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

At Ways to Combine MAC & Enc.
- Encrypt & MAC
- MAC then encrypt
- Encrypt then MAC

AEAD
[authenticated associated data]
- header of non-confidential
- used to prevent replay attacks, reordering

Forward Security
- take: re-use key... and make key
derivation steps:

For these:

\[ H(K_i) \rightarrow K_{i+1} \]

Problem:
Attacker could see \( \text{Peek}(C_i) \) after learning \( K \) at time \( t \).

Goal:
Messages sent prior to attack + are still secure even after.

How to solve?

In public key setting:

Long-term secret

\[ \text{sk}_A, \text{pk}_A, \text{pk}_B \]

Each session

\[ a \in Z_p \]

\[ A = g^a, \sigma = \text{Sign}(sk_a, A, A, \sigma) \]

\[ ssk = B^a \]

\[ \text{read}(ssk, \ldots) \rightarrow c, \text{tag} \]

End of session:

\[ \text{pk}_A, \text{pk}_B \]
Delete a, ssh

Plausible Deniability:
- For later