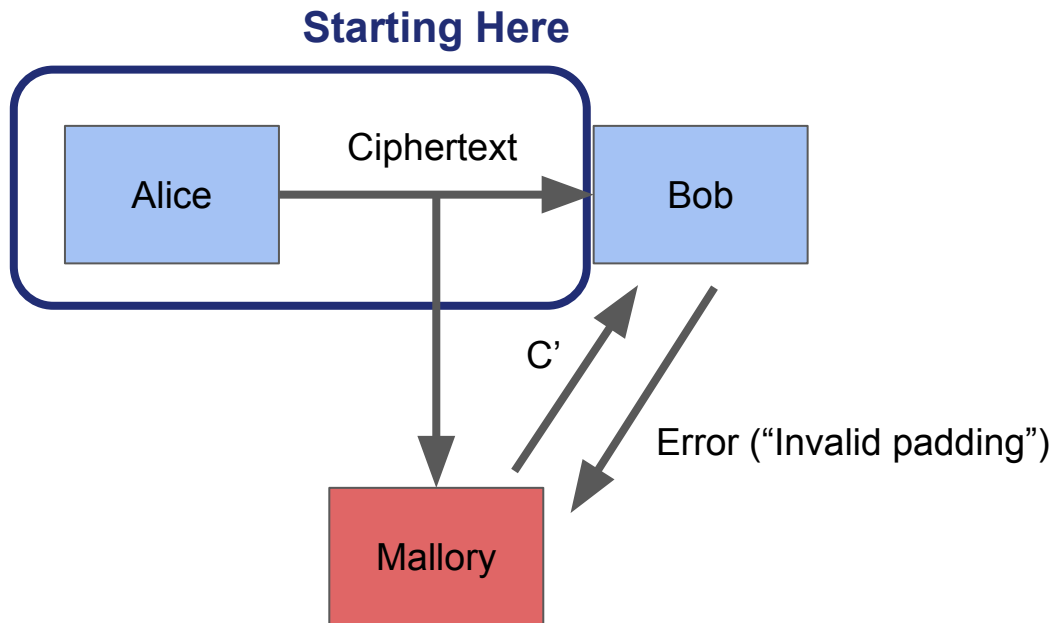


Alice's Encryption (cont.)



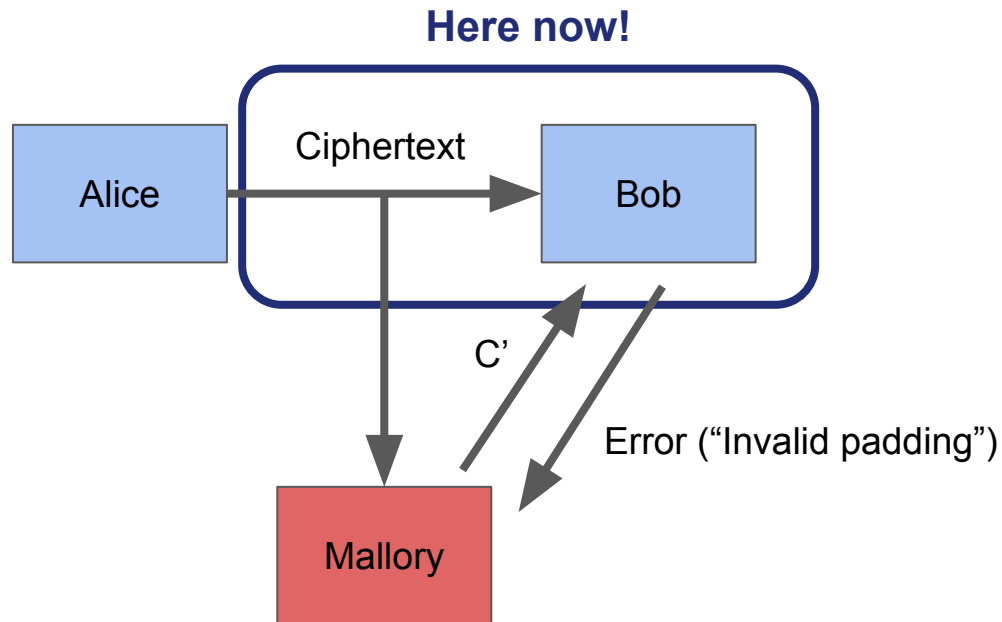
Premise

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



Premise

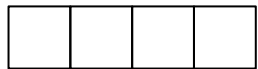
- Mallory initially only knows the ciphertext
- Mallory is able to query Bob to incrementally decrypt the ciphertext



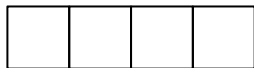
Ciphertext

ED	85	6E	F4	70	26	C6	AC	7B	2E	6A	00	91	0D	2D	5B
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Initialization Vector



