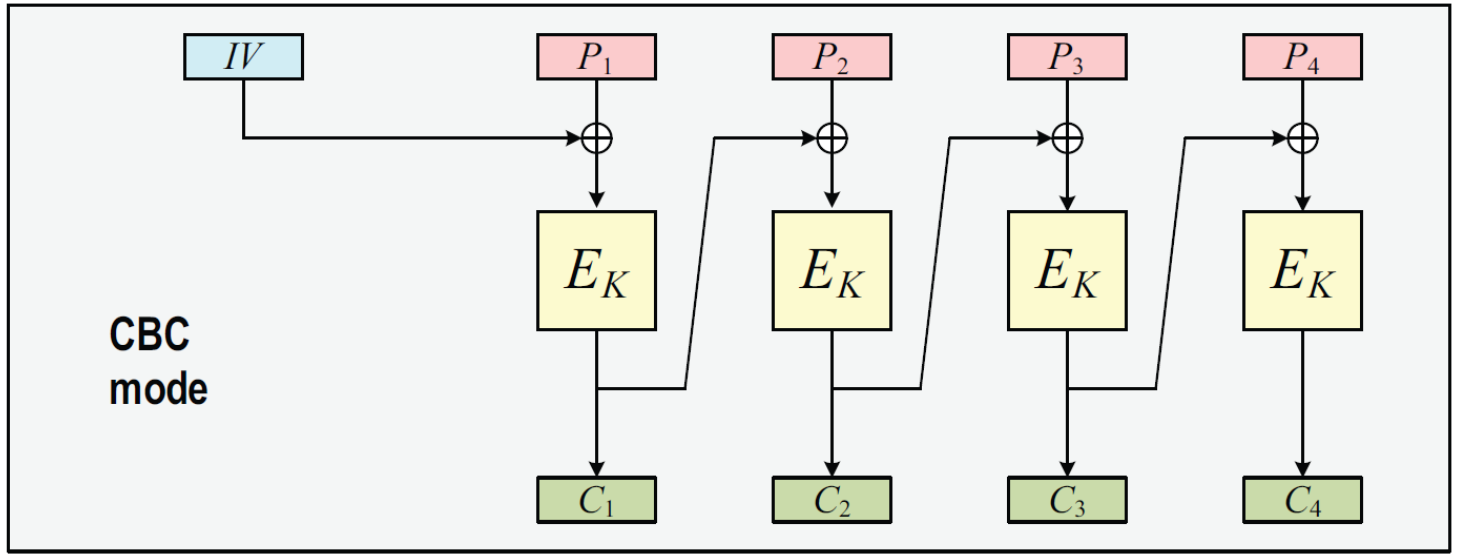
Padding Oracle Attack

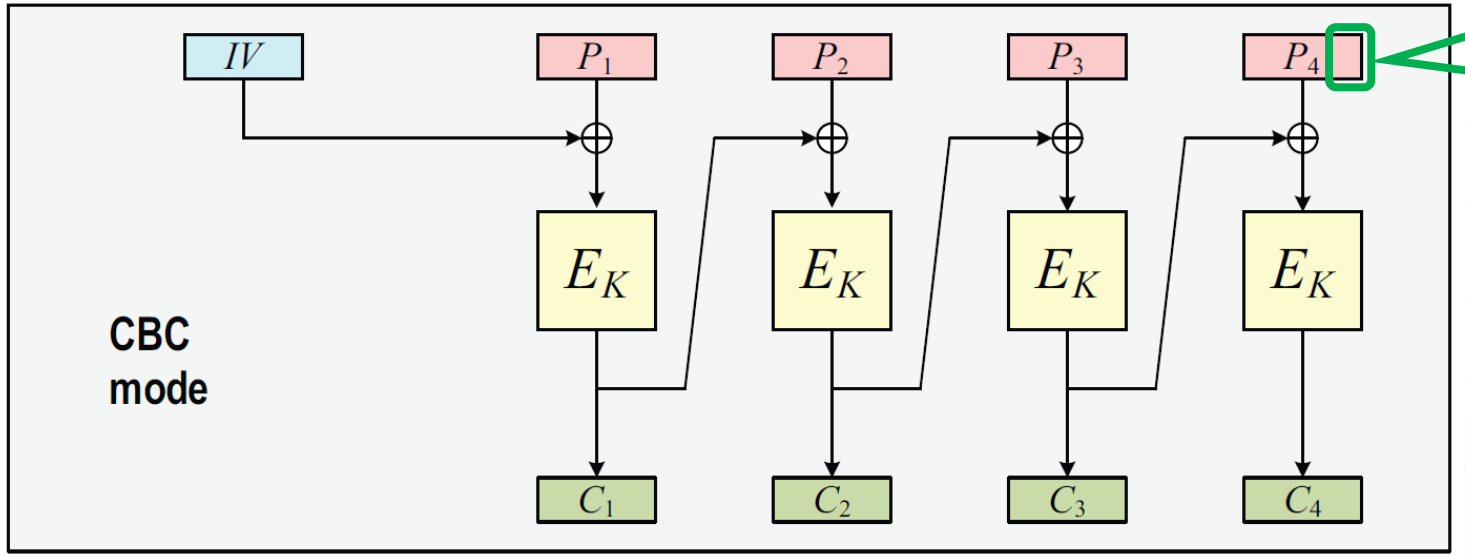
Chanathip Namprempre

Recall CBC Mode



Source of all drawings of modes: https://www.cs.ucdavis.edu/~rogaway/papers/modes.pdf

CBC Mode with Padding (simplified)



0x03 0x03 0x03
if padding with 3 bytes

Valid pads:

- 0x01
- 0x02 0x02
- 0x03 0x03 0x03
- …

Source of all drawings of modes: https://www.cs.ucdavis.edu/~rogaway/papers/modes.pdf

Padding Oracle Attack: Formal Definition

Source:

Bellare and Rogaway, unpublished notes.

Game $\mathrm{POA}_{\mathcal{SE}}$

procedure Initialize

$K \xleftarrow{\$} \mathcal{K}$; $M^* \xleftarrow{\$} \{0,1\}^n$

Return $\mathcal{E}_K(M^*)$

procedure CheckPad(C)

$M \leftarrow \mathcal{D}_K(C)$

If $M \neq \perp$ then Return 1

Return 0

procedure Finalize(M)

