Hash Based Message Authentication Code

Step 1 :

The length of the message m must be equal to the length of the key.

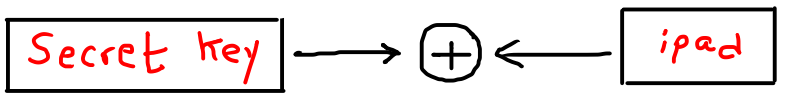
Hash Based Message Authentication Code

Step 1 :

The length of the message m must be equal to the length of the key.

Step 2 :

The secret key is XOR 'ed with ipad to produce OS1.



Where,

ipad = input pad = The String 0x36 repeated 64 times.
OS1= Output of Step1.

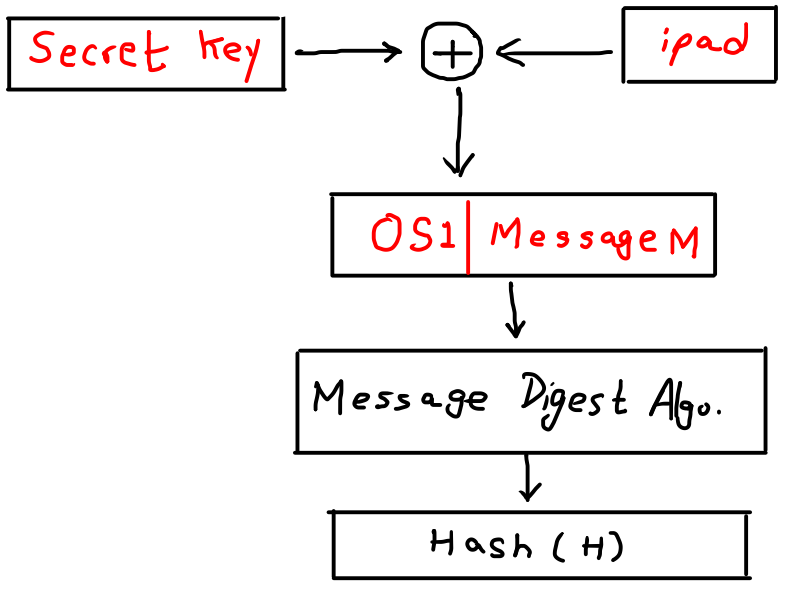
Hash Based Message Authentication Code

Step 3 :

Append the message M to output of Step 2

Step 4 :

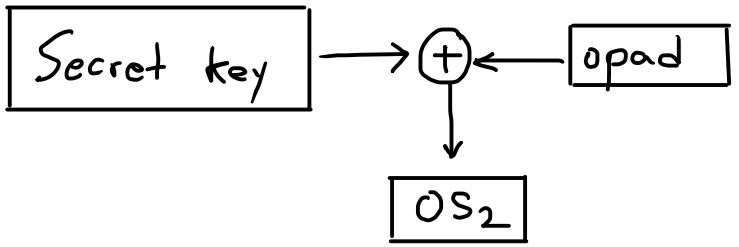
Any Message Digest (MD5 or SHA1) is applied on the output of Step 3. This will produce thr output hash.



Hash Based Message Authentication Code

Step 5 :

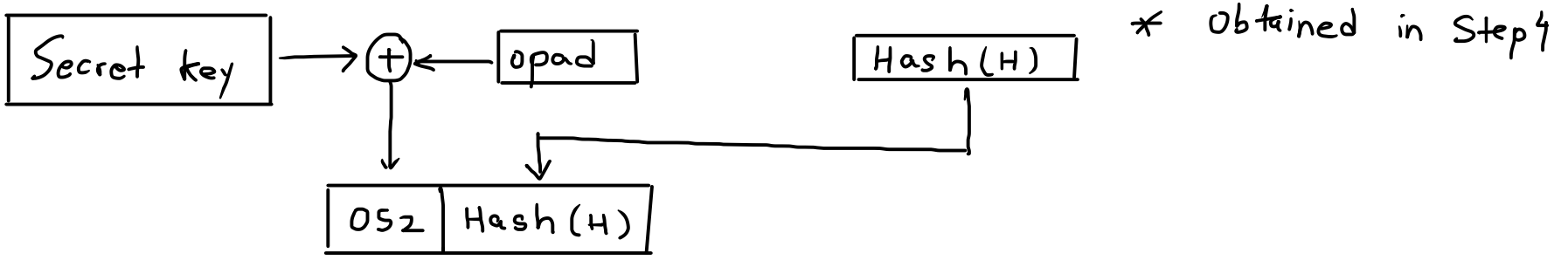
XOR the secret key K with opad to produce output variable called OS2.



Hash Based Message Authentication Code

Step 6 :

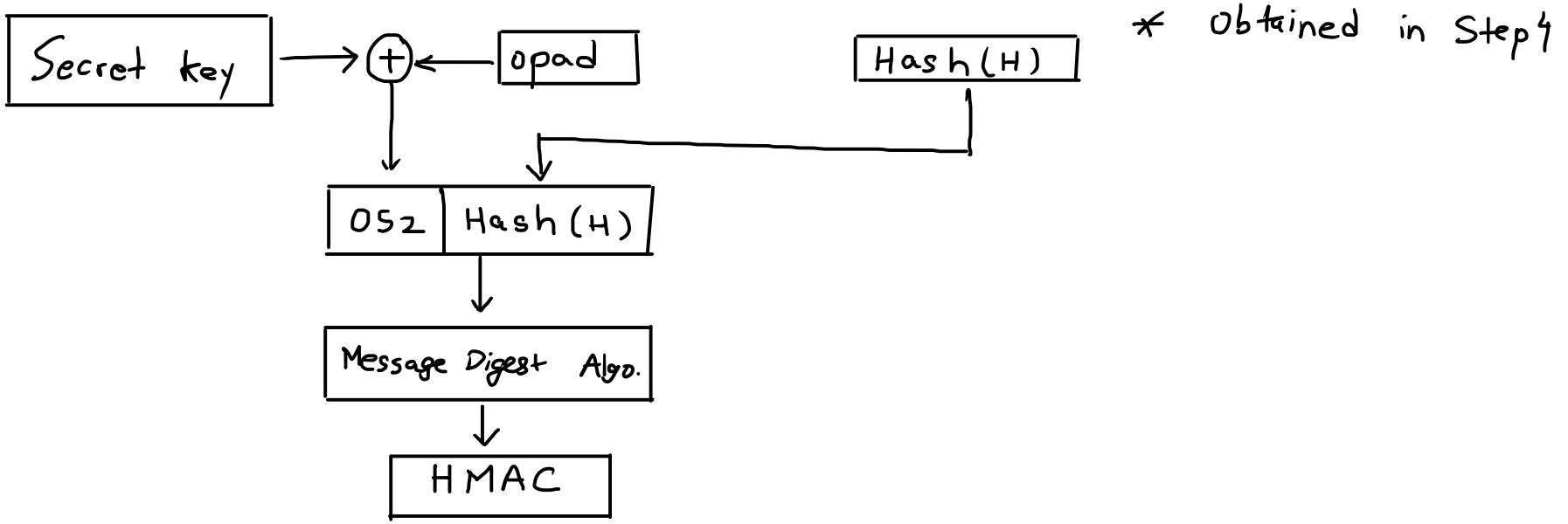
Add Hash H with OS2 and appended with output of Step 5



Hash Based Message Authentication Code

Step 7 :

Message Digest algorithm is applied on output of step 6 to generate final output called as HMAC.



Final Diagram