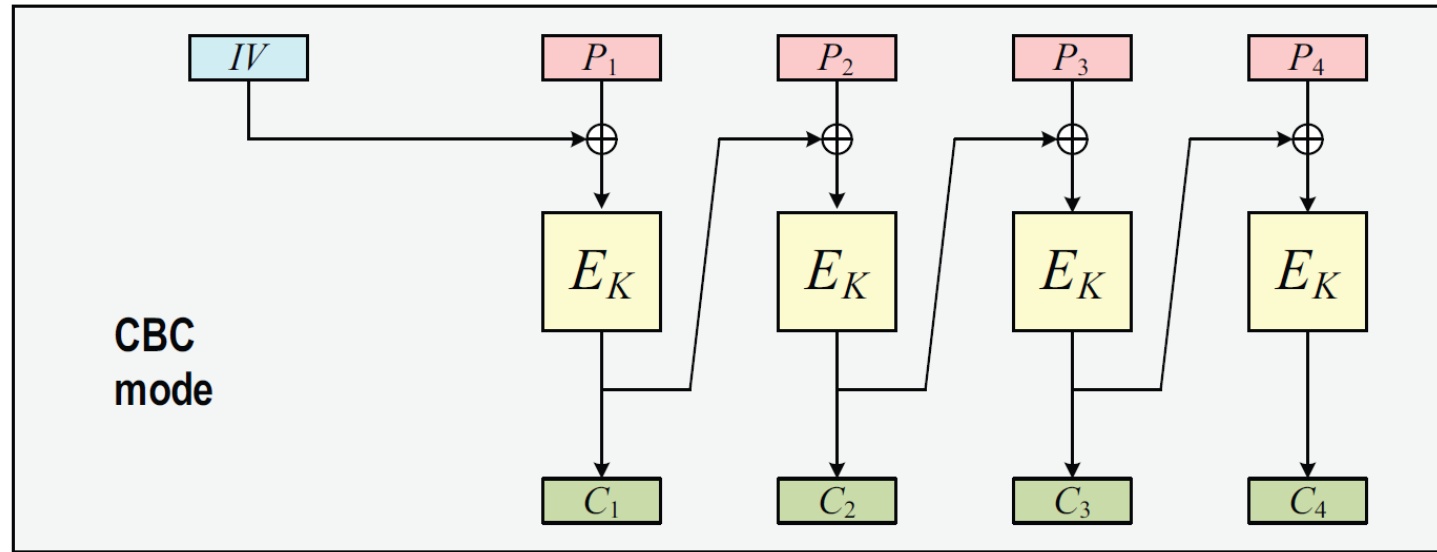


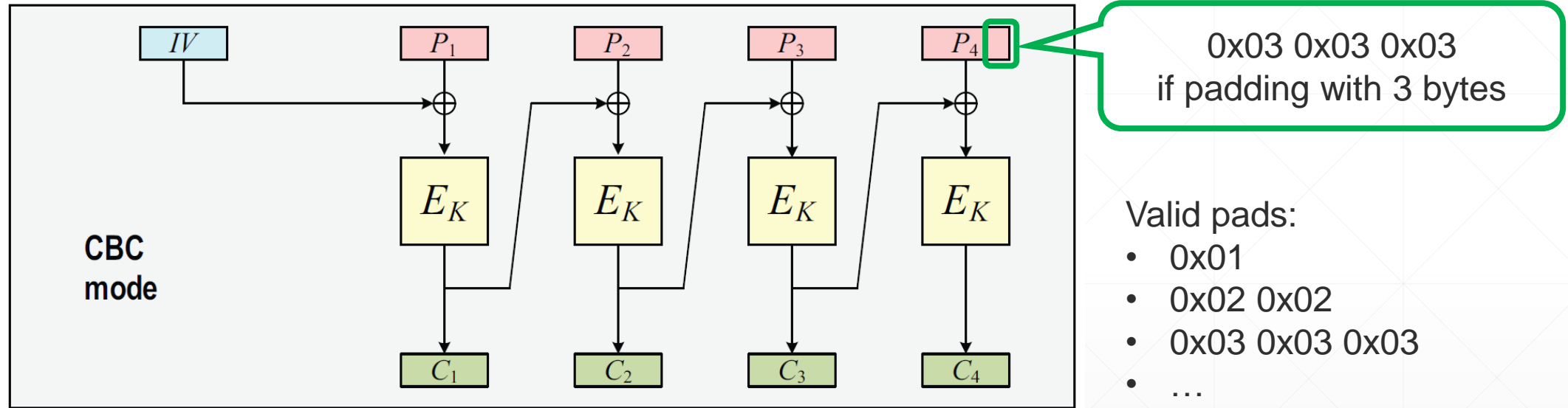
Padding Oracle Attack

Chanathip Namprempre

Recall CBC Mode



CBC Mode with Padding (simplified)



Padding Oracle Attack: Formal Definition

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