Ciphertext

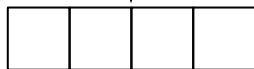


Key

Block
Cipher
Decryption

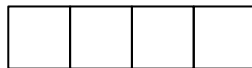


XOR



Plaintext

Ciphertext

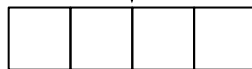


Key

Block
Cipher
Decryption

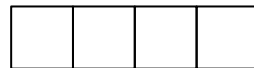


XOR



Plaintext

Ciphertext

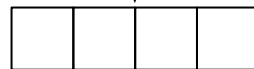


Key

Block
Cipher
Decryption



XOR



Plaintext

Bob's Decryption

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

Key

Block
Cipher
Decryption

XOR

Plaintext

Ciphertext

7B 2E 6A 00

Key

Block
Cipher
Decryption

XOR

Plaintext

Ciphertext

91 0D 2D 5B

Key

Block
Cipher
Decryption

XOR

Plaintext

Bob's Decryption (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

Alice and Bob
share *secret* key

XOR

XOR

XOR

Plaintext

Plaintext

Plaintext

Bob's Decryption (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

Decrypt first block

AA EA 4E B6

XOR

Plaintext

XOR

Plaintext

XOR

Plaintext

Bob's Decryption (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

Key

Block
Cipher
Decryption

AA EA 4E B6

XOR

47 6F 20 42

Plaintext

Ciphertext

7B 2E 6A 00

Key

Block
Cipher
Decryption

XOR

Plaintext

Ciphertext

91 0D 2D 5B

Key

Block
Cipher
Decryption

XOR

Plaintext

XOR with previous
block

Bob's Decryption (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

Continue for rest of
message

AA EA 4E B6

1C 53 A3 8C

5A 2D 69 03

XOR

XOR

XOR

47 6F 20 42

Plaintext

6C 75 65 20

Plaintext

21 03 03 03

Plaintext

Bob's Decryption (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

Key

Block
Cipher
Decryption

AA EA 4E B6

XOR

47 6F 20 42

Plaintext

Ciphertext

7B 2E 6A 00

Key

Block
Cipher
Decryption

1C 53 A3 8C

XOR

6C 75 65 20

Plaintext

Ciphertext

91 0D 2D 5B

Key

Block
Cipher
Decryption

5A 2D 69 03

XOR

21 03 03 03

Plaintext

Now have
plaintext!

Bob's Decryption (cont.)

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
----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----

Plaintext

47	6F	20	42	6C	75	65	20	21	03	03	03
----	----	----	----	----	----	----	----	----	----	----	----

Remove Padding

47	6F	20	42	6C	75	65	20	21
----	----	----	----	----	----	----	----	----

Decode (utf-8)

G	o	_	B	i	u	e	_	!
---	---	---	---	---	---	---	---	---

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...

