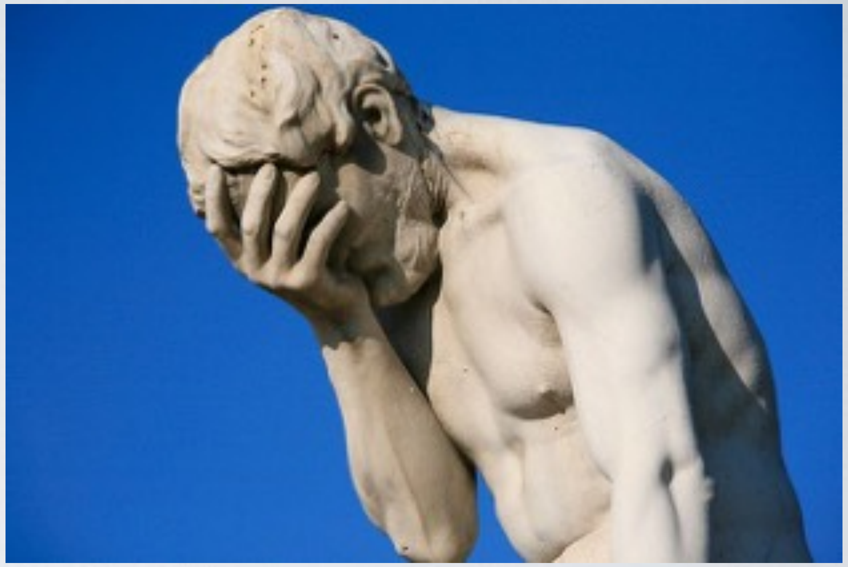
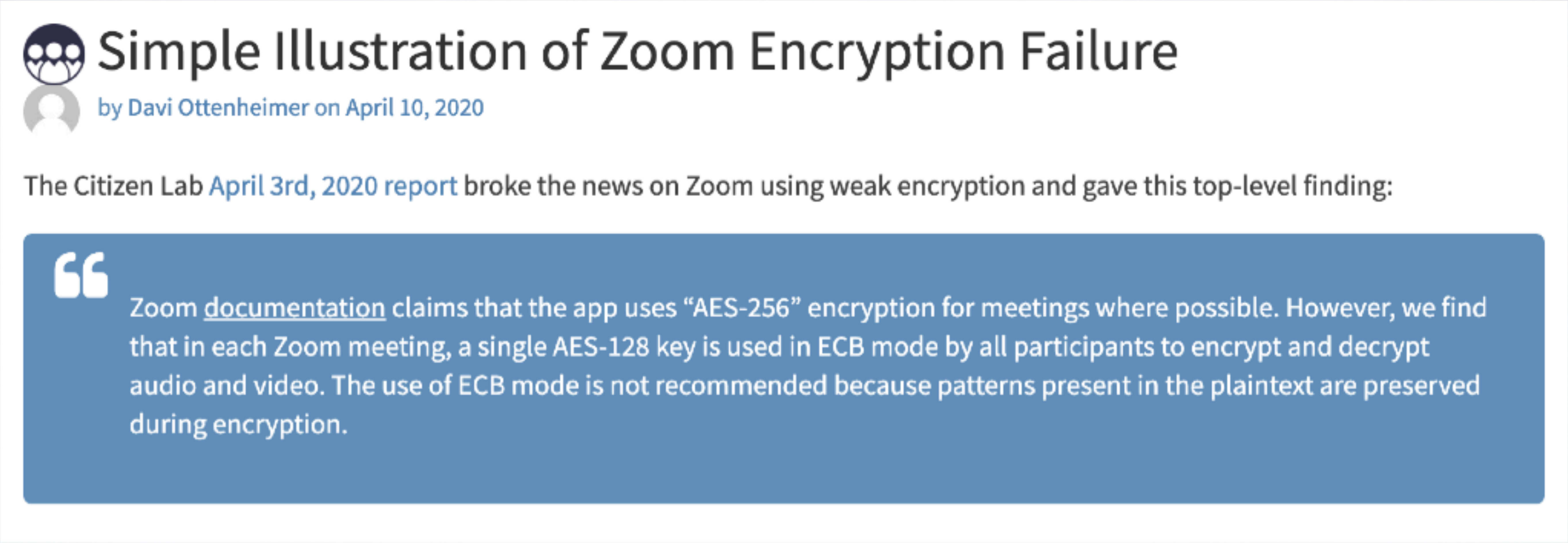