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 $(M^* = M)$

Source:

Bellare and Rogaway, unpublished notes.

Fun Video: CBC padding oracle attack

Attacking Modern Cryptography

<https://youtu.be/8Tr2aj6JETg>

3:57

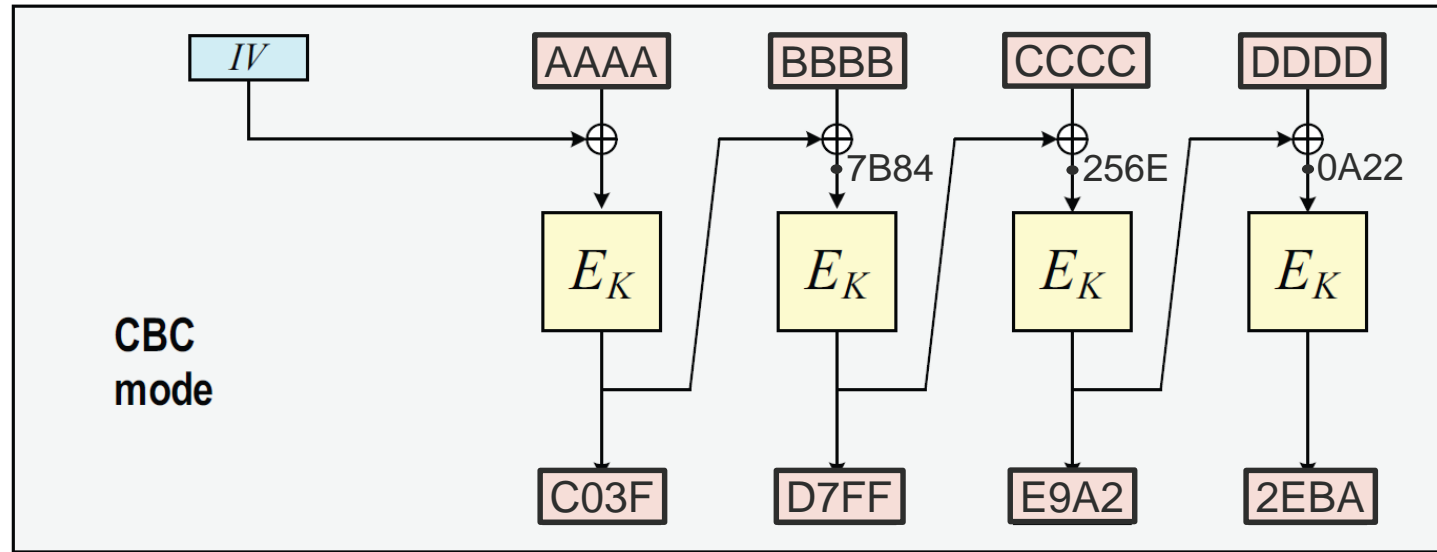
By Pastie's Bin

(Recommendation: watch it at reduced speed!)