Key

Block
Cipher
Decryption

Key

Block
Cipher
Decryption

Key

Block
Cipher
Decryption

Server will respond
with **Padding Error**
or **Padding Valid**

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
??	??	??	4B

Plaintext

Secret Plaintext

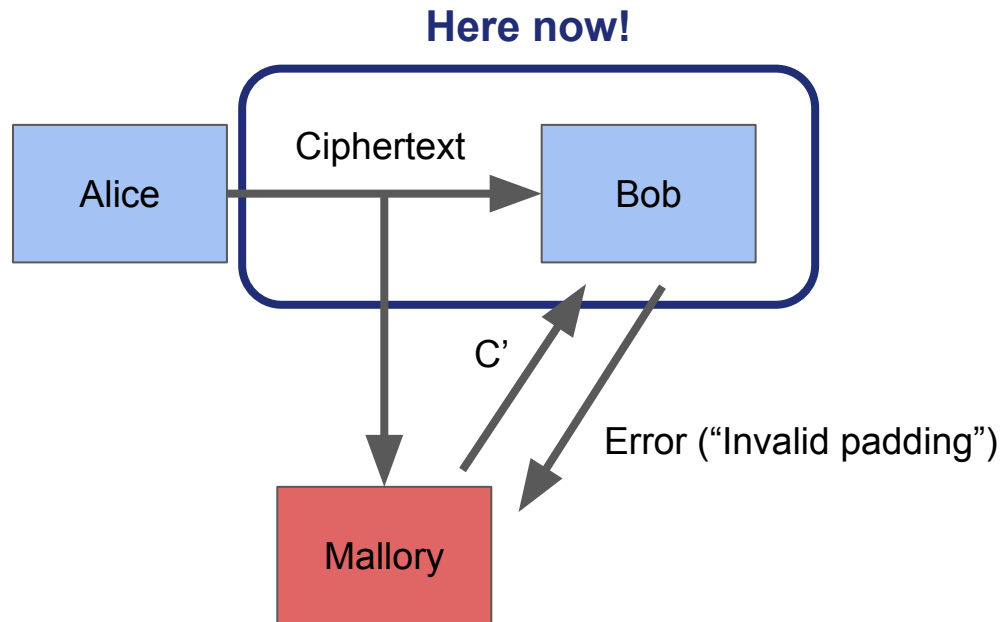
47	6F	20	42
----	----	----	----

6C	75	65	20
----	----	----	----

21	03	03	03
----	----	----	----

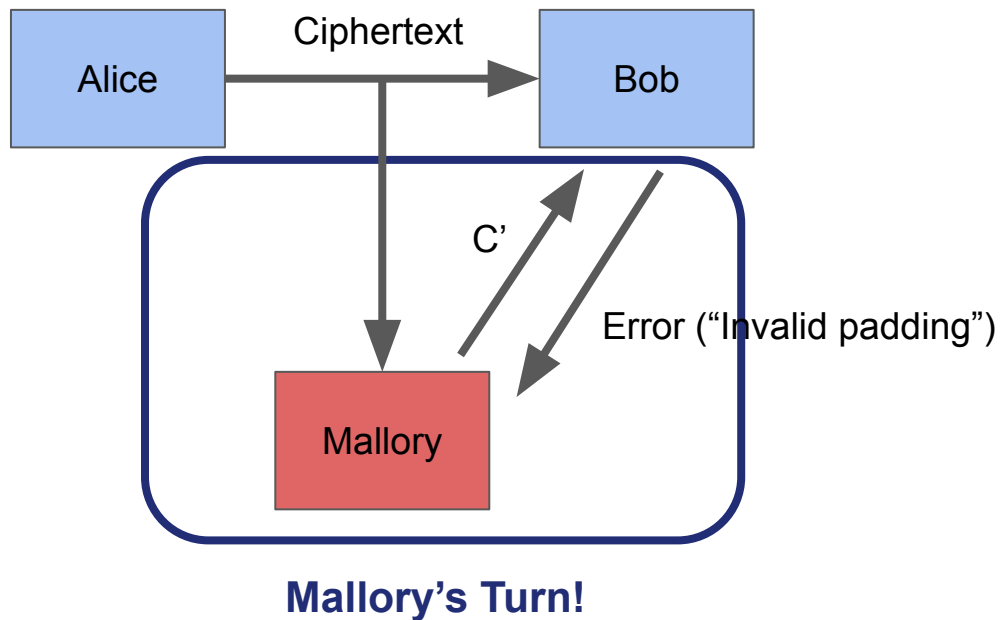
Premise

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



Premise

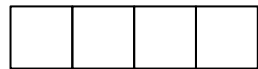
- Mallory initially only knows the ciphertext
- Mallory is able to query Bob to incrementally decrypt the ciphertext



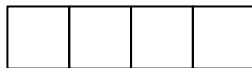
Ciphertext

ED 85 6E F4 70 26 C6 AC 7B 2E 6A 00 91 0D 2D 5B

Initialization Vector



Ciphertext

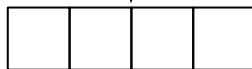


Key

Block
Cipher
Decryption

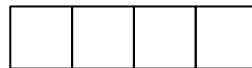


XOR



Plaintext

Ciphertext

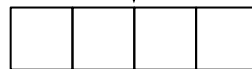


Key

Block
Cipher
Decryption

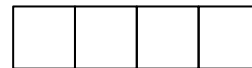


XOR



Plaintext

Ciphertext

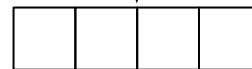


Key

Block
Cipher
Decryption



XOR



Plaintext

Mallory's Attack

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

Key

Block
Cipher
Decryption

XOR

Plaintext

Ciphertext

7B 2E 6A 00

Key

Block
Cipher
Decryption

XOR

Plaintext

Ciphertext

91 0D 2D 5B

Key

Block
Cipher
Decryption

XOR

Plaintext

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

Mallory does not
know the Key!

XOR

XOR

XOR

Plaintext

Plaintext

Plaintext

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

Key

Block
Cipher
Decryption

Can't decrypt any
block!

?? ?? ?? ??

XOR

?? ?? ?? ??

Plaintext

Ciphertext

7B 2E 6A 00

Key

Block
Cipher
Decryption

?? ?? ?? ??

XOR

?? ?? ?? ??

Plaintext

Ciphertext

91 0D 2D 5B

Key

Block
Cipher
Decryption

?? ?? ?? ??

XOR

?? ?? ?? ??

Plaintext

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

Key

Block
Cipher
Decryption

?? ?? ?? ??

XOR

?? ?? ?? ??

Plaintext

Ciphertext

7B 2E 6A 00

Key

Block
Cipher
Decryption

?? ?? ?? ??

XOR

?? ?? ?? ??

Plaintext

Ciphertext

91 0D 2D 5B

Key

Block
Cipher
Decryption

?? ?? ?? ??

XOR

?? ?? ?? ??

Plaintext

Padding Oracle
Attack time!

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
----	----	----	----

Key →

Block
Cipher
Decryption

??	??	??	??
----	----	----	----

XOR

??	??	??	??
----	----	----	----

Plaintext

Secret Plaintext

47	6F	20	42
----	----	----	----

Ciphertext

7B	2E	6A	00
----	----	----	----

Key →

Block
Cipher
Decryption

??	??	??	??
----	----	----	----

XOR

??	??	??	??
----	----	----	----

Plaintext

6C	75	65	20
----	----	----	----

Ciphertext

91	0D	2D	5B
----	----	----	----

Key →

Block
Cipher
Decryption

??	??	??	??
----	----	----	----

XOR

??	??	??	??
----	----	----	----

Plaintext

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

Key

Block
Cipher
Decryption

D5 D6 D7 D8
?? ?? ?? ??

