Module `crypto-lib.hmac.hmac`

Classes

`class H_MAC (type=1)`

Class for making a hash based MAC for genrating a tag in CCA-secure encryption schemes. These are faster than the CBC MAC.

Initialize the type of the one way function.

Methods

`def key_gen(self, n)`

Generate an n-bit key for performing MAC using PRG.

`def mac(self, message, key)`

Genrate a tag for a given message and a key. The tag is a fixed length value genrated by taking the hash in two stps using the previously defined MerkleDamgard function.

`def verify(self, message, key, tag)`

Verify if the message and the tag generated match up.