



MAC-Message Authentication Code

Alice and Bob share a key  $k$

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

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







$\min_{\mathbf{N}} \text{MAE}_k(\mathbf{n})$

MACKey





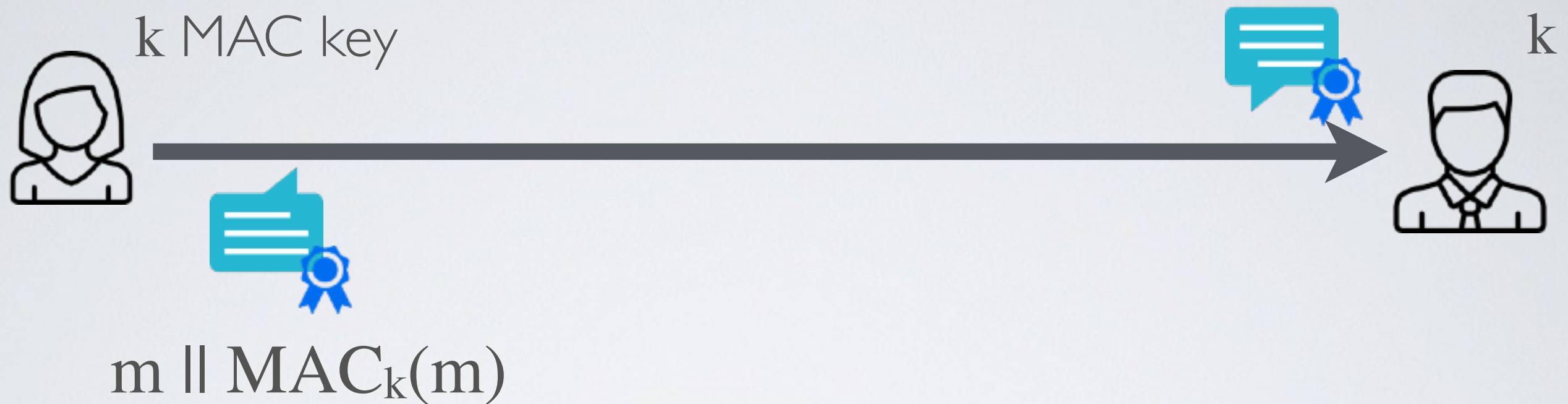








# MAC - Message Authentication Code



Alice and Bob share a key  $k$

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

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

# Length Extension Attack

**Vulnerable** : All Merkle–Damgård-based hash functions  
so MD5, SHA-1 and SHA-2 (but not SHA-3)