XOR

P5 P6 P7 P8
?? ?? ?? ??

Plaintext

Secret Plaintext

47 6F 20 42

Ciphertext

C9 C10 C11 C12
7B 2E 6A 00

Key

Block
Cipher
Decryption

D9 D10 D11 D12
?? ?? ?? ??

XOR

P9 P10 P11 P12
?? ?? ?? ??

Plaintext

6C 75 65 20

Ciphertext

C13 C14 C15 C16
91 0D 2D 5B

Key

Block
Cipher
Decryption

D13 D14 D15 D16
?? ?? ?? ??

XOR

P13 P14 P15 P16
?? ?? ?? ??

Plaintext

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

Key

Block
Cipher
Decryption

D5 D6 D7 D8
?? ?? ?? ??

XOR

P5 P6 P7 P8
?? ?? ?? ??

Plaintext

Secret Plaintext

47 6F 20 42

Ciphertext

C9 C10 C11 C12
7B 2E 6A 00

Key

Block
Cipher
Decryption

D9 D10 D11 D12
?? ?? ?? ??

XOR

P9 P10 P11 P12
?? ?? ?? ??

Plaintext

6C 75 65 20

Ciphertext

C13 C14 C15 C16
91 0D 2D 5B

Key

Block
Cipher
Decryption

D13 D14 D15 D16
?? ?? ?? ??

XOR

P13 P14 P15 P16
?? ?? ?? ??

Plaintext

21 03 03 03

Want to find value
of P16

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

Try all values of c (0-255)
until you get valid padding

Ciphertext

C13	C14	C15	C16
91	0D	2D	5B

Key

Block
Cipher
Decryption

Key

Block
Cipher
Decryption

Key

Block
Cipher
Decryption

Can modify C12 to
change decrypted
value of P16

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

D13	D14	D15	D16
??	??	??	??

XOR

P13	P14	P15	P16
??	??	??	??

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

Change C12 to first "guess"

Note: Don't actually know value of P16' here

Key

Block Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Key

Block Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

Key

Block Cipher
Decryption

D13	D14	D15	D16
??	??	??	??

XOR

P13	P14	P15	P16
??	??	??	4B

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

Padding Error

Keep changing
C12...

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D13	D14	D15	D16
??	??	??	??

XOR

P13	P14	P15	P16
??	??	??	4B

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 7F

Ciphertext

C13 C14 C15 C16
91 0D 2D 5B

Padding Error

Key

Block
Cipher
Decryption

D5 D6 D7 D8
?? ?? ?? ??

XOR

P5 P6 P7 P8
?? ?? ?? ??

Plaintext

Key

Block
Cipher
Decryption

D9 D10 D11 D12
?? ?? ?? ??

XOR

P9 P10 P11 P12
?? ?? ?? ??

Plaintext

Key

Block
Cipher
Decryption

D13 D14 D15 D16
?? ?? ?? ??

XOR

P13 P14 P15 P16
?? ?? ?? 7C

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

Key

Block
Cipher
Decryption

D5 D6 D7 D8
?? ?? ?? ??

XOR

P5 P6 P7 P8
?? ?? ?? ??

Plaintext

Secret Plaintext

47 6F 20 42

Ciphertext

C9 C10 C11 C12
7B 2E 6A 6F

Key

Block
Cipher
Decryption

D9 D10 D11 D12
?? ?? ?? ??

XOR

P9 P10 P11 P12
?? ?? ?? ??

Plaintext

6C 75 65 20

Ciphertext

C13 C14 C15 C16
91 0D 2D 5B

Key

Block
Cipher
Decryption

D13 D14 D15 D16
?? ?? ?? ??

XOR

P13 P14 P15 P16
?? ?? ?? 6C

Plaintext

21 03 03 03

Padding Error

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

Padding is correct!

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

Secret Plaintext

47	6F	20	42
----	----	----	----

6C	75	65	20
----	----	----	----

21	03	03	03
----	----	----	----

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D13	D14	D15	D16
??	??	??	??

XOR

P13	P14	P15	P16
??	??	??	01

Plaintext

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

Key

Block
Cipher
Decryption

D5 D6 D7 D8
?? ?? ?? ??

XOR

P5 P6 P7 P8
?? ?? ?? ??

Plaintext

Secret Plaintext

47 6F 20 42

Ciphertext

C9 C10 C11 C12
7B 2E 6A 02

Key

Block
Cipher
Decryption

D9 D10 D11 D12
?? ?? ?? ??

XOR

P9 P10 P11 P12
?? ?? ?? ??

Plaintext

6C 75 65 20

Ciphertext

C13 C14 C15 C16
91 0D 2D 5B

Key

Block
Cipher
Decryption

D13 D14 D15 D16
?? ?? ?? ??

XOR

P13 P14 P15 P16
?? ?? ?? 01

Plaintext

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

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D13	D14	D15	D16
??	??	??	??

XOR

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

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

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D13	D14	D15	D16
??	??	??	??