Simple Illustration of Zoom Encryption Failure

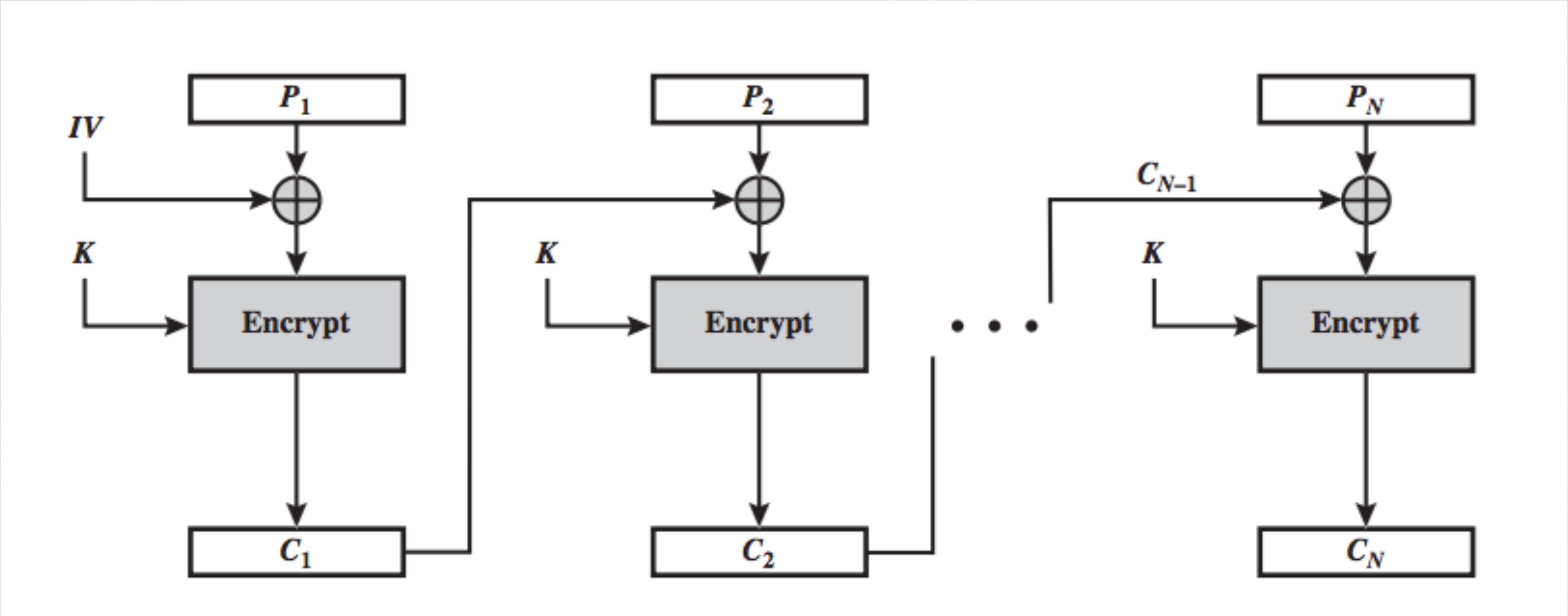
by Davi Ottenheimer on April 10, 2020

The Citizen Lab April 3rd, 2020 report broke the news on Zoom using weak encryption and gave this top-level finding:

> Zoom documentation claims that the app uses "AES-256" encryption for meetings where possible. However, we find that in each Zoom meeting, a single AES-128 key is used in ECB mode by all participants to encrypt and decrypt audio and video. The use of ECB mode is not recommended because patterns present in the plaintext are preserved during encryption.

source: *Security Boulevard*

CBC - Cipher Block Chaining (a.k.a Chaining Mode)



Introduce some randomness using the previous ciphertext block

✓ Repeating plaintext blocks are not exposed in the ciphertext

◉ No parallelism

➡ The Initialization Vector should be known by the recipient