The attack described here is applicable to SSLv3.

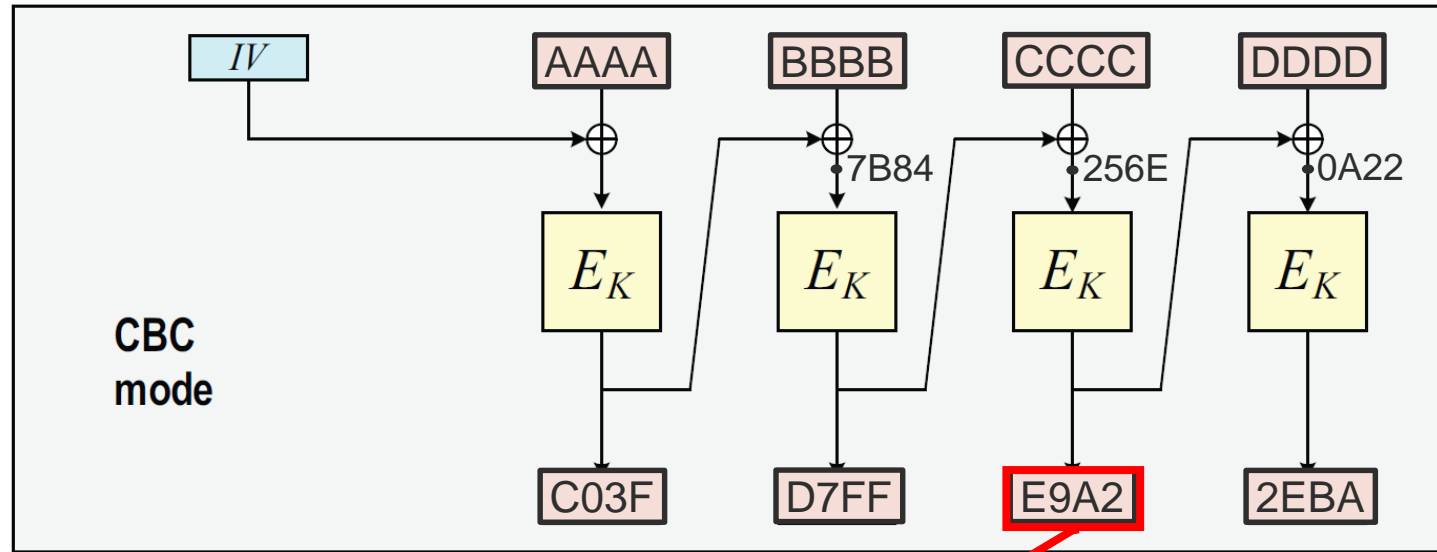
It was originally pointed out in a 1997 paper by David Wagner and Bruce Schneier.

Redrawing pictures from the video



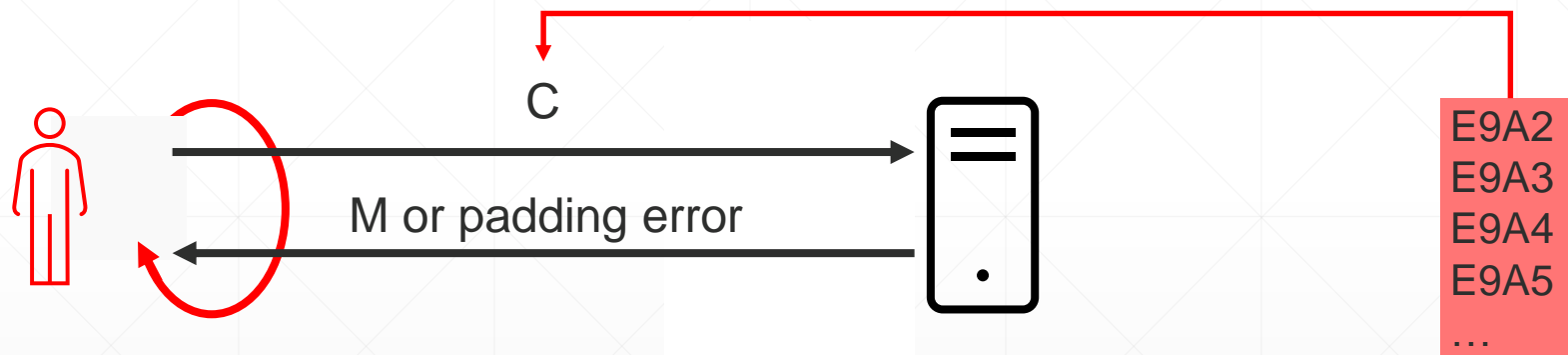
The video does not show the IV.

