MAC Documentation

__init__(self, t):

Input variables: t(0,1)

- t decides which secure mode of cpa is to be used, by initializing self.mode

genKey(self,x):

Input variables: n(int)

- Generates a random binary string of length n

getxor(self, s1, s2):

Input variables: s1(str), s2(str)

- Performs xor between to binary strings and returns the outcome in binary string format

mac_simple(self, prg, prf, m, k=None):

Input variables:prg(prg obj), prf(prf obj), k (str), m(str)

- Takes in a prg object, and a prf object, key and a message m
- Implements a fixed-length secure MAC using the prg and prf objects
- Returns t, the generated mac

mac(self, l, m, k=None):

Input variables: prg(prg obj), prf(prf obj), m(str), n(int), k(str)

- Implements a variable length mac
- If key is not given, then a random key is generated using length n = len(m)/l ang

genKey()

- Given a key, message mac_simple is used to make a variable-length mac
- Returns t, the generated mac

mac_vrfy(self, prg, prf, k, m, t):

Input variables: prg(prg obj), prf(prg obj), m(str), k(str), t(str)

- Implements the verification step of ecure mac scheme