H MAC

Input: A Key of length n, an initialization vector of length n and a message of arbitrary length.

Output: Returns the hash of input message.

Algorithm:

n=16

opad = 0x36

ipad = 0x5c

Repeat opad and ipad as many times as possible such that the length is equal to n.

Find the xor of key and ipad.

Find the fixed length hash of key and initialization vector.

Find the Merkle Damgard Transformation of the arbitrary length message with the above result as initialization vector.

Find the xor of key and opad.

Find the fixed length hash of above result and the original initialization vector.

Find the fixed length hash of above result and the Merkle Damgard Transformation.

Return the result as H Mac tag.