Unauthenticated encryption in the wild

Carl Svensson

September 12, 2017

SEC-T 2017

About me

- Carl Svensson, 26
- MSc in Computer Science, KTH
- Head of Security, Kry
- CTF-player, HackingForSoju
- calle.svensson@zeta-two.com
- @zetatwo
- https://zeta-two.com

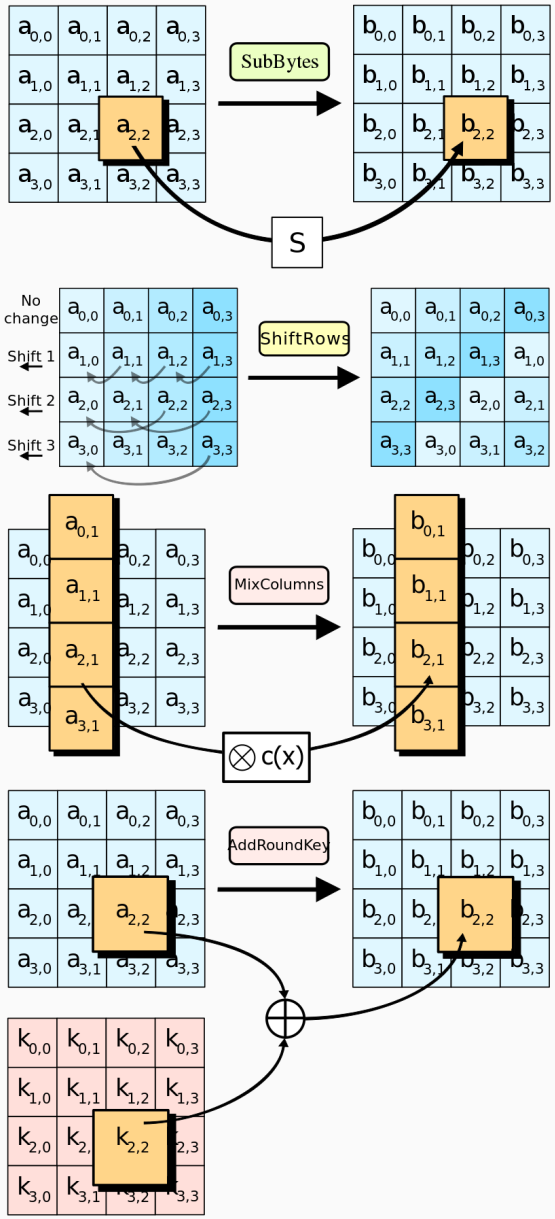
KRY

Cryptography in 30 seconds

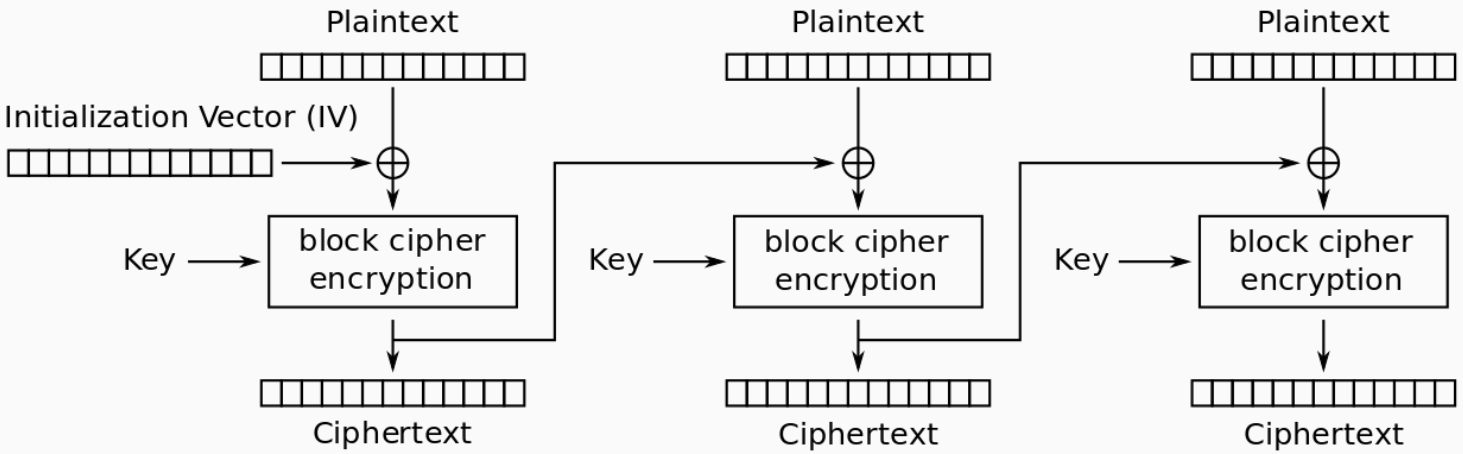
- Transform data
- Maths, a lot of it
- Many possible goals
  - Confidentiality (Hide)
  - Integrity (Verify)
  - Authentication (Identify)
  - Non-Repudiation (No take-backsies)
- Modularity

