Semester: VI Subject: CSS Academic Year: 2023-2024

HMAC → Hash Based Message Authentication Code.

* HMAC is used to maintain the integrity of the messages sent by the sender.

Notations Used:

MD → The message digest/hash function used. (eg. MD5/SHA-1).
M → The input message.
L → The no. of blocks in the message.
b → The no. of bits in each block.
K → The shared symmetric key.
ipad → A string 00110110 repeated b/8 times.
(eg) if b = 16 bits then b/8 = 2. The string is repeated 2 times.
00110110 00110110.
opad → A string 01011010 repeated b/8 times.
(eg) if b = 32 bits then b/8 = 32/8 = 4. The string is repeated 4 times.
01011010 01011010 01011010 01011010.

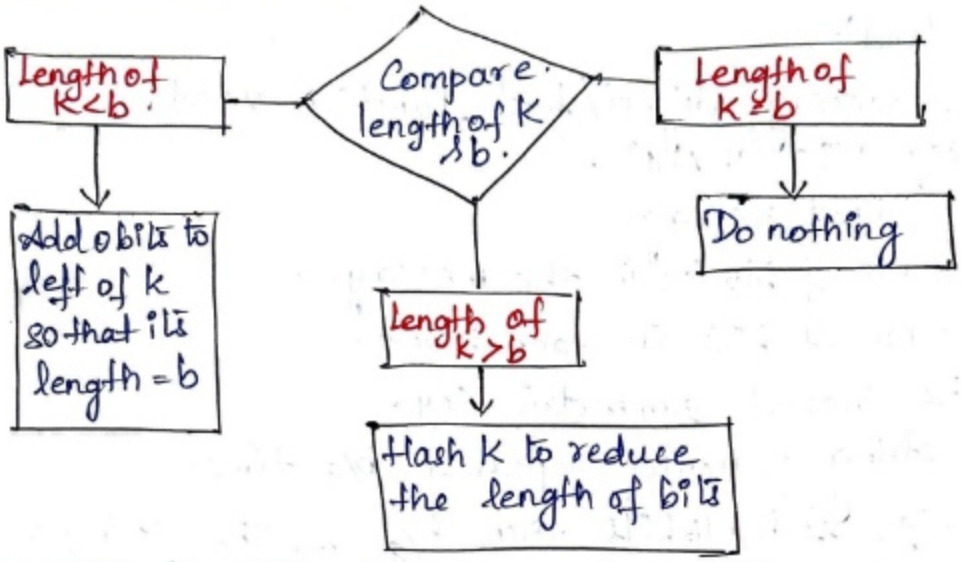
Steps in HMAC:

Step 1: Make the length of K equal to b.
Step 2: XOR K with ipad to produce S1.
Step 3: Append M to S1.
Step 4: Apply Message Digest Algorithm.
Step 5: XOR K with opad to produce S2.
Step 6: Append H to S2.
Step 7: Apply Message Digest Algorithm.

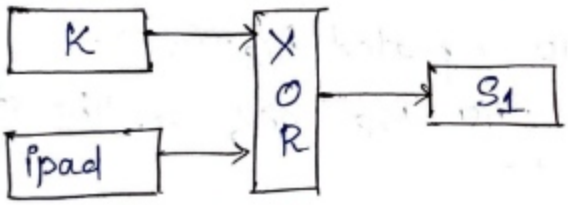
Semester : VI Subject : CSS Academic Year: 2023-2024

Step 1: Make the length of K equal to b.

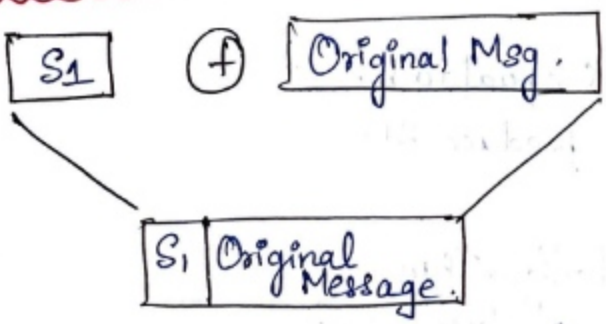
There are 3 cases, if
$K < b$, $K > b$, $K = b$.



Step 2: XOR K with ipad to produce S1.

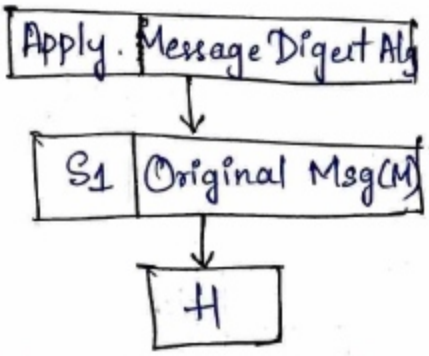


Step 3: Append M to S1

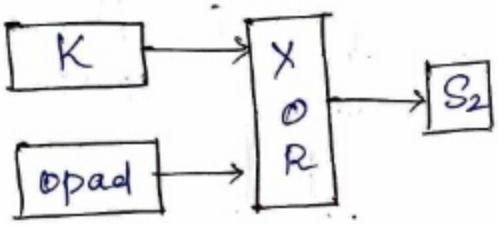


Semester : VI Subject : CSS Academic Year: 2023-2024

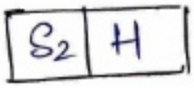
Step 4: Apply Message Digest Algorithm.



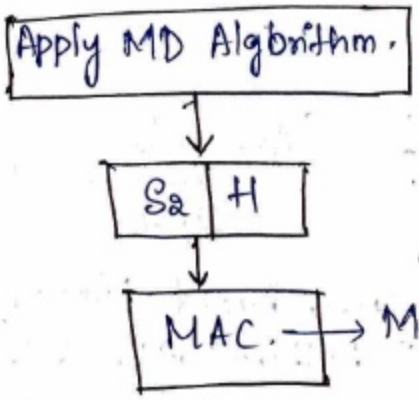
Step 5: XOR K with opad to produce S_2.



Step 6: Append H to S_2



Step 7: Apply Message Digest Algorithm.



→ Message Authentication Code.

Semester : VI Subject : CSS Academic Year: 2023 2024.

Complete HMAC Operation: