Experiment No. 03

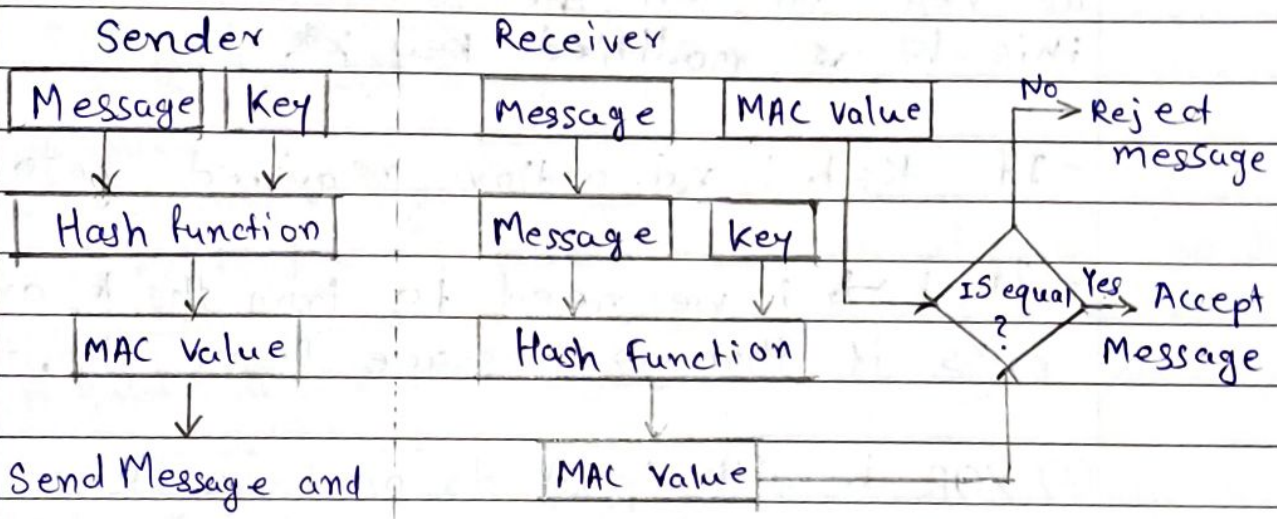
Aim: Study of different Hashing Techniques: HMAC and CMAC

Theory:

① HMAC (Hash Message Authentication Code):

ⓐ In HMAC, a hashing function is used as a MAC function to calculate the MAC value

ⓑ The hashing function could be general hash functions such as MD5, SHA-1 or SHA-2.



ⓒ Variables that are used in HMAC are as follows:-

MD = Message Digest / hash function

M = input message who's MAC is to be calculated.

L = No. of blocks in the message M
b = no. of bits in each block
K = Shared symmetric key

ipad = A string 00110110 repeated b/8 times

opad = A string 01011010

Steps -

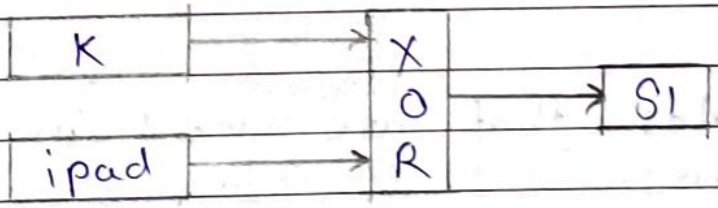
① Make the length of k equal to b -

- If $k < b$; we will add as many 0 bits as required to the left of k and call this k as modified key k*.

- If $K = b$; no action required goto step2.

- If $k > b$; we need to trim the k and so pass it through Message Digest Algorithm.