AES - Very good, at one specific thing

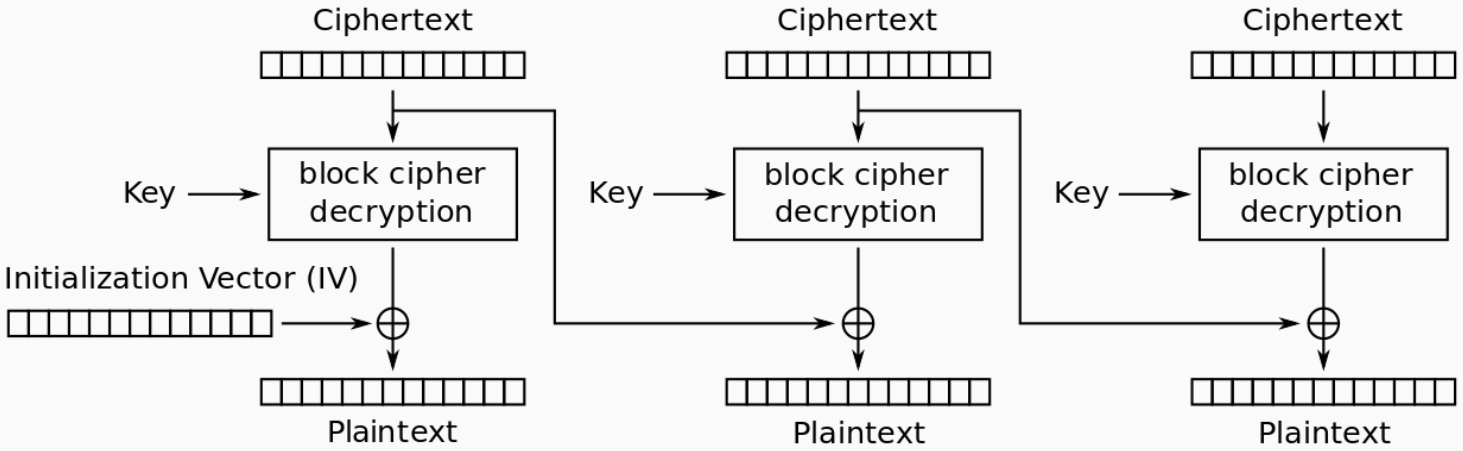
- Block cipher
- Key
- Basic building block
- No known attacks*



