MAC - Message Authentication Code

Alice an Bob share a key **k**

- ➡ HMAC - use a hash function on the message and the key

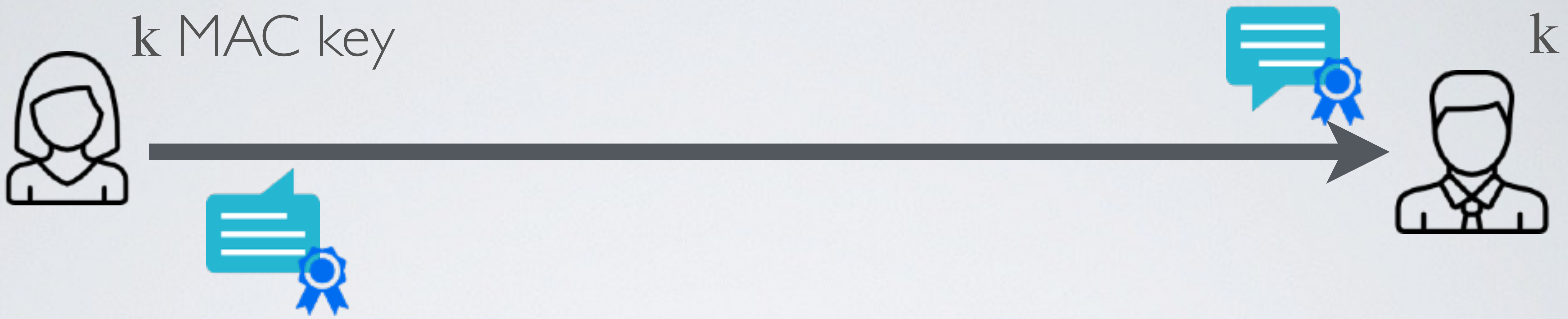
$$\mathbf{MAC_k(m) = H(k \,||\, m)}$$

$$m \,\|\, \mathrm{MAC}_k(m)$$

k MAC key

k

MAC - Message Authentication Code



k MAC key

k

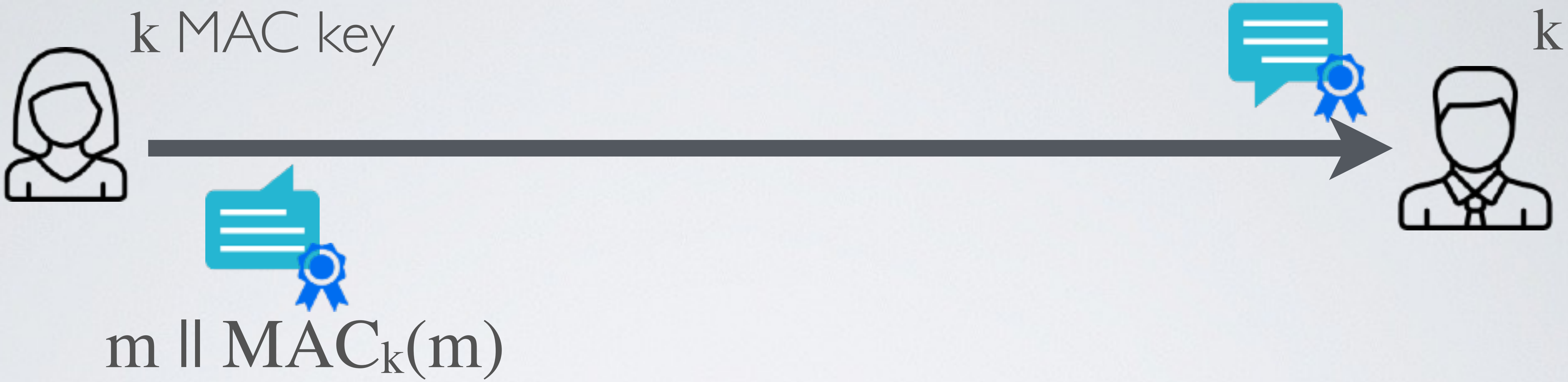
$m \,||\, MAC_k(m)$

Alice an Bob share a key **k**

➡ HMAC - use a hash function on the message and the key

$$MAC_k(m) = H(\xcancel{k \,||}\, m)$$

Good HMAC



k MAC key

k

$m \,||\, MAC_k(m)$

Alice an Bob share a key **k**

- ➡ Option 1 : envelope method

$$MAC_k(m) = H(k \,||\, m \,||\, k)$$

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

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