Good HMAC

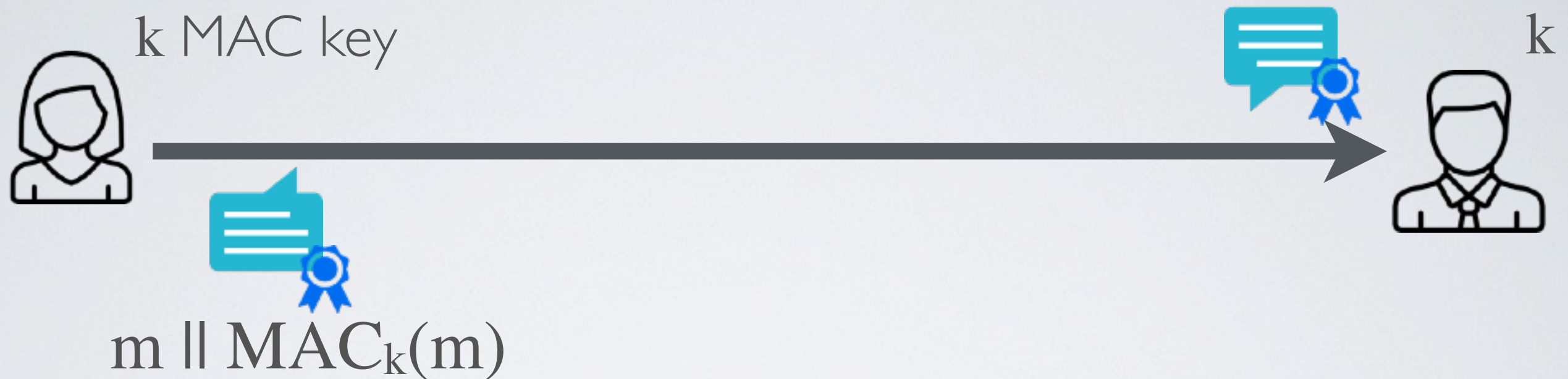k MAC key   k

m ∥ $\text{MAC}_k(m)$

Alice an Bob share a key k

➡ Option 1 : envelope method

$$\text{MAC}_k(m) = H(k \parallel m \parallel k)$$

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

$$\text{HMAC}_k(m) = H((k \oplus \text{opad}) \parallel H((k \oplus \text{ipad}) \parallel m))$$

Authenticated Encryption