1 Building MACS using Hashing (H-MAC)

The working of HMAC starts with taking a message M containing blocks of length b bits. An input signature is padded to the left of the message and the whole is given as input to a hash function which gives us a temporary message-digest MD'. MD' again is appended to an output signature and the whole is applied a hash function again, the result is our final message digest MD. The design is as follows:

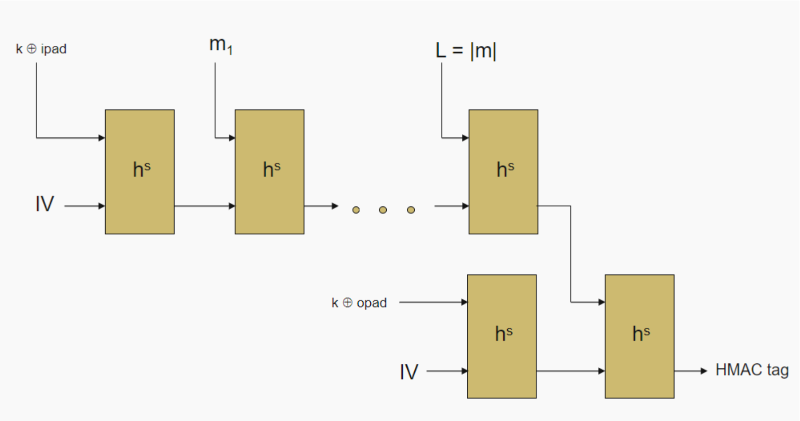

Figure 1: H-MAC scheme

- (Gen,h): A fixed length hash function
- (Gen, H): Hash function after applying MD transform to (Gen,h)
- Fixed constants- IV (initial vector), ipad(input pad) and opad(output pad)
- ipad: 0x5c repeated as many times as needed : 0x36 repeated as many times as needed

HMAC TAG for m =

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