HMAC Documentation

init:

Params:
p: prime number
bit_length: bit_length of p
ipad: fixed input pad 0x5c
opad: fixed output pad 0x36

get_key:

Returns:
Retrieves the current key

update_key:

Updates the key value with a random value generated by using the current key value as the seed.

set_key:

Params:
Takes a key as input

Sets key variable to the input value.

generate_tag:

Params:
message: message to tag
msg_len: length of message in bits

Returns:
Fixed size MAC code for the message

Appends the XOR of ipad repeated to match the size of the private key to the message with the private key. Then this new message is passed through the MD_Hash function. The output of this is then concatenated to the XOR of opad repeated to match the key and the key. This is again passed through the MD_Hash function to return the final MAC code.