HMAC

A MAC based on hashing is faster and works using variable length hash functions.

The HMAC algorithm works as follows -

$$HMAC_K(m) = H^s_{IV}((k \oplus opad) \,||\, H^s_{IV}((k \oplus ipad) \,||\, m))$$

where $H^s_{IV}(x)$ is the variable length hash of x &

opad = 0x36 repeated as many times as req.

ipad = 0x5C repeated " " " " "

Visually this looks like,