2021201041
NVSS Maneesh Gupta

Function var_hash

Input Arguments

- Msg- the plain text message, binary string
- iv- initial vector, binary string
- here iv is a fixed constant
- any value of iv with length equal to length of P should be taken

Output

Hash value – binary string

Logic

- This is the implementation of Merkle Damgard Transform
- Here the size of each block is length of prime P in binary
- Append the length of the message as an extra block to the msg
- Input a msg block, iv to the fixed_hash function the output is taken as iv for the next iteration
- The loop continues till all the msg blocks are used

Return the output of the final block

Usage

This function is used to create HMAC