

## Use collision resistant hash function to build H-MACs

H-MACs is a message authentication code where

1. (Gen, h) : A fixed length hash function
2. (Gen, H) : Hash function after applying MD transform to (Gen,h)
3. Fixed constants are IV, opad and ipad

$$\text{HMAC tag for } m = H_{IV}^s(k \oplus \text{opad}) \parallel (H_{IV}^s(k \oplus \text{ipad}) \parallel m)$$

The message is broken into blocks of a predefined size and repeatedly hash them using a fixed length hash function. The input to this hash is the previous block and the current message block.

The initial input is the hash of the two values which are  $(k \oplus \text{ipad})$  and IV where k is the key, ipad is the repeated inner pad and IV is the initialization vector.

The final value that is obtained as output is also hashed again with the hash of the two values which are  $k \oplus \text{opad}$  and IV where opad is the repeated outer pad.

H-MACs are usually derived from NMACs. NMACs require two different keys, whereas HMACs require only a single key which is 'xor'ed with the inner pad.

The outer pad has only one security requirement which says that the two keys should be different from one another.

The code has been explained in the comments present in the script wherever necessary.