Return $(M^* = M)$

Fun Video: CBC padding oracle attack

Attacking Modern Cryptography

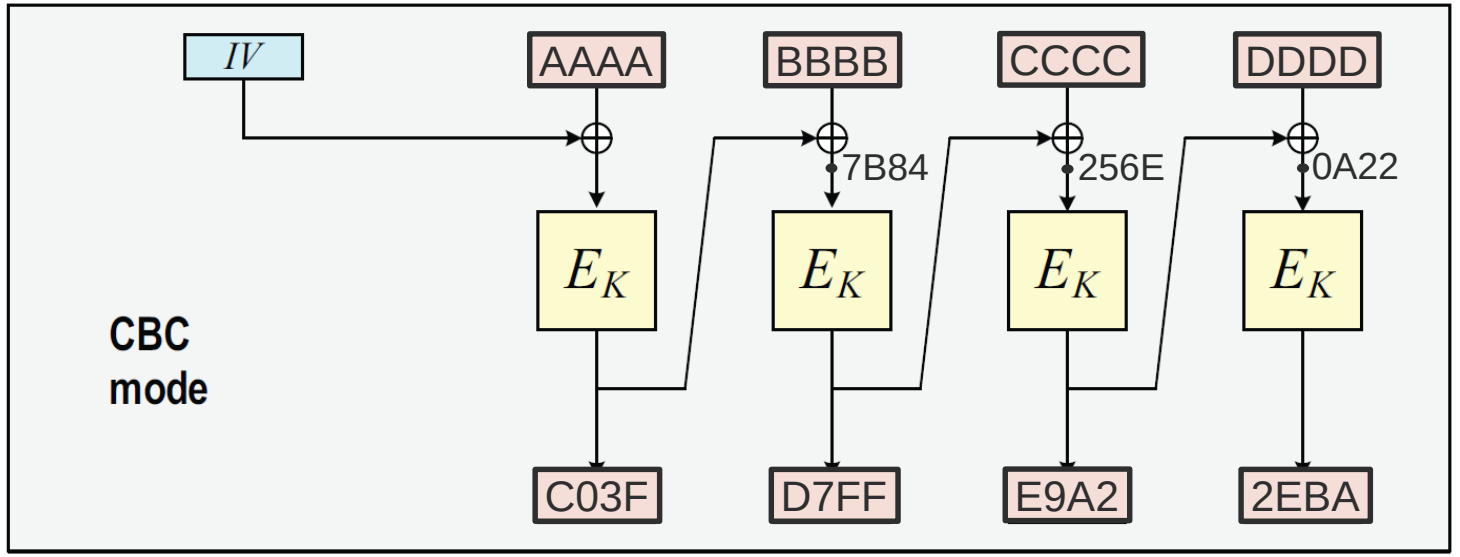
https://youtu.be/8Tr2aj6JETg

3:57

By Pastie's Bin

(Recommendation: watch it at reduced speed!)

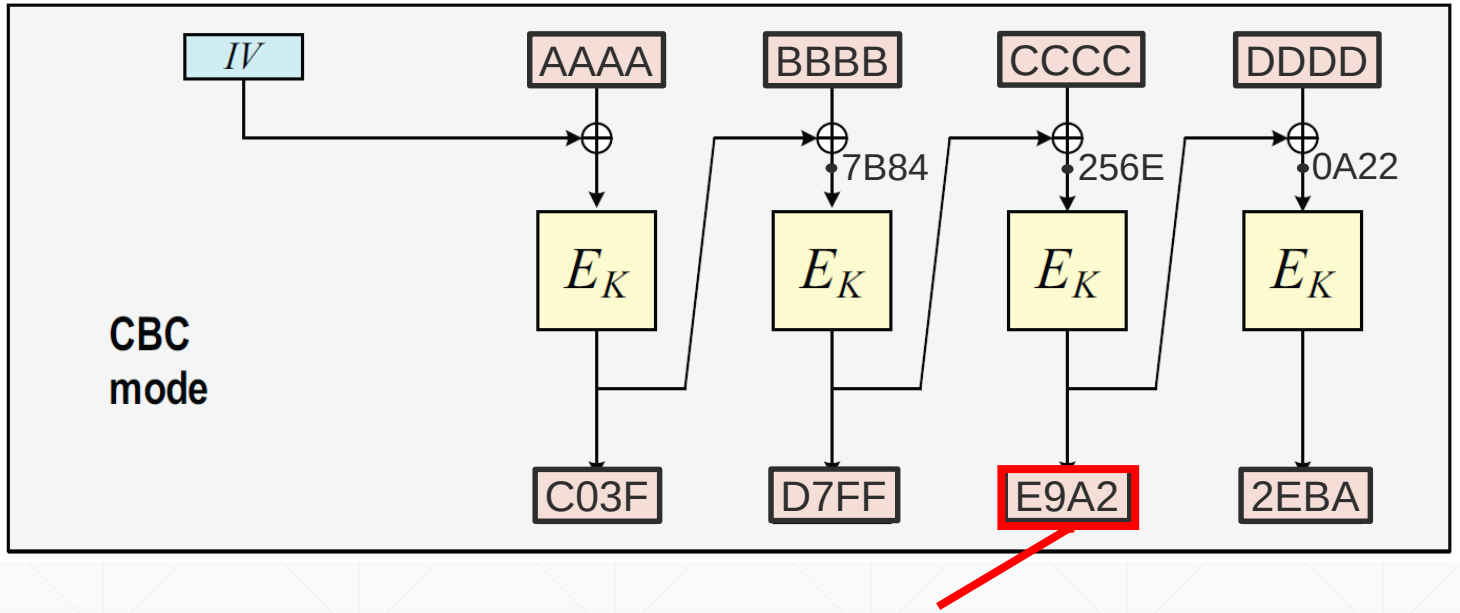
Redrawing pictures from the video



The video does not show the IV.