XOR

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

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

$C12' = 0x02$

$P16' = 0x01$

$P16' = C12' \oplus D16$

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D13	D14	D15	D16
??	??	??	??

XOR

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

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

$C12' = 0x02$

$P16' = 0x01$

$P'16 = C12' \oplus D16$

$D16 = C12' \oplus P'16$

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D13	D14	D15	D16
??	??	??	??

XOR

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

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

$C12' = 0x02$

$P16' = 0x01$

$P'16 = C12' \oplus D16$

$D16 = C12' \oplus P'16$

$D16 = 0x02 \oplus 0x01$

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D13	D14	D15	D16
??	??	??	??

XOR

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

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

$C12' = 0x02$

$P16' = 0x01$

$P'16 = C12' \oplus D16$

$D16 = C12' \oplus P'16$

$D16 = 0x02 \oplus 0x01$

$D16 = 0x03$

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D13	D14	D15	D16
??	??	??	03

XOR

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

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

$C12' = 0x02$

$P16' = 0x01$

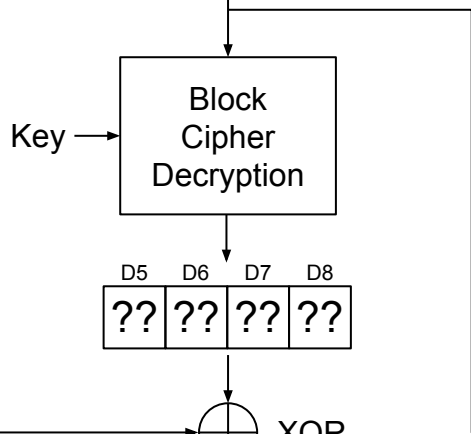
$P'16 = C12' \oplus D16$

$D16 = C12' \oplus P'16$

$D16 = 0x02 \oplus 0x01$

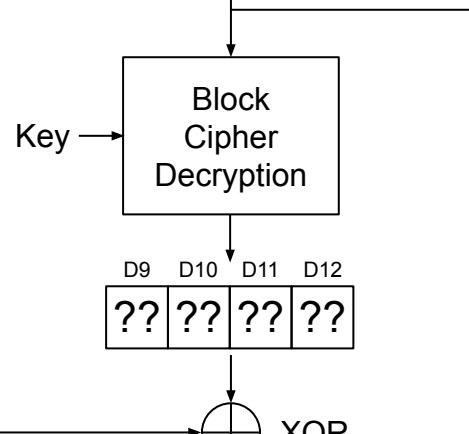
$D16 = 0x03$

$P16 = D16 \oplus C12$



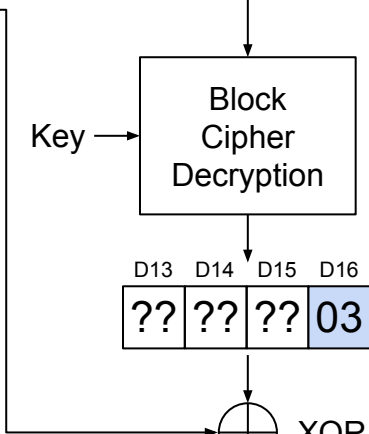
Plaintext

47	6F	20	42
----	----	----	----



Plaintext

6C	75	65	20
----	----	----	----



Plaintext

21	03	03	03
----	----	----	----

Secret Plaintext

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

$C12' = 0x02$

$P16' = 0x01$

$P'16 = C12' \oplus D16$

$D16 = C12' \oplus P'16$

$D16 = 0x02 \oplus 0x01$

$D16 = 0x03$

$P16 = D16 \oplus C12$

Secret Plaintext

47	6F	20	42
----	----	----	----

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D13	D14	D15	D16
??	??	??	03

XOR

P13	P14	P15	P16
??	??	??	01

Plaintext

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

$C12' = 0x02$

$P16' = 0x01$

$P'16 = C12' \oplus D16$

$D16 = C12' \oplus P'16$

$D16 = 0x02 \oplus 0x01$

$D16 = 0x03$

$P16 = D16 \oplus C12$

Secret Plaintext

47	6F	20	42
----	----	----	----

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D13	D14	D15	D16
??	??	??	03

XOR

P13	P14	P15	P16
??	??	??	03

Plaintext

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

Key

Block
Cipher
Decryption

D5 D6 D7 D8
?? ?? ?? ??

XOR

P5 P6 P7 P8
?? ?? ?? ??

Plaintext

Secret Plaintext

47 6F 20 42

Ciphertext

C9 C10 C11 C12
7B 2E 6A 00

Key

Block
Cipher
Decryption

D9 D10 D11 D12
?? ?? ?? ??

XOR

P9 P10 P11 P12
?? ?? ?? ??

