





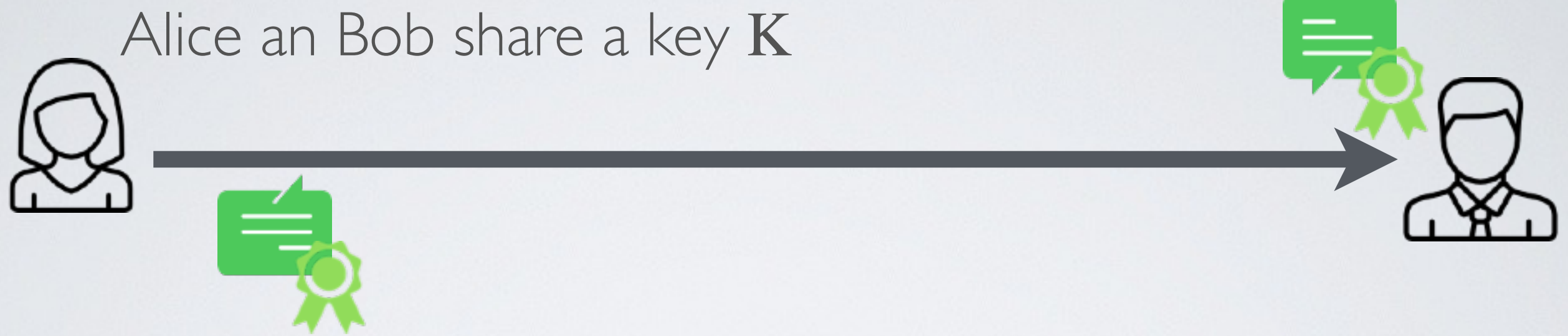


Security mechanisms

	Encryption	MAC	Authenticated Encryption
Confidentiality			
Integrity			

Authenticated Encryption (2013)



Encrypt-and-MAC (E&M)

$$AE_K(m) = E_K(m) \parallel H_K(m)$$

SSH

MAC-then-Encrypt (MtE)

$$AE_K(m) = E_K(m \parallel H_K(m))$$

SSL

Encrypt-then-MAC (EtM)

$$AE_K(m) = E_K(m) \parallel H_K(E_K(m))$$

AES-GCM