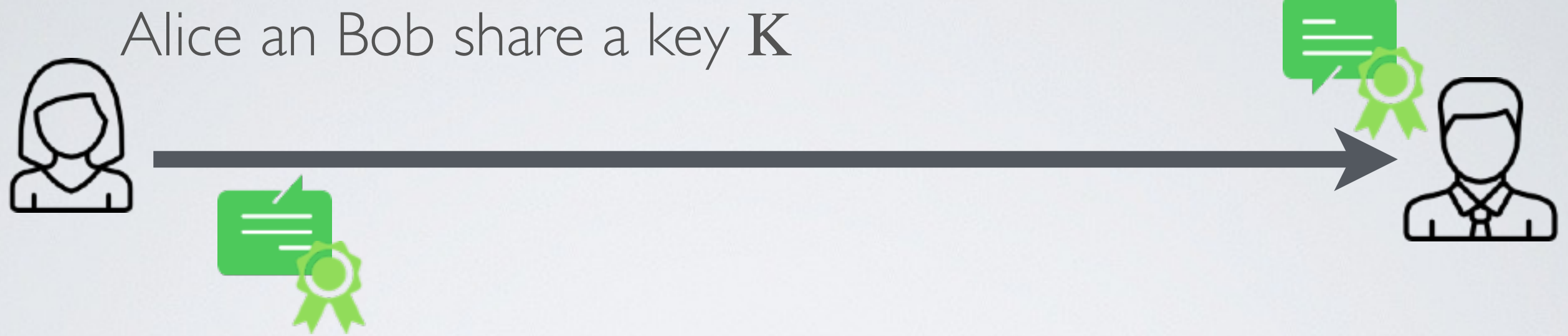


# Authenticated Encryption (2013)



Encrypt-and-MAC (E&M)  
considered vulnerable

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

*Old SSH*

~~MAC then Encrypt (MtE)~~  
considered vulnerable

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

*TLS 1.0-1.1*

Encrypt-then-MAC (EtM)  
considered standard

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

*AES-GCM  
New SSH  
TLS 1.2-1.3*

# Digital Signatures