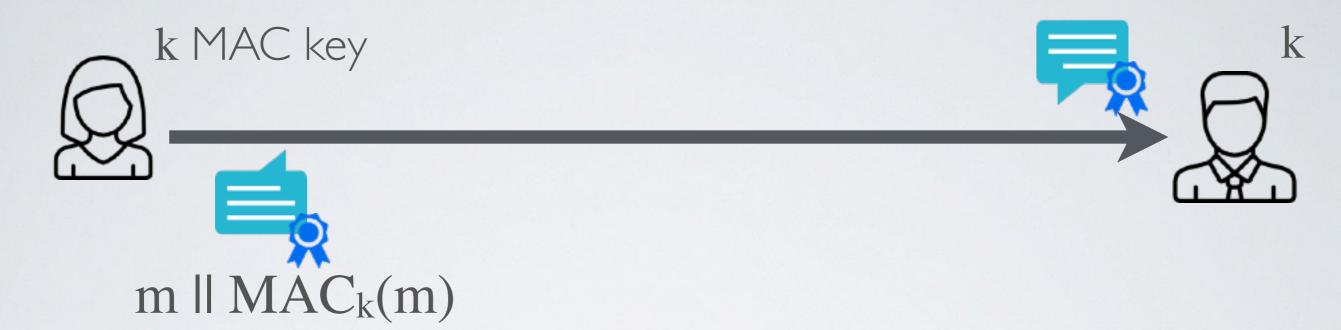
Good HMAC



Alice an Bob share a key k

→ Option I : envelope method

 $MAC_k(m) = H(k \parallel m \parallel k)$

→ Option 2 : padding method (i.e. HMAC standard)

 $HMAC_k(m) = H((k \oplus opad) || H((k \oplus ipad) || m))$

Authenticated Encryption