Block cipher modes, when you have more data



Cipher Block Chaining (CBC) mode encryption

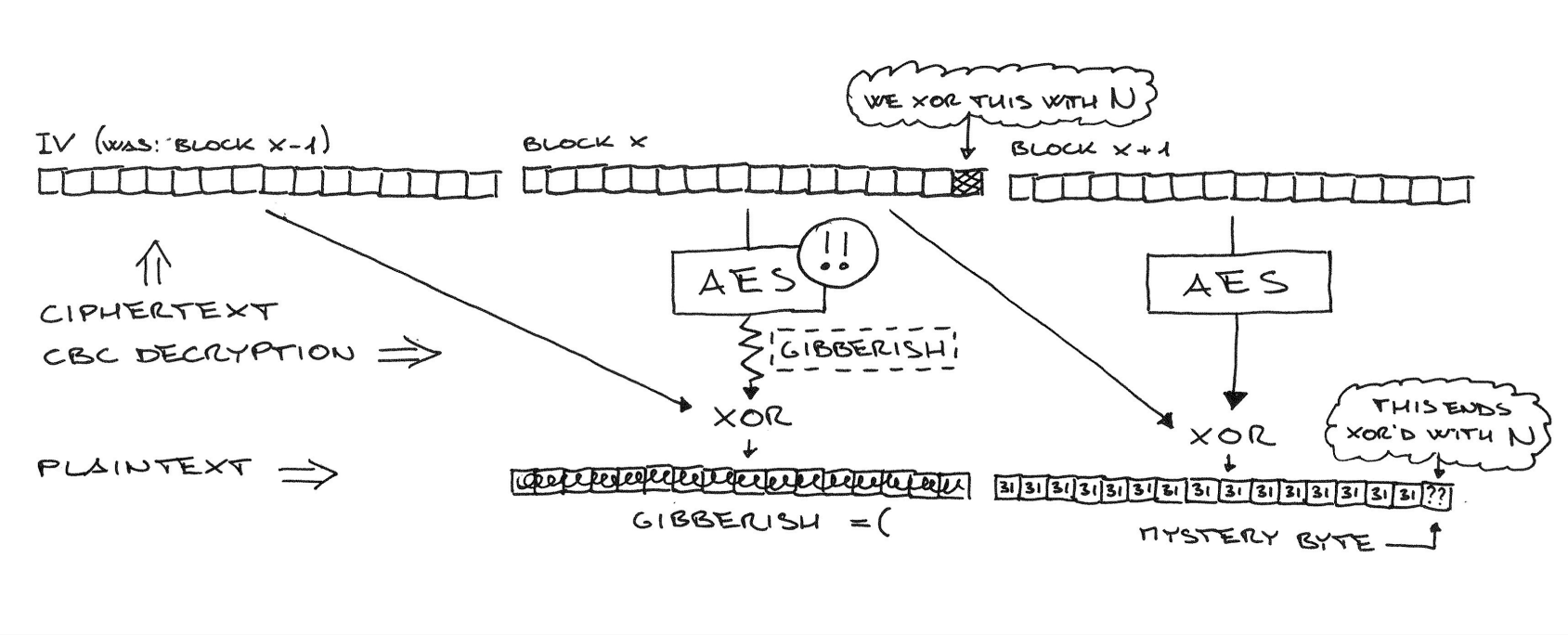


Cipher Block Chaining (CBC) mode decryption

Encryption is not authentication

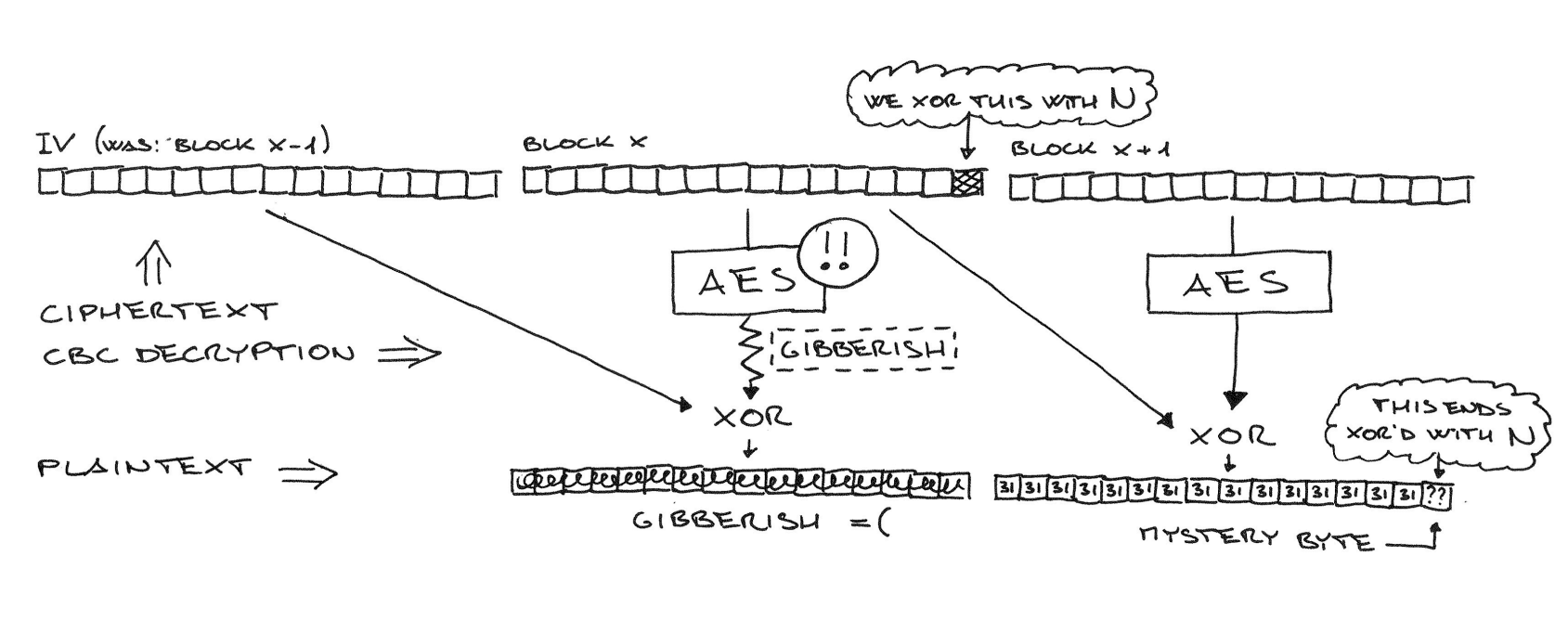
- A priori, no way to differentiate
- Has to accept all ciphertexts
- Might be able to tell later
- The Cryptographic Doom Principle

