

AE and AEAD

Right now we know

- **Encryption** which takes care of the confidentiality problem

an attacker cannot get any info about the plaintext from a ciphertext

- **MAC** which takes care of **Integrity**

An authorized party (receiver) can check if the data is genuine or tempered with

But we have yet to define a method that combines them. We are going to do it now

Authenticated Encryption

Authenticated encryption (AE) provides confidentiality and data authenticity simultaneously.

Security

A Secure AE system is secure against chosen ciphertext attacks

Let

- (E, D) = cipher
- (S, V) = MAC

Types

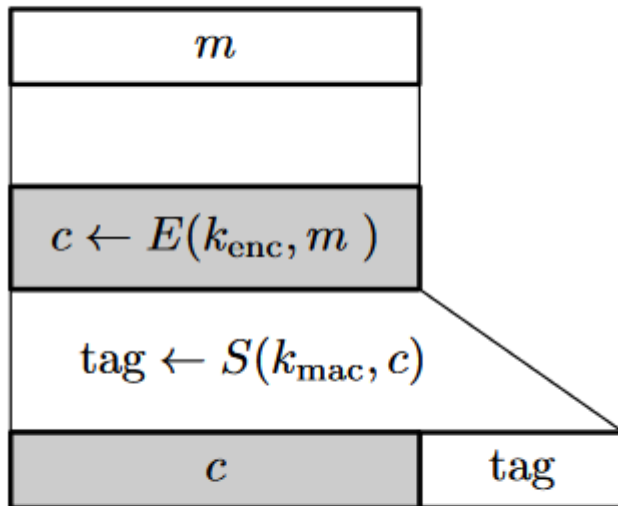
Encrypt-then-MAC

Encryption

- $c = E(k_e, m)$
- $t = S(k_m, c)$

Decryption

- $V(k_m, c, t)$
 - = reject \Rightarrow reject
 - = *textaccept* \Rightarrow return $D(k_e, c)$



encrypt-then-mac

Mistakes

- $k_e = k_m \rightarrow$ they must be chosen independently
- apply the MAC to only a part of the ciphertext
 - Ex: Not signing the IV in a CBC mode \Rightarrow An attacker can queue a custom IV' and the challenger must decrypt c

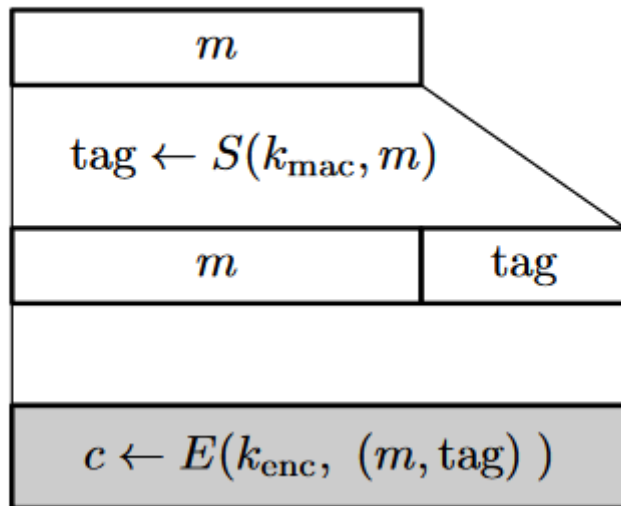
MAC-then-Encrypt

Encryption

- $t = S(k_{\text{mac}}, m)$
- $c = E(k_{\text{enc}}, (m, t))$

Decryption

- $(m, t) = D(k_e, c)$
- $V(k_m, m, t)$
 - = reject \Rightarrow reject
 - = accept \Rightarrow return m



•

Broken

- Vulnerable to CCA
 - Padding oracle attacks <https://www.youtube.com/watch?v=O5SeQxErXA4>

Encrypt-and-MAC

- $t = S(k_{\text{mac}}, m)$
- $c = E(k_{\text{enc}}, m)$

Broken too

The MAC is not designed for confidentiality => It can reveal information about the message

Authenticated Encryption with Additional Data

Extension of AE

- We give AE an additional input -> **Associated data** d
- Integrity protected, Secrecy not
- $c = E(k, m, d, n)$ where n is a nonce
- m or reject = $D(k, c, d, n)$

Security

AEAD is secure if (E, D) is CPA secure and has ciphertext integrity

Encrypt then MAC

Encryption

- $c = E(k_e, m, n)$
- $t = S(k_m, (c, d), n)$

Decryption

- $V(k_m, (c, d), t, n)$
 - = reject \Rightarrow reject
 - = accept $\Rightarrow D(k_e, c, d, n)$

Resources

- https://en.wikipedia.org/wiki/Authenticated_encryption
- <https://crypto.stackexchange.com/questions/12178/why-should-i-use-authenticated-encryption-instead-of-just-encryption>

- <https://crypto.stackexchange.com/questions/12178/why-should-i-use-authenticated-encryption-instead-of-just-encryption>