Redrawing pictures from the video

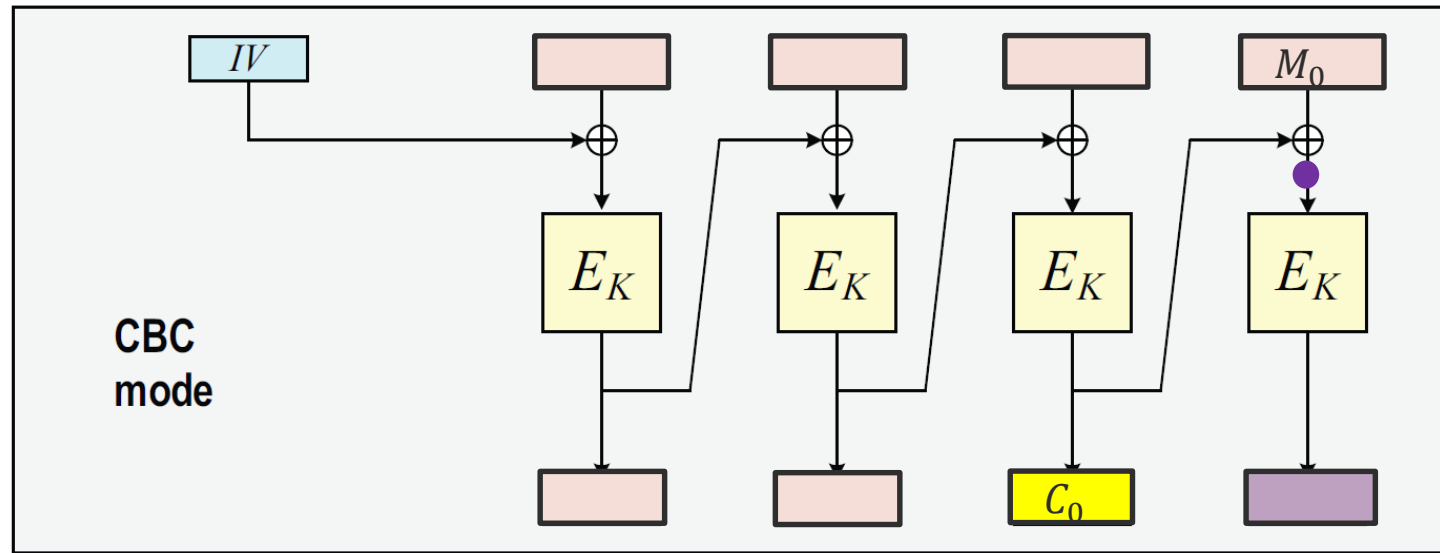


In the video, we cycle through this value one by one from right to left.