Plaintext

6C 75 65 20

Ciphertext

C13 C14 C15 C16
91 0D 2D 5B

Key

Block
Cipher
Decryption

D13 D14 D15 D16
?? ?? ?? 03

XOR

P13 P14 P15 P16
?? ?? ?? 03

Plaintext

21 03 03 03

Want to find value
of P15

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

Need to force P16
to be 0x02 to get a
valid padding with
P15

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

D13	D14	D15	D16
??	??	??	03

XOR

P13	P14	P15	P16
??	??	??	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

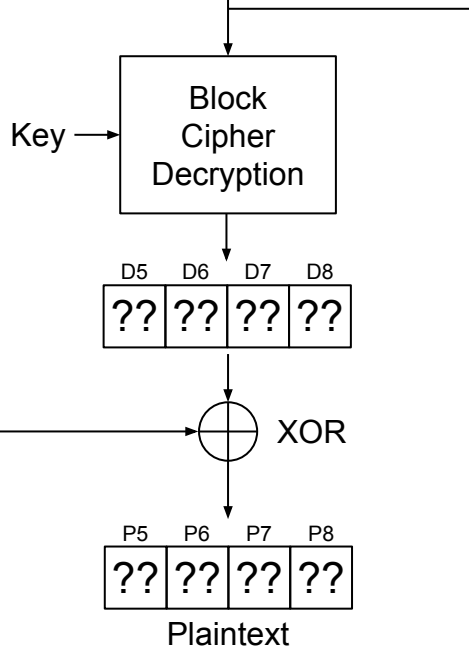
C13	C14	C15	C16
91	0D	2D	5B

$$P16' = D16 \oplus C12''$$

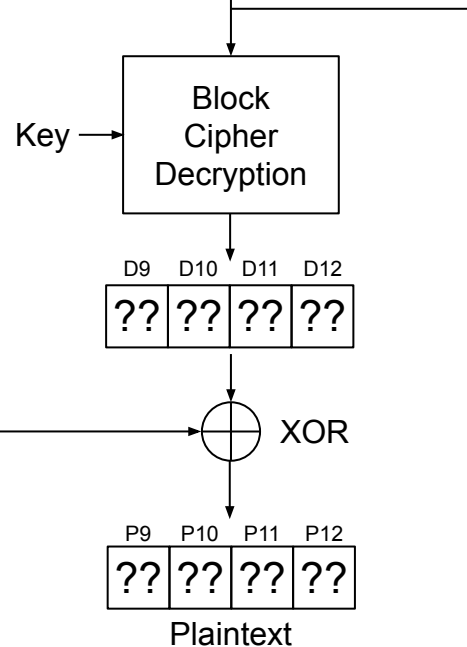
We know P16' and D16!

$$C12'' = D16 \oplus P16'$$

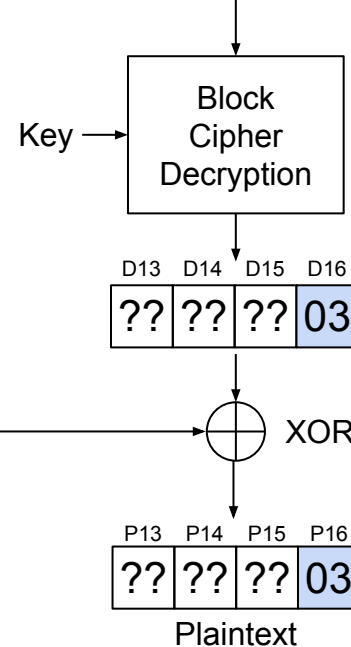
$$C12'' = 0x03 \oplus 0x02$$



47	6F	20	42
----	----	----	----



6C	75	65	20
----	----	----	----



21	03	03	03
----	----	----	----

Secret Plaintext

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

$$P16' = D16 \oplus C12''$$

We know P16' and D16!

$$C12'' = D16 \oplus P16'$$

$$C12'' = 0x03 \oplus 0x02$$

Ciphertext

C5	C6	C7	C8
70	26	C6	AC

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Secret Plaintext

47	6F	20	42
----	----	----	----

Ciphertext

C9	C10	C11	C12
7B	2E	6A	01

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

6C	75	65	20
----	----	----	----

Ciphertext

C13	C14	C15	C16
91	0D	2D	5B

Key

Block
Cipher
Decryption

D13	D14	D15	D16
??	??	??	03

XOR

P13	P14	P15	P16
??	??	??	02

Plaintext

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

Padding Error

Key

Block
Cipher
Decryption

D5 D6 D7 D8
?? ?? ?? ??

XOR

P5 P6 P7 P8
?? ?? ?? ??

Plaintext

Key

Block
Cipher
Decryption

D9 D10 D11 D12
?? ?? ?? ??

XOR

P9 P10 P11 P12
?? ?? ?? ??

Plaintext

Key

Block
Cipher
Decryption

D13 D14 D15 D16
?? ?? ?? 03

XOR

P13 P14 P15 P16
?? ?? EE 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

Key

Block
Cipher
Decryption

D5 D6 D7 D8
?? ?? ?? ??

XOR

P5 P6 P7 P8
?? ?? ?? ??

Plaintext

Ciphertext

C9 C10 C11 C12
7B 2E 26 01

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
?? ?? ?? 03

XOR

P13 P14 P15 P16
?? ?? 4F 02

Plaintext

Padding Error

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

Key

Block
Cipher
Decryption

D5 D6 D7 D8
?? ?? ?? ??

