Course: Modern Cryptography

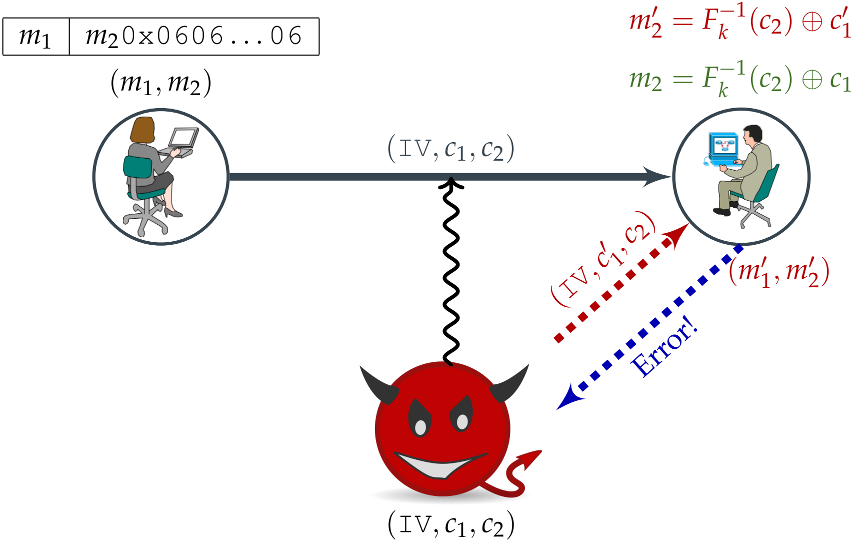
CCA Security

Shashank Singh

IISER Bhopal

September 17, 2025

Padding-Oracle Attack[1]



m_1 | $m_2$0x0606...06

(m_1, m_2)

$(\mathtt{IV}, c_1, c_2)$

$m_2' = F_k^{-1}(c_2) \oplus c_1'$

$m_2 = F_k^{-1}(c_2) \oplus c_1$

$(\mathtt{IV}, c_1', c_2)$

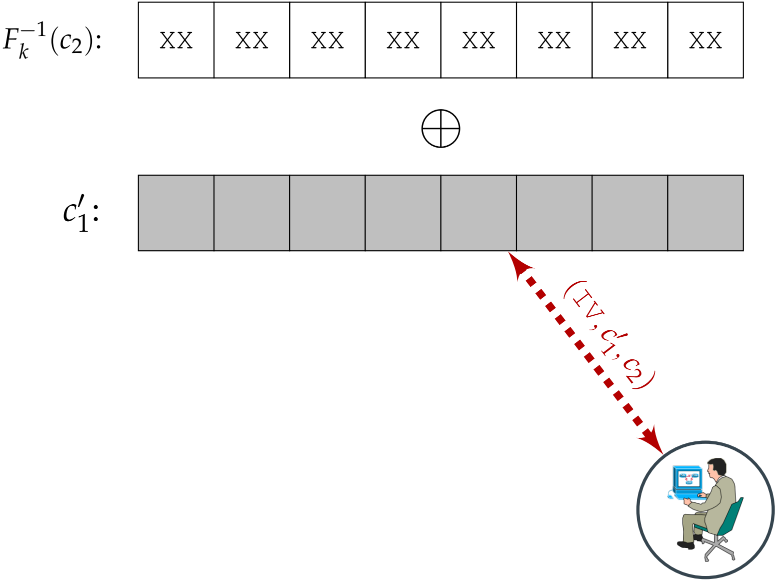
(m_1', m_2')

Error!

