Confidentiality

Encryption

- plaintext ⇒ ciphertext
- Under key $k_\mathrm{E} \in K$

Decryption

- ciphertext ⇒ plaintext
- Under key $k_\mathrm{D} \in K$

Symmetric cryptography: $k_\mathrm{E} = k_\mathrm{D}$ is the secret key.

Asymmetric cryptography: k_E is public and k_D is private.

Authenticity

Authentication

- message ⇒ (message, **tag**)
- Under key $k_\mathrm{A} \in K$

Verification

- (message, **tag**) ⇒ $\{$message, $\perp\}$
- Under key $k_\mathrm{V} \in K$

Symmetric cryptography: $k_\mathrm{A} = k_\mathrm{V}$ is the secret key.
The tag is called a *message authentication code* (MAC).

Asymmetric cryptography: k_A is private and k_V is public.
The tag is called a *signature*.