HMAC

→ HMAC is the current industry standard as CBC-MAC is deemed to be slow.

(Gen, h) : A fixed length hash function

(Gen, H) : Hash function after applying MD transform to (Gen, h).

Fixed constants IV, opad and ipad.

$$\text{HMAC tag for } m = H^s_{IV}(k \oplus \text{opad} \,||\, H^s_{IV}((k \oplus \text{ipad}) \,||\, m))$$

opad: 0x36 repeated as many times as needed

ipad: 0x5c repeated as many times as needed.