Bit flipping attack



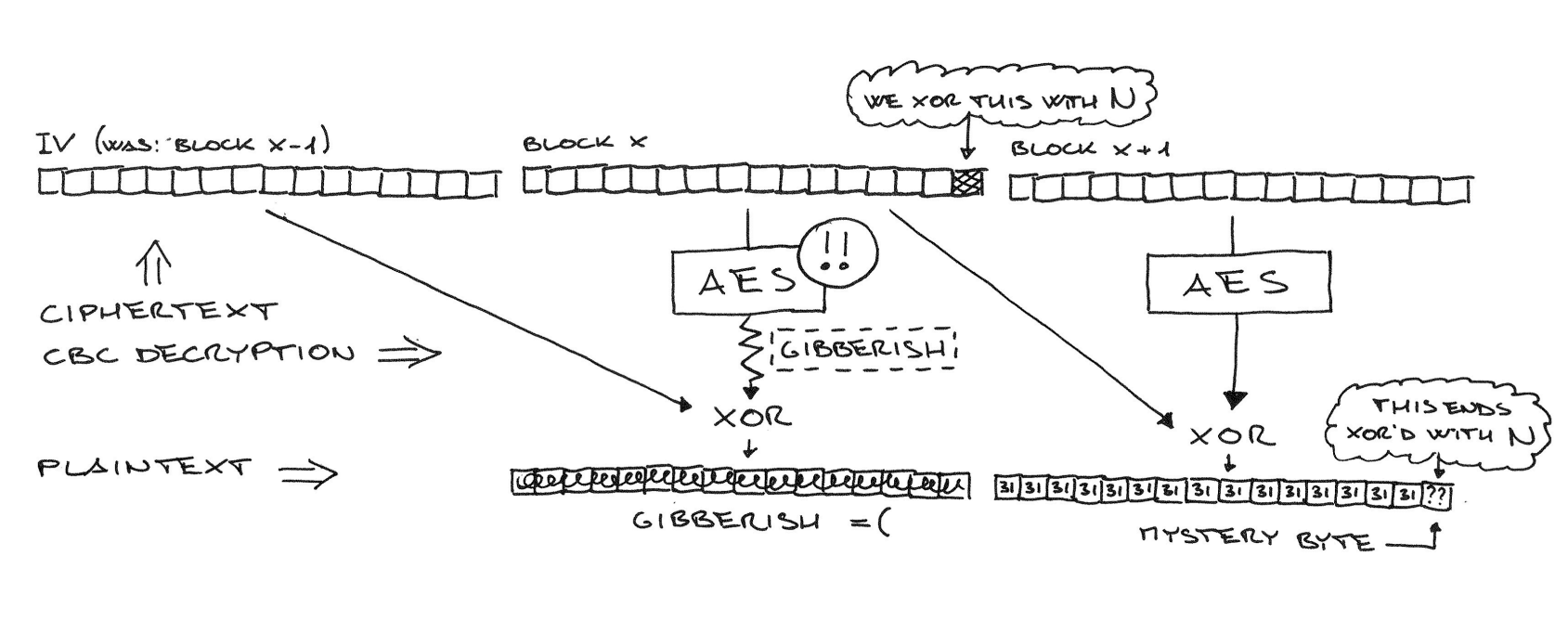
Example: Open redirect as a service

- https://link.a.com/AAAA/BBBBBBBBBBBBBBBBBBBBB
- Known plaintext, just visit
- $x \oplus m_1 = m_2 \Leftrightarrow x = m_1 \oplus m_2$
- Edit link contents