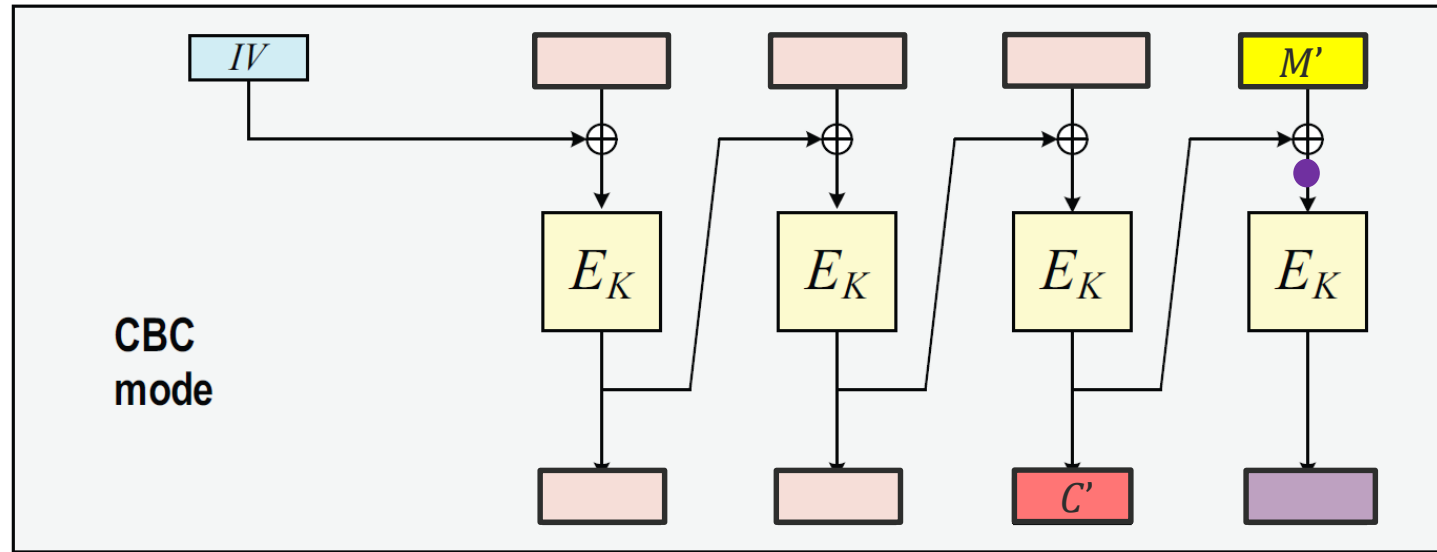
What does a padding oracle attack look like?



