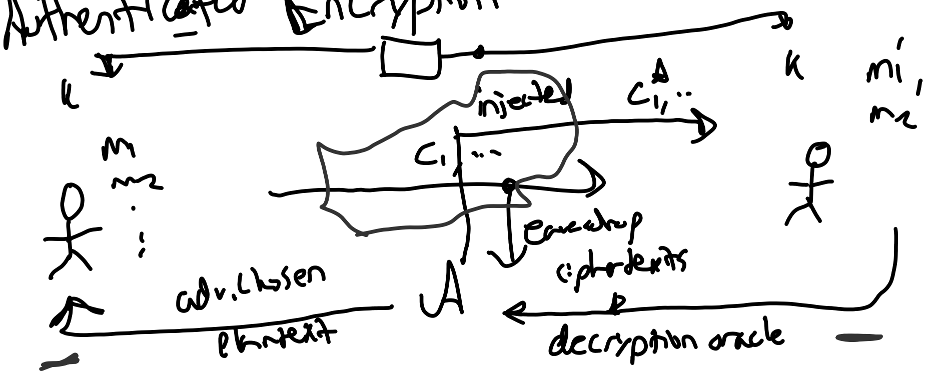
Encryption Extras

Friday, November 12, 2021 3:50 PM

Authenticated Encryption

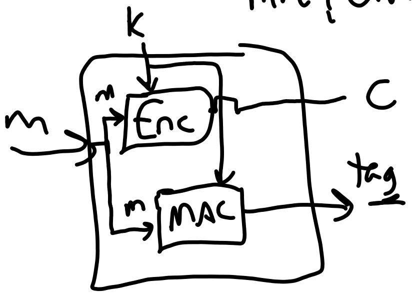


- Combine Integrity & privacy
- Any decrypted message output by Bob was sent by Alice

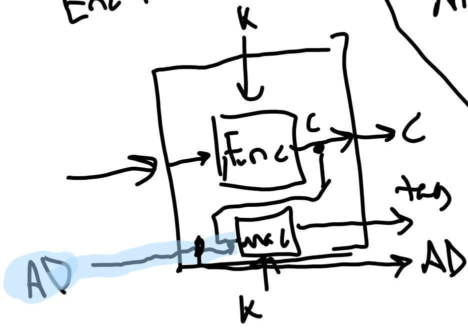
Ways to combine MAC & Enc.

X - Encrypt & mac
- Mac then encrypt
+ - Encrypt then mac

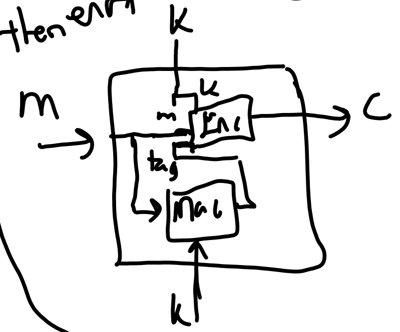
mac & encrypt

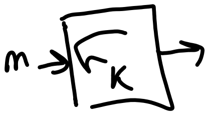


Enc then mac



mac then encript





$tag = F_K(m)$

Really "check then decrypt" only decrypts after Mac passes

AEAD

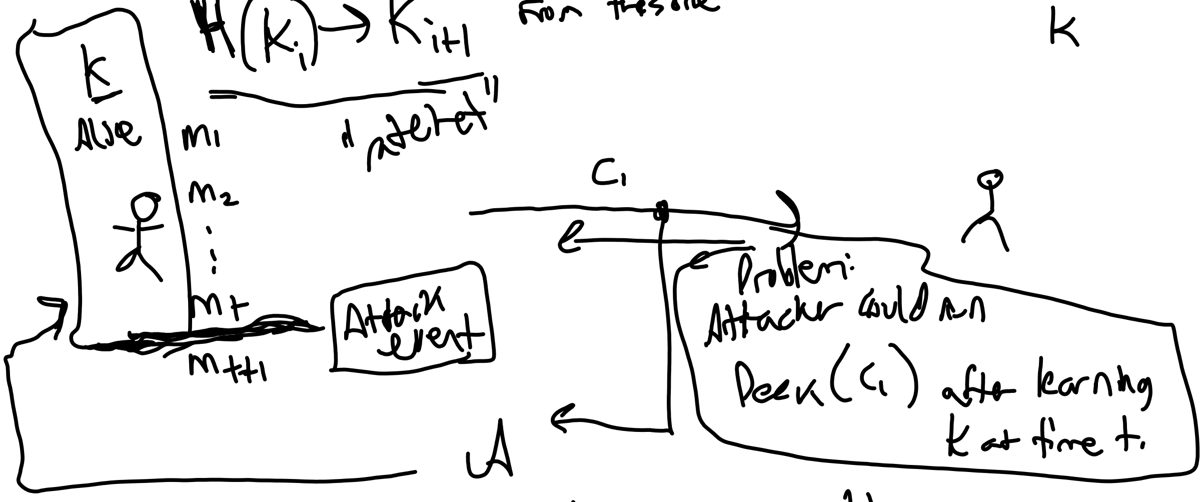
← authenticated associated data.
- header of non-confidential
- used to prevent replay attacks, reorging

Forward Security

Idea: rotate key ... next round's key

derive
From this one

$H(k_i) \rightarrow K_{i+1}$



- $\mathcal{A}$ gets an entire snapshot of Alice at time t.

- Goal: messages sent prior to attack t are still secure even after.

How to solve?

In public key setting:

Long term secret

sk_A pk_A pk_B

sk_B pk_B
pk_A

Each session

$a \xleftarrow{\$} \mathbb{Z}_q$

$A = g^a$

$\sigma_A = Sign(sk_A, A) \xrightarrow{A,\ \sigma_A}$

$\xleftarrow{\sigma_B,\ B}$

$ssk = B^a$

$aead(ssk, m) \xrightarrow{c, tag}$

End of session:

delete a, ssk

Plausible Deniability:

- for later