② XOR K with ipad to produce S1 :-



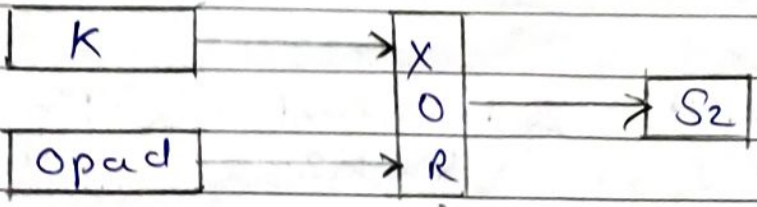
③ Append M to S1 -

S1 + Original Message =

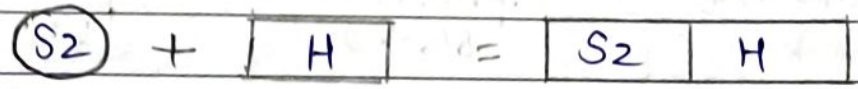
S1	Original Message (M)

④ Message Digest Algorithm:-
Now the selected message digest algorithm is applied to the output of step 3 which produces an output H.

⑤ XOR K with opad to produce S_2 -



⑥ Append H to S_2 :-



⑦ Message Digest Algorithm:
Now the selected message digest algorithm is applied to the output of step 6 which produces final MAC.

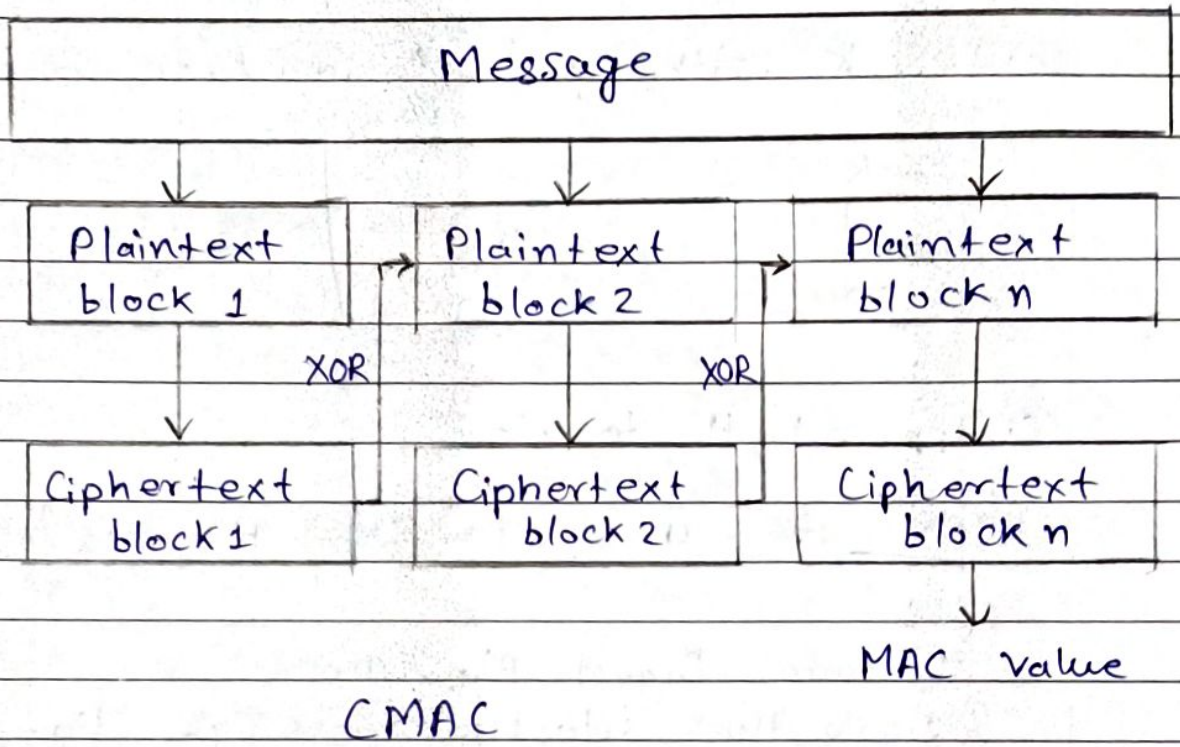
② CMAC (Cipher based Message Authentication Code) :-

ⓐ In CMAC, a symmetric block cipher encryption function is used as the MAC function to calculate the MAC value.

ⓑ CMAC is typically calculated using AES-128 algorithm and provides strongest form of

message authentication and integrity.

© CMAC is also called as One-key MAC or OMAC.



CMAC

Conclusion;

Hence, we successfully studied different Hashing Techniques: HMAC and CMAC.