Source of all drawings of modes: https://www.cs.ucdavis.edu/~rogaway/papers/modes.pdf

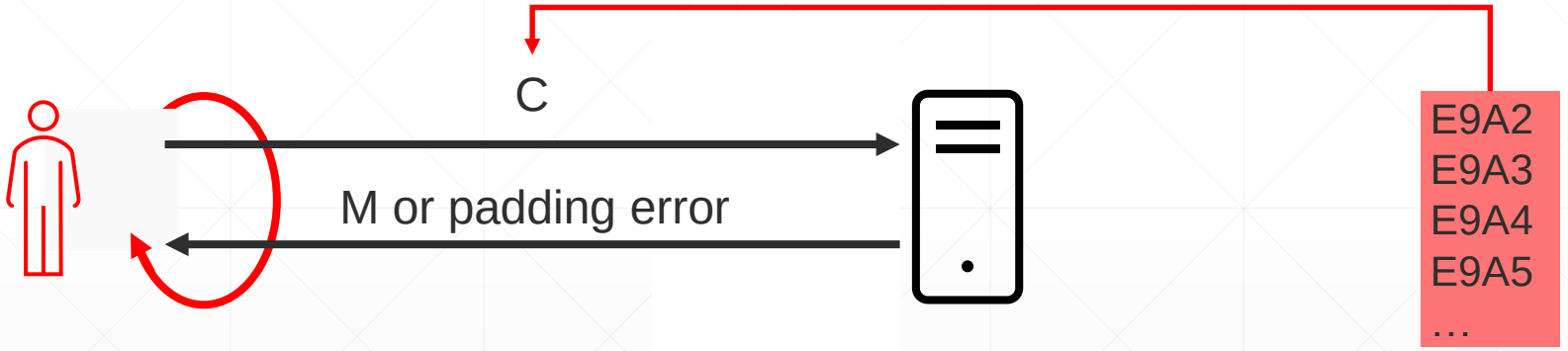
Redrawing pictures from the video



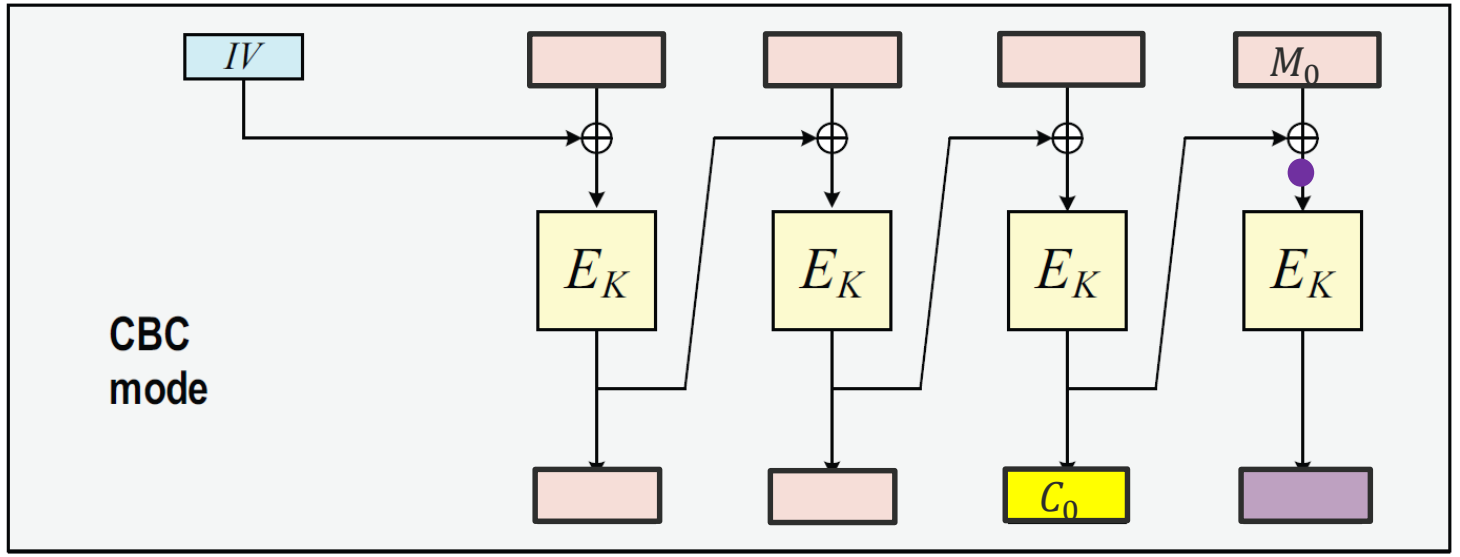
In the video, we cycle through this value one by one from right to left.