XOR

P5 P6 P7 P8
?? ?? ?? ??

Plaintext

Ciphertext

C9 C10 C11 C12
7B 2E 6B 01

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
?? ?? ?? 03

XOR

P13 P14 P15 P16
?? ?? 02 02

Plaintext

Padding Valid

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

Padding Valid

Find D15 and P15

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

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

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

Secret Plaintext

47 6F 20 42

Ciphertext

C9 C10 C11 C12
7B 2E 6A 00

Key

Block
Cipher
Decryption

D9 D10 D11 D12
?? ?? ?? ??

XOR

P9 P10 P11 P12
?? ?? ?? ??

Plaintext

6C 75 65 20

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

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
?? ?? ?? ??

P9 P10 P11 P12
?? ?? ?? ??

P13 P14 P15 P16
?? 3E 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

Padding Valid

Key

Block
Cipher
Decryption

D5 D6 D7 D8
?? ?? ?? ??

XOR

P5 P6 P7 P8
?? ?? ?? ??

Plaintext

Key

Block
Cipher
Decryption

D9 D10 D11 D12
?? ?? ?? ??

XOR

P9 P10 P11 P12
?? ?? ?? ??

Plaintext

Key

Block
Cipher
Decryption

D13 D14 D15 D16
?? ?? 69 03

XOR

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

Finish the block

Ciphertext

C5 C6 C7 C8
70 26 C6 AC

Key

Block
Cipher
Decryption

D5 D6 D7 D8
?? ?? ?? ??

XOR

P5 P6 P7 P8
?? ?? ?? ??

Plaintext

Secret Plaintext

47 6F 20 42

Ciphertext

C9 C10 C11 C12
7B 2E 6A 00

Key

Block
Cipher
Decryption

D9 D10 D11 D12
?? ?? ?? ??

XOR

P9 P10 P11 P12
?? ?? ?? ??

Plaintext

6C 75 65 20

Ciphertext

C13 C14 C15 C16
91 0D 2D 5B

Key

Block
Cipher
Decryption

D13 D14 D15 D16
5A 2D 69 03

XOR

P13 P14 P15 P16
21 03 03 03

Plaintext

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

After a block is done, we can “chop it off”, and move on to the previous one

Ciphertext

C5	C6	C7	C8
70	26	C6	AC

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Secret Plaintext

47	6F	20	42
----	----	----	----

Ciphertext

C9	C10	C11	C12
7B	2E	6A	00

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

6C	75	65	20
----	----	----	----

Ciphertext

C13	C14	C15	C16
91	0D	2D	5B

Key

Block
Cipher
Decryption

D13	D14	D15	D16
5A	2D	69	03

XOR

P13	P14	P15	P16
21	03	03	03

Plaintext

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

Change C8 until
P12 becomes
0x01

(Only send
C1–C12 to the
server, so P12 is
the final byte)

Secret Plaintext

Ciphertext

C5	C6	C7	C8
70	26	C6	AC

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

47	6F	20	42
----	----	----	----

Ciphertext

C9	C10	C11	C12
7B	2E	6A	00

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

6C	75	65	20
----	----	----	----

Ciphertext

C13	C14	C15	C16
91	0D	2D	5B

Key

Block
Cipher
Decryption

D13	D14	D15	D16
5A	2D	69	03

XOR

P13	P14	P15	P16
21	03	03	03

Plaintext

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

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Secret Plaintext

47	6F	20	42
----	----	----	----

Ciphertext

C9	C10	C11	C12
7B	2E	6A	00

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	01

Plaintext

6C	75	65	20
----	----	----	----

Ciphertext

C13	C14	C15	C16
91	0D	2D	5B

Key

Block
Cipher
Decryption

D13	D14	D15	D16
5A	2D	69	03

XOR

P13	P14	P15	P16
21	03	03	03

Plaintext

21	03	03	03
----	----	----	----

Padding Valid

Calculate D12 and
P12

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

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Secret Plaintext

47	6F	20	42
----	----	----	----

Ciphertext

C9	C10	C11	C12
7B	2E	6A	00

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	8C

XOR

P9	P10	P11	P12
??	??	??	20

Plaintext

6C	75	65	20
----	----	----	----

Ciphertext

C13	C14	C15	C16
91	0D	2D	5B

Key

Block
Cipher
Decryption

D13	D14	D15	D16
5A	2D	69	03

XOR

P13	P14	P15	P16
21	03	03	03

Plaintext

21	03	03	03
----	----	----	----

Padding Valid

Calculate D12 and
P12

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

Repeat for each
block...

D5	D6	D7	D8
AA	EA	4E	B6

XOR

P5	P6	P7	P8
47	6F	20	42

Plaintext

D9	D10	D11	D12
1C	53	A3	8C

XOR

P9	P10	P11	P12
6C	75	65	20

Plaintext

D13	D14	D15	D16
5A	2D	69	03

XOR

P13	P14	P15	P16
21	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

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

P9 P10 P11 P12
6C 75 65 20

P13 P14 P15 P16
21 03 03 03

Plaintext

Plaintext

Plaintext

We now know the
Secret Plaintext!