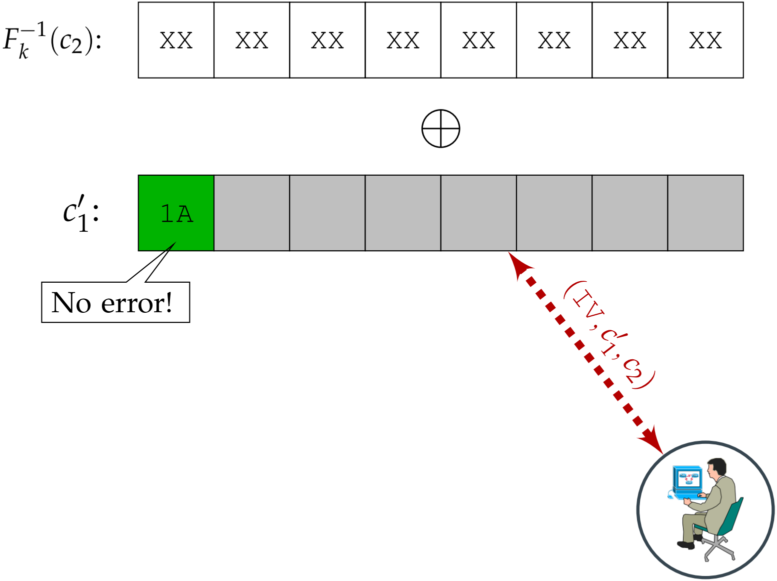
$(\mathtt{IV}, c_1, c_2)$

[1] Thanks Prof. Katz for this example.

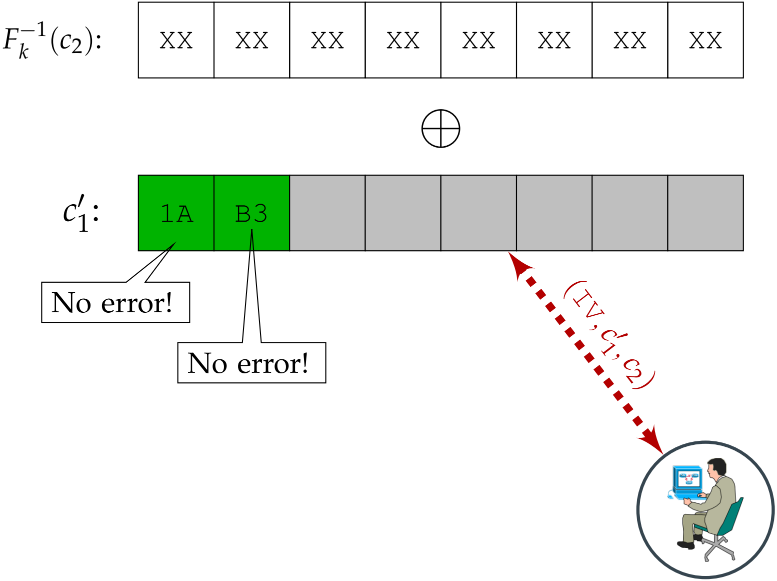
Padding-Oracle Attack..



Padding-Oracle Attack..



Padding-Oracle Attack..



$F_k^{-1}(c_2)$: XX XX XX XX XX XX XX XX

$\oplus$

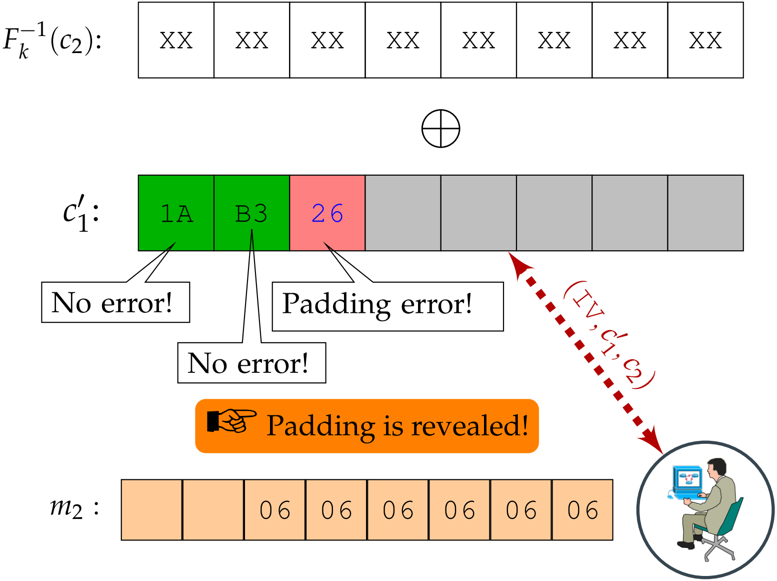
c_1': 1A B3

No error!