Source of all drawings of modes: https://www.cs.ucdavis.edu/~rogaway/papers/modes.pdf

What does a padding oracle attack look like?

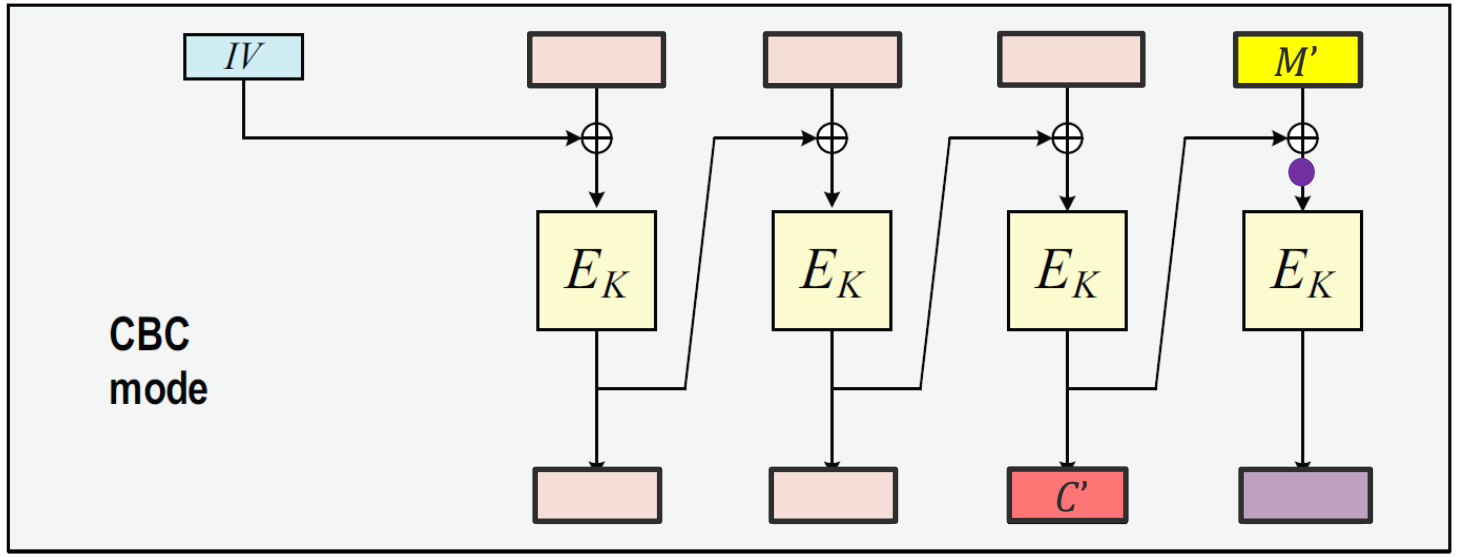


We want to find M_0



Source of all drawings of modes: https://www.cs.ucdavis.edu/~rogaway/papers/modes.pdf

The Main Point



We control this!