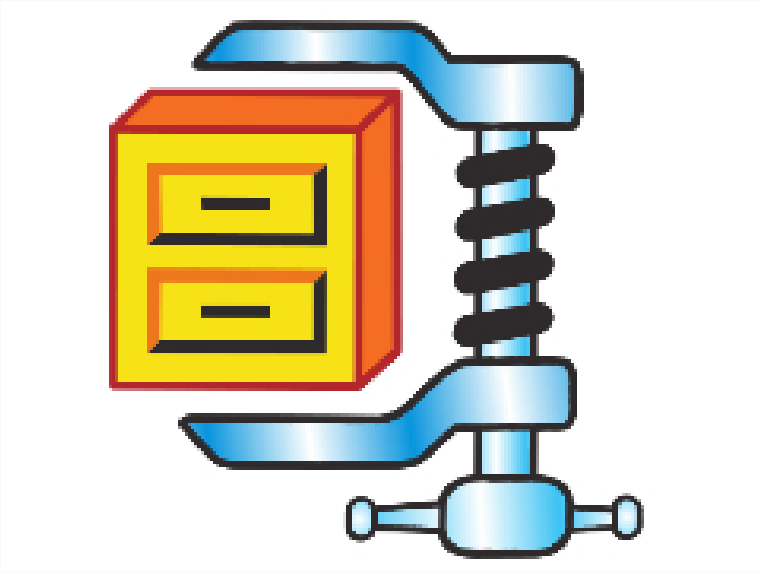
Padding Oracle attack

- PKCS7 padding
- bool oracle(input) { ... }
- Differing error messages
- $x \oplus g = t \Leftrightarrow x = g \oplus t$
- $16 \cdot 256 \ll 256^{16}$



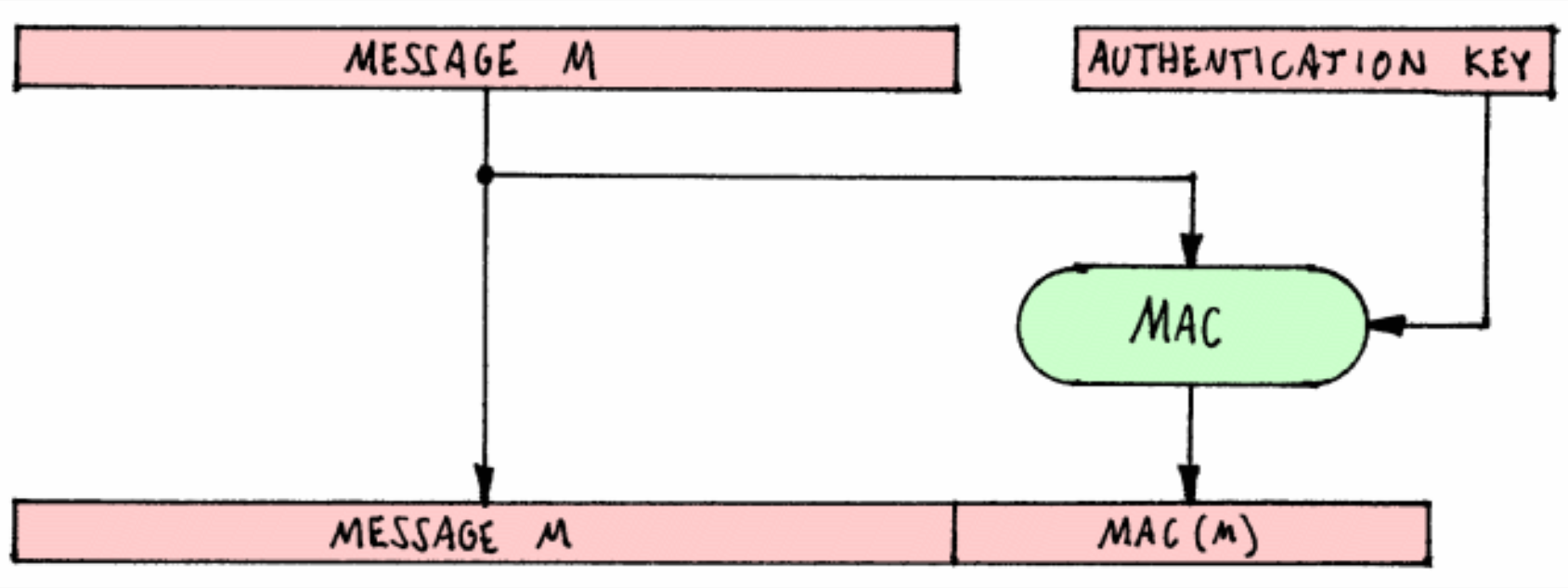
Example: Extracting secrets -> RCE

- Backup data
- File format:
  $Enc_{Km}(key1)||Enc_{Ks}(zipfile)$
- Padding Oracle -> Key -> Craft zip
- Zip relative paths -> RCE



What to do? Authenticate!

- Encryption AND authentication
- Message Authentication Code
- $HMAC_k(message) = tag$
- $Verify_k(tag, message) \in True, False$



Thanks for listening!