We want to find M_0

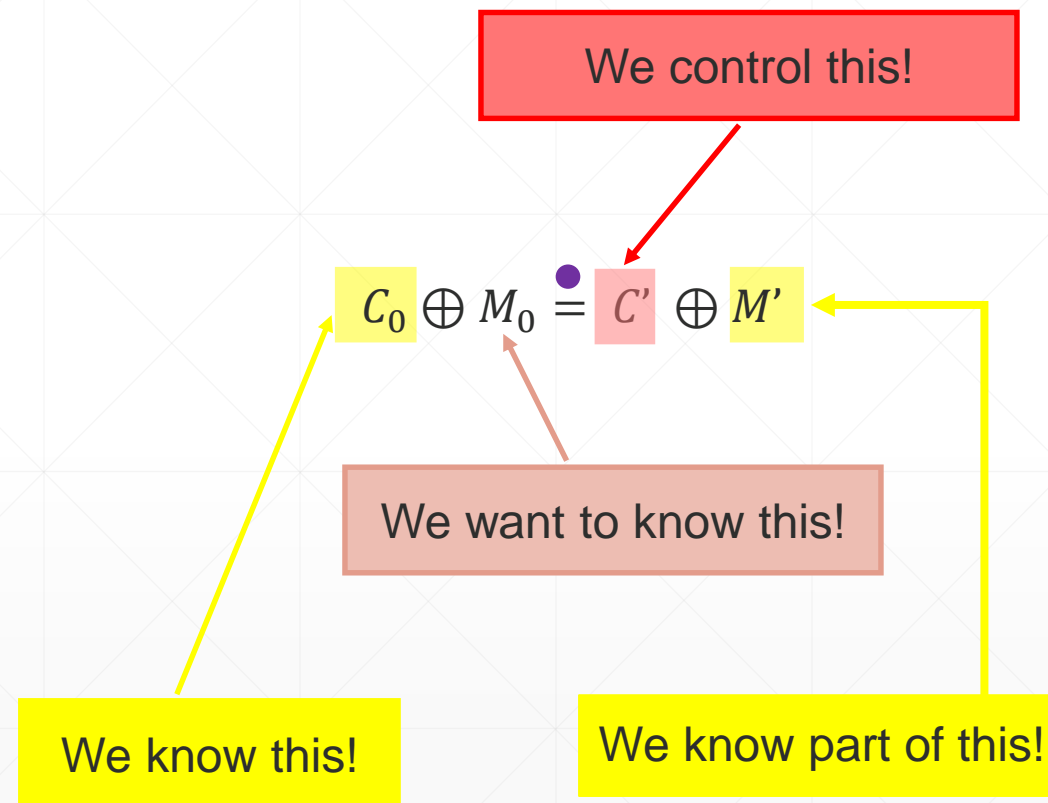
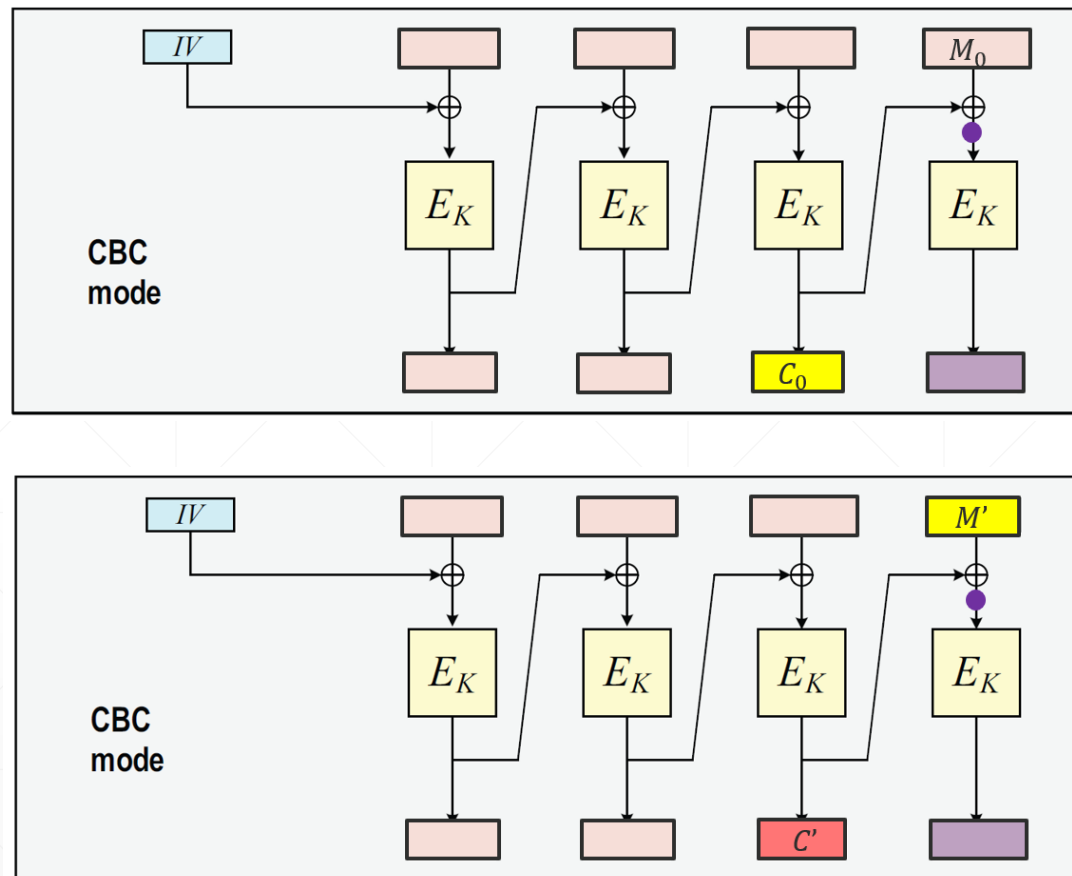