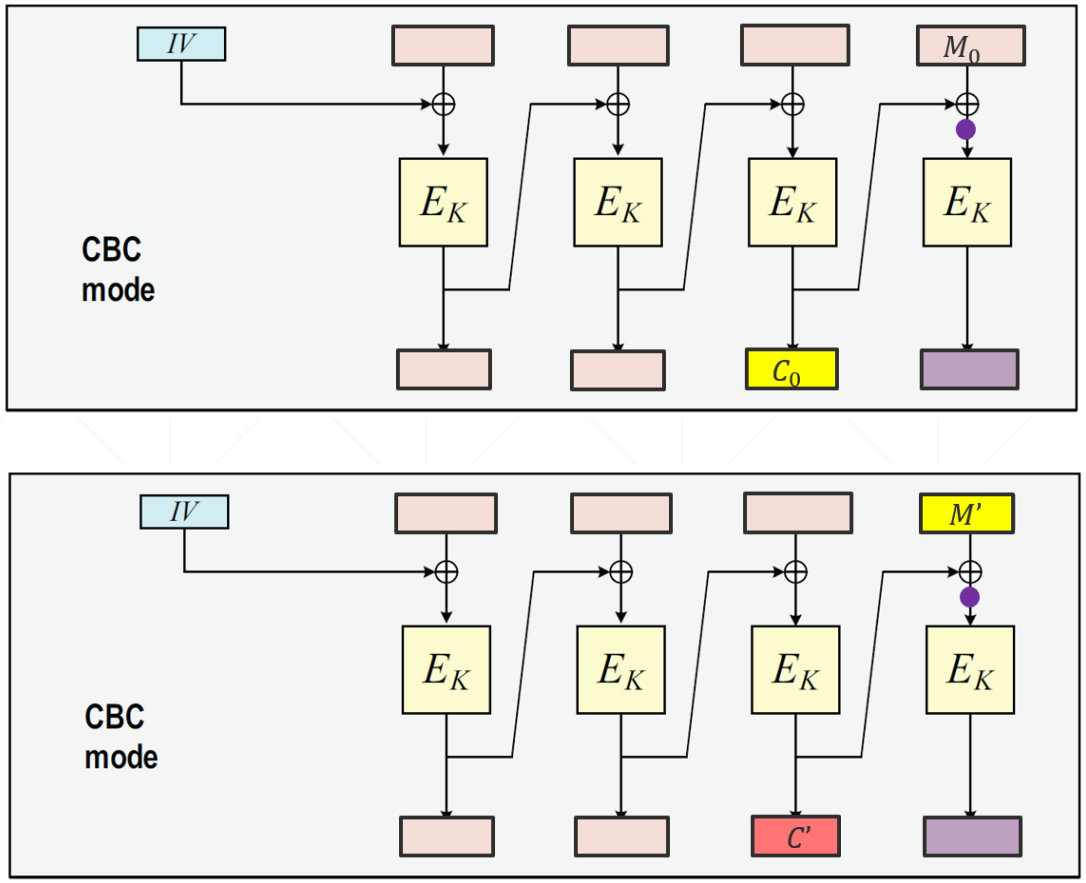
$C_0 \oplus M_0 = C' \oplus M'$

We want to know this!

We know these!

Source of all drawings of modes: https://www.cs.ucdavis.edu/~rogaway/papers/modes.pdf

In summary



We control this!