Secret Plaintext

47 6F 20 42

6C 75 65 20

21 03 03 03

Tricky Edge Case

- What if one of the blocks of Plaintext is

ED	85	02	FF
----	----	----	----

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

ED	85	02	01
----	----	----	----

ED	85	02	02
----	----	----	----

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

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

Secret Plaintext

47	6F	20	42
----	----	----	----

Ciphertext

C9	C10	C11	C12
7B	2E	6A	00

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
??	??	??	??

Plaintext

ED	85	02	FF
----	----	----	----

Ciphertext

C13	C14	C15	C16
91	0D	2D	5B

Key

Block
Cipher
Decryption

D13	D14	D15	D16
5A	2D	69	03

XOR

P13	P14	P15	P16
21	03	03	03

Plaintext

21	03	03	03
----	----	----	----

Already found
P13–P16

Want to find P12...

Start changing C8

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

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

47	6F	20	42
----	----	----	----

Secret Plaintext

Ciphertext

C9	C10	C11	C12
7B	2E	6A	00

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
ED	85	02	01

Plaintext

ED	85	02	FF
----	----	----	----

Ciphertext

C13	C14	C15	C16
91	0D	2D	5B

Key

Block
Cipher
Decryption

D13	D14	D15	D16
5A	2D	69	03

XOR

P13	P14	P15	P16
21	03	03	03

Plaintext

21	03	03	03
----	----	----	----

Padding Valid

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

Key

Block
Cipher
Decryption

D5	D6	D7	D8
??	??	??	??

XOR

P5	P6	P7	P8
??	??	??	??

Plaintext

47	6F	20	42
----	----	----	----

Secret Plaintext

Ciphertext

C9	C10	C11	C12
7B	2E	6A	00

Key

Block
Cipher
Decryption

D9	D10	D11	D12
??	??	??	??

XOR

P9	P10	P11	P12
ED	85	02	02

Plaintext

ED	85	02	FF
----	----	----	----

Ciphertext

C13	C14	C15	C16
91	0D	2D	5B

Key

Block
Cipher
Decryption

D13	D14	D15	D16
5A	2D	69	03

XOR

P13	P14	P15	P16
21	03	03	03

Plaintext

21	03	03	03
----	----	----	----

Padding Valid

(still!)

How can we
prevent this?

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

Bleichenbacher Attack (RSA Signature Forgery)

Textbook RSA Signatures

Signing

$$s = m^d \pmod{n}$$

Diagram illustrating the signing process:

- s : signature
- m : message to be signed
- d : private exponent
- n : public modulus

Verifying

$$s^e = m \pmod{n}$$

Diagram illustrating the verification process:

- s : signature
- m : message that was signed
- e : public exponent
- n : public modulus

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 confidentially with RSA



(m, s)



She sends *both* the message
and the signature



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

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

What if e is really small, like, 3?

Bleichenbacher Attack: Vulnerability 2

- How should a secure bank's operations work?



$m = \text{"gimme some \$\$\$"}$

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



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

Bleichenbacher Attack: Vulnerability 2

- How do the bank's operations actually work?



$m = \text{"gimme some \$\$\$"}$

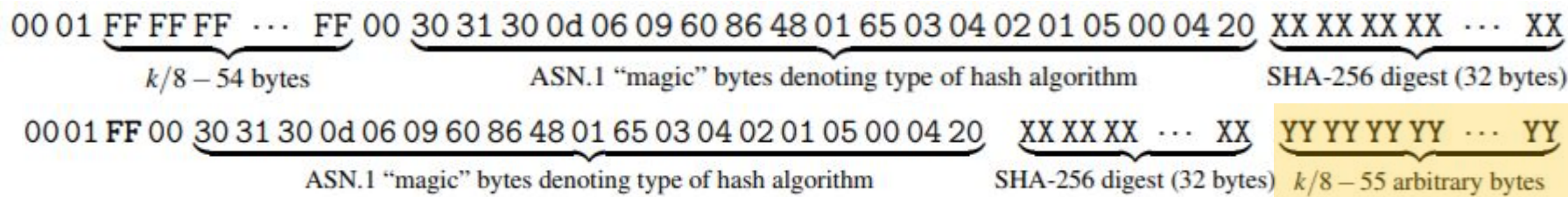
$$s = (\text{PKCS-PAD}(m))^d \bmod N$$



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

Bleichenbacher Attack

What the result of the signature verification should look like ($s^e \bmod N$)



Format of PKCS-PAD(m) above.

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

Accepted due to poor implementation

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 $m \pmod n$?
 - How does the "lazy implementation" of checking signatures help with this?

Signing

$$s = m^d \pmod n$$

Diagram labels for Signing:

- signature: points to s
- private exponent: points to d
- public modulus: points to n
- message to be signed: points to m

Verifying

$$s^e = m \pmod n$$

Diagram labels for Verifying:

- signature: points to s
- public exponent: points to e
- public modulus: points to n
- message that was signed: points to m



See you next week!