POIS ASSIGNMENT 1

TASK 8

USE COLLISION RESISTANT HASH FUNCTION TO BUILD H-MACS

THEORY

In cryptography, a keyed hash message authentication code (HMAC) is a specific type of message authentication code (MAC) involving a cryptographic hash function(hence the ‘H’) in combination with a secret cryptographic key.

We can use HMAC with multiple iterable hash functions such as MD5, SHA-1 in combination with a secret shared key.

The basic idea is to secure our data, by generating a cryptographic hash of the actual data combined with a shared secret key. The final result is sent without the secret key but the resulting hash can be used to check the transmitted or stored message.

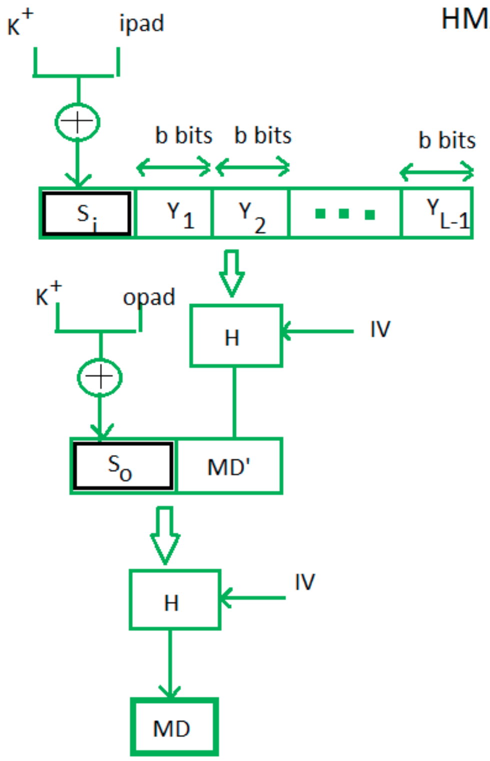
It can be used to check data for integrity and authenticity. It lets us calculate message authenticity and integrity using a shared key between two parties without the use of complex public key infrastructure involving certificates.

The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output, and on the size and quality of the key. HMAC authentication mechanism can be used in any place where security is important like public network services. For example, in public network we are sending an important file/data through a pipe or socket, that file/data should be signed and then the signature should be tested before the data is used.

WORKING :

The working of HMAC starts with taking a message M containing blocks of length b bits. An input signature is padded to the left of the message and the whole is given as input to a hash function which gives us a temporary message-digest MD’. MD’ again is appended to an output signature and the whole is applied a hash function again, the result is our final message digest MD.
Here is a simple structure of HMAC:

HMAC construct



Here, H stands for Hashing function,
M is the original message
Si and So are input and output signatures respectively,
Yi is the ith block in original message M, where I ranges from [1, L)
L = the count of blocks in M
K is the secret key used for hashing
IV is an initial vector (some constant)
The generation of input signature and output signature Si and So respectively.

$S_i = K^+ \oplus \text{ipad}$ where K^+ is nothing but K padded with zeros on the left so that the result is b bits in length

$S_o = K^+ \oplus \text{opad}$ where ipad and opad are 00110110 and 01011100 respectively taken b/8 times repeatedly.

$$MD' = H(S_i \,||\, M)$$

$$MD = H(S_o \,||\, MD') \quad \text{or } MD = H(S_o \,||\, H(S_i \,||\, M))$$

To a normal hash function, HMAC adds a compression instance to the processing. This structural implementation holds efficiency for shorter MAC values.