$C_0 \oplus M_0 = C' \oplus M'$

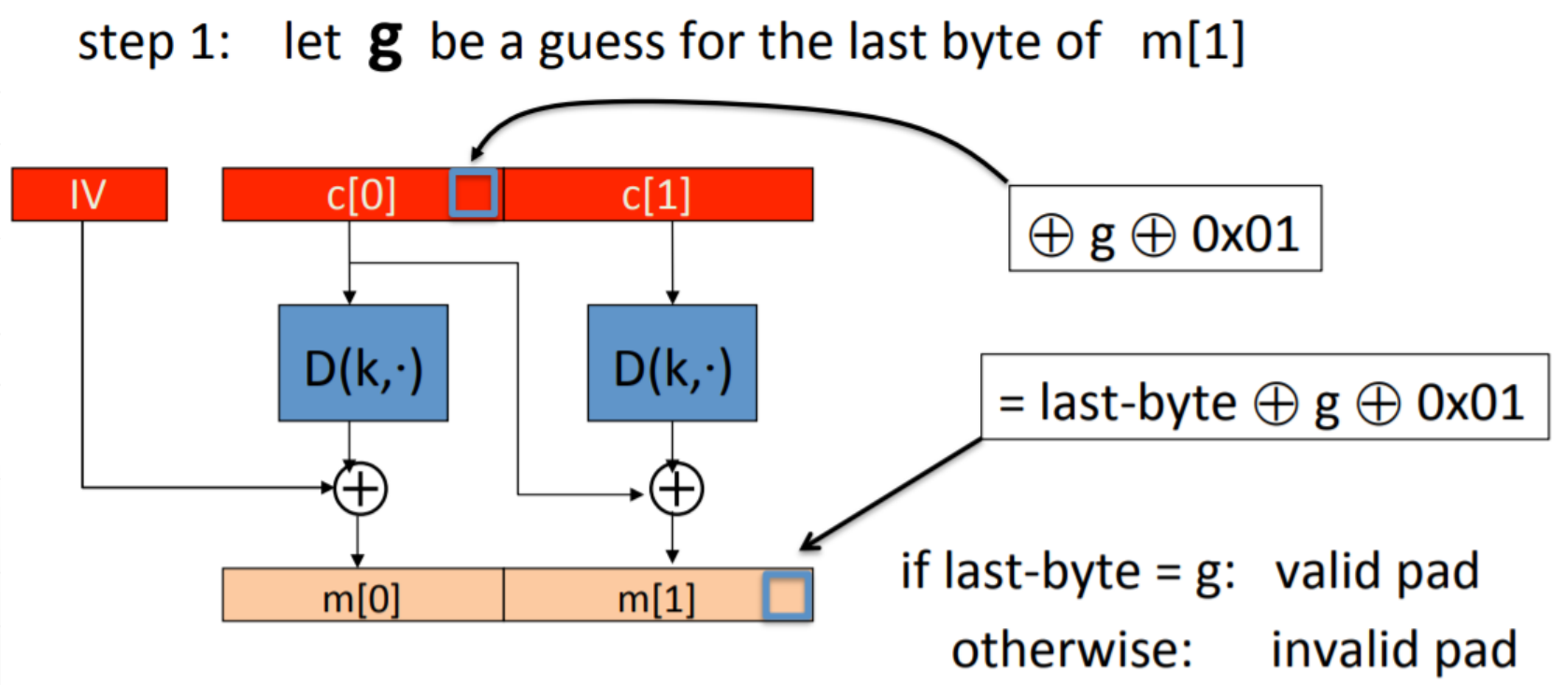
We want to know this!

We know this!

We know part of this!

Source of all drawings of modes: https://www.cs.ucdavis.edu/~rogaway/papers/modes.pdf

Strategy: Guess one byte at a time



Source:

https://xianmu.github.io/posts/2018-11-30-padding-oracle-attack.html

UML for the Padding Oracle Attack against CBC

Source:

Reply in https://crypto.stackexchange.com/questions/70570/how-does-the-cbc-padding-oracle-attack-work-in-general by “SEJPM”