MAC - Message Authentication Code

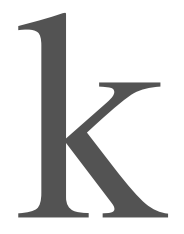
Alice an Bob share a key $\mathbf{k}$

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

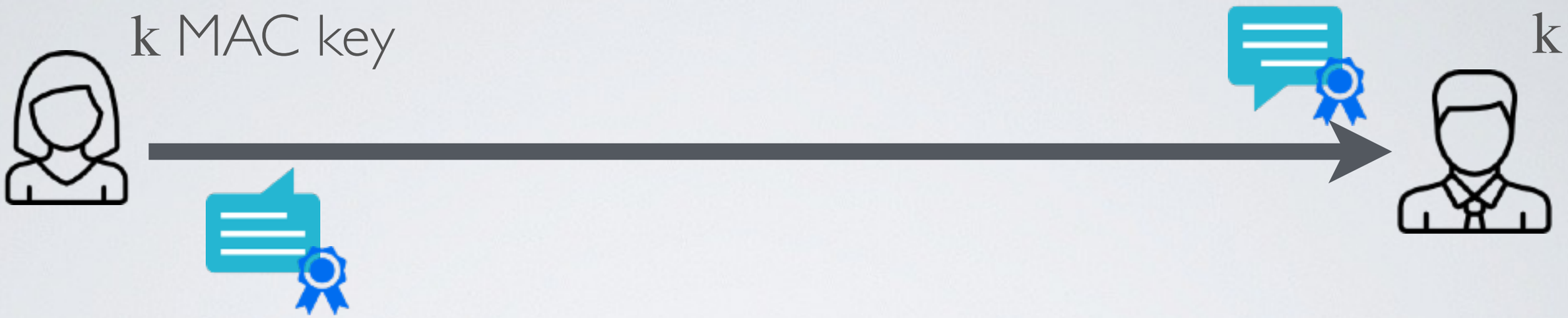
$$\mathbf{MAC}_k(\mathrm{m}) = \mathrm{H}(\mathrm{k} \,||\, \mathrm{m})$$


m || MAC_k(m)


k MAC key



MAC - Message Authentication Code



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

Alice an Bob share a key k

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

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

Length Extension Attack

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