No error!

(IV, c_1', c_2)

Padding-Oracle Attack..



$F_k^{-1}(c_2)$:

XX	XX	XX	XX	XX	XX	XX	XX

$\oplus$

c'_1:

1A	B3	26					

No error!

No error!

Padding error!

(IV, c'_1, c_2)

☞ Padding is revealed!

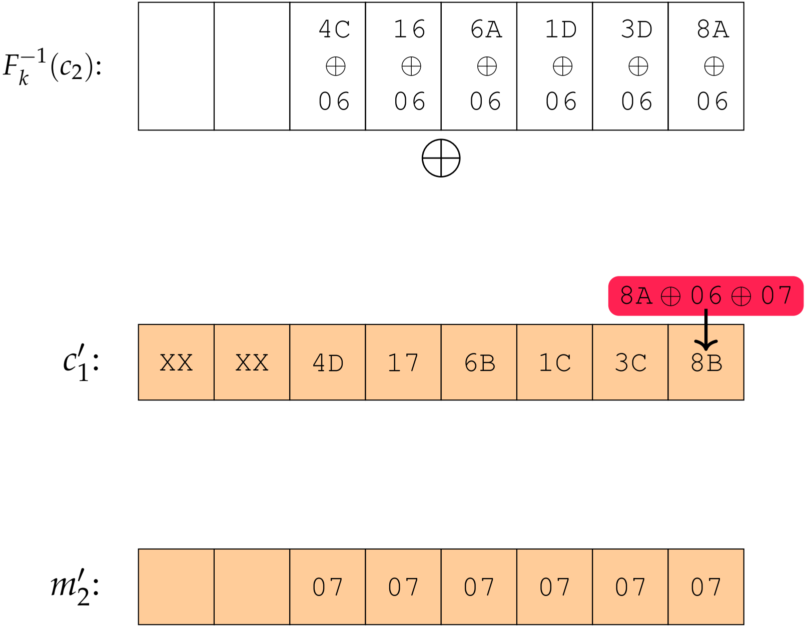
m_2 :

		06	06	06	06	06	06

Padding-Oracle Attack..

$F_k^{-1}(c_2)$:			4C ⊕ 06	16 ⊕ 06	6A ⊕ 06	1D ⊕ 06	3D ⊕ 06	8A ⊕ 06
				⊕				
c_1:	3A	AB	4C	16	6A	1D	3D	8A
m_2:			06	06	06	06	06	06

Padding-Oracle Attack..



$F_k^{-1}(c_2)$:			4C ⊕ 06	16 ⊕ 06	6A ⊕ 06	1D ⊕ 06	3D ⊕ 06	8A ⊕ 06
c_1':	XX	XX	4D	17	6B	1C	3C	8B
m_2':			07	07	07	07	07	07

$\oplus$

8A ⊕ 06 ⊕ 07

Padding-Oracle Attack..

$F_k^{-1}(c_2)$:			4C $\oplus$ 06	16 $\oplus$ 06	6A $\oplus$ 06	1D $\oplus$ 06	3D $\oplus$ 06	8A $\oplus$ 06

$$\oplus$$

☞ We query the padding oracle for all possibilities for second byte of c_1'. No error reveals the second byte of $F_k^{-1}(c_2)$ and hence of m_2.

c_1':	XX	XX	4D	17	6B	1C	3C	8B

☞ Similarly we can obtail the first byte of m_2 as well.

m_2':			07	07	07	07	07	07