The Main Point



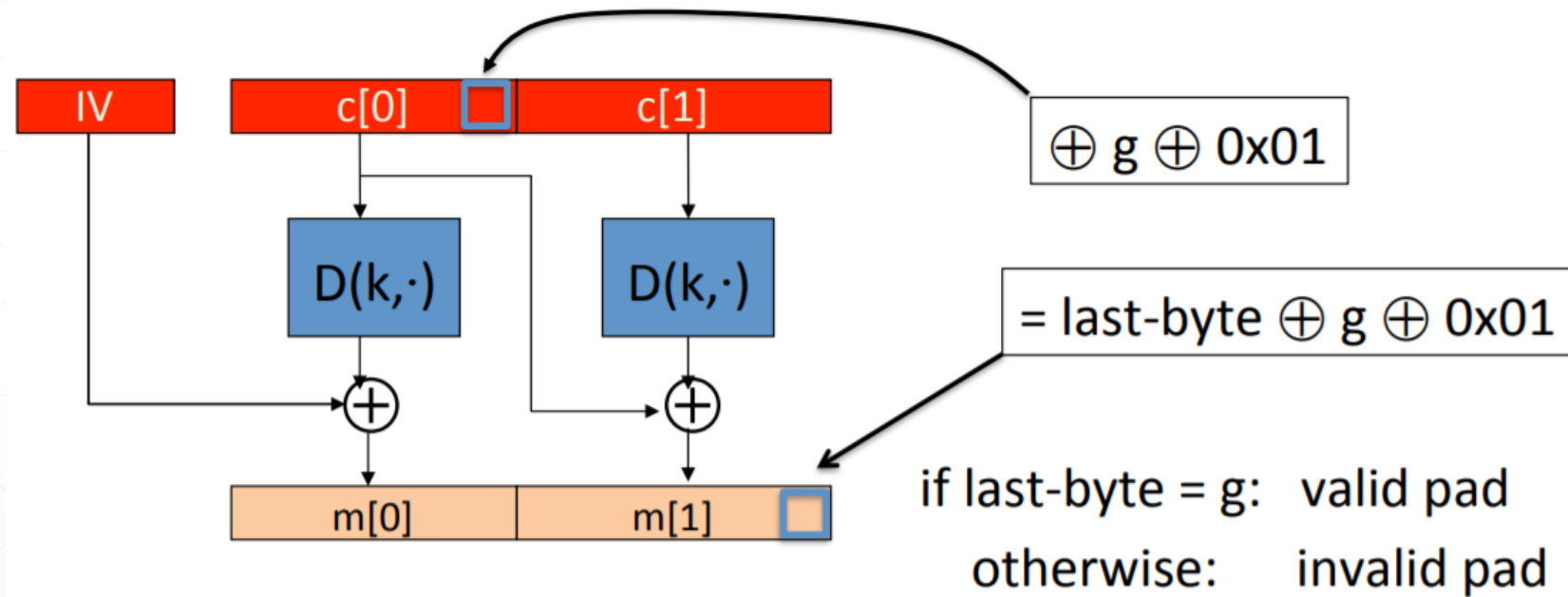
We modify C_0 to get C' and observe the server's response, which depends on M' .

In summary



Strategy: Guess one byte at a time

step 1: let g be a guess for the last byte of $m[1]$



Source:

Dan Boneh's coursera slides: <https://course.ece.cmu.edu/~ece733/lectures/07-authenc-part2.pdf>

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”

