Module `crypto-lib.mac.mac`

Classes

`class CBC_MAC (type=1)`

Implements a Cipher Block Chaining Message Authentication Code which can be used to generate a tag which verifies if the ciphertext provided is valid corresponding to the tag.

Initialize the type of one-way function to use.

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 due to usage of cipher-block-chaining.

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

Verify if the message and the tag pair are valid or not.