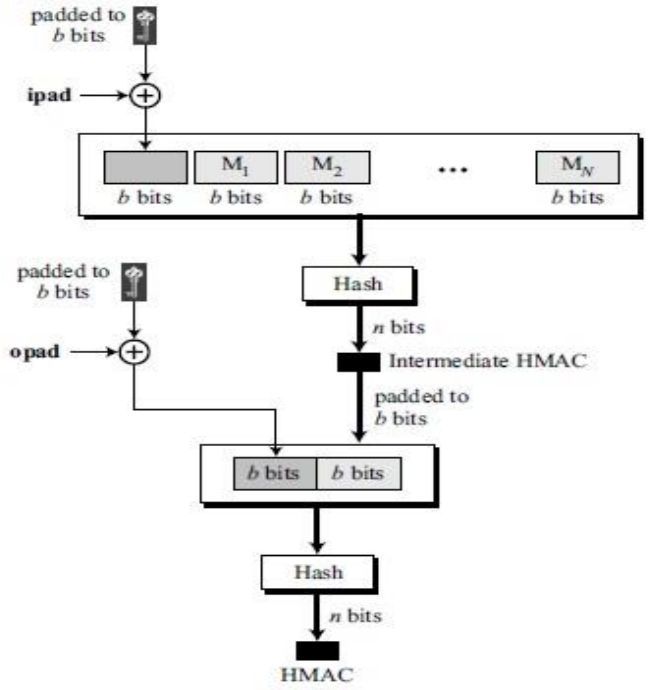
Tutorial – XII (Message Authentication)

1. Explain HMAC generation procedure with suitable diagram



Procedure:

(i) The message is divided into N blocks, each of b bits.

(ii) The secret key is left-padded with 0's to create a b-bit key. Note that it is recommended that the secret key (before padding) be longer than n bits, where n is the size of the HMAC.

(iii) The result of step (ii) is exclusive-ored with a constant called ipad (input pad) to create a b-bit block. The value of ipad is the b/8 repetition of the sequence 00110110 (36 in hexadecimal).

(iv) The resulting block is prepended to the N-block message. The result is N + 1 blocks.

(v) The result of step (iv) is hashed to create an n-bit digest. We call the digest the intermediate HMAC.

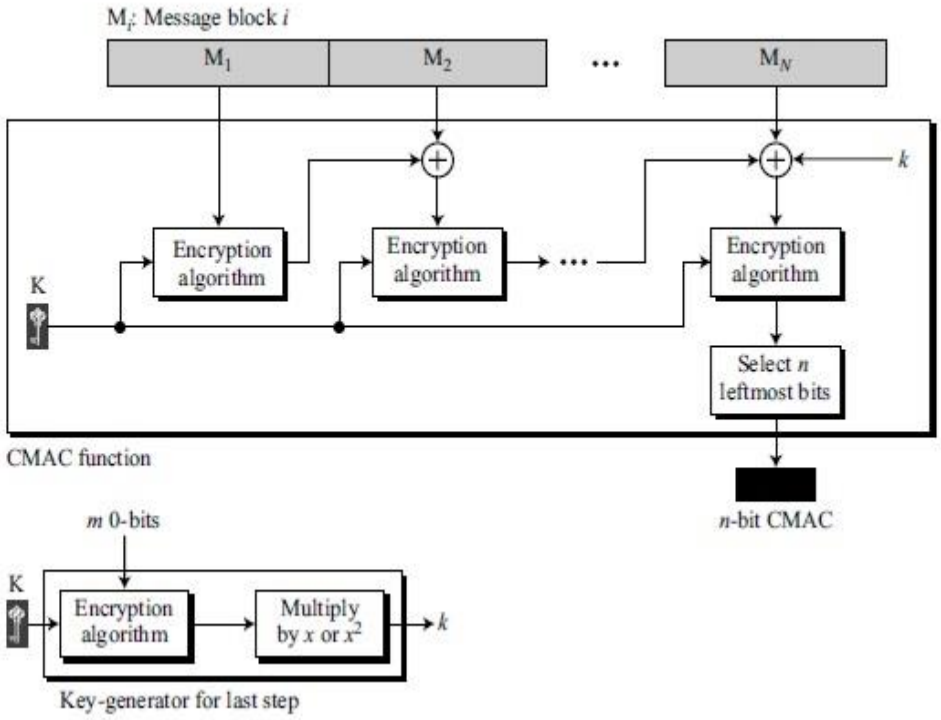
(vi) The intermediate n-bit HMAC is left padded with 0s to make a b-bit block.

(vii) Steps (ii) and (iii) are repeated by a different constant opad (output pad). The value of opad is the b/8 repetition of the sequence 01011100 (5C in hexadecimal).

(viii) The result of step (vii) is prepended to the block of step (vi).

(ix) The result of step (viii) is hashed with the same hashing algorithm to create the final n-bit HMAC.

2. Explain CMAC generation procedure with suitable diagram.



The method is similar to the cipher block chaining (CBC) mode discussed in Chapter 8 for symmetric-key encipherment. However, the idea here is not to create N blocks of ciphertext from N blocks of plaintext. The idea is to create one block of MAC from N blocks of plaintext using a symmetric-key cipher N times.The message is divided into N blocks, each m bits long. The size of the CMAC is n bits. If the last block is not m bits, it is padded with a 1-bit followed by enough 0-bits to make it m bits. The first block of the message is encrypted with the symmetric key to create an m-bit block of encrypted data. This block is XORed with the next block and the result is encrypted again to create a new m-bit block. The process continues until the last block of the message is encrypted. The n leftmost bit from the last block is the CMAC.

In addition to the symmetric key, K, CMAC also uses another key, k, which is applied only at the last step. This key is derived from the encryption algorithm with plaintext of m 0-bits using the cipher key, K. The result is then multiplied by x if no padding is applied and multiplied by x^2 if padding is applied. The multiplication is in $GF(2^m)$ with the irreducible polynomial of degree m selected by the particular protocol used.

Note that this is different from the CBC used for confidentiality, in which the output of each encryption is sent as the ciphertext and at the same time XORed with the next plaintext block. Here the intermediate encrypted blocks are not sent as ciphertext;
they are only used to be XORed with the next block.

3. Analyze attack against secret prefix MACs.