CCA 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

cca(self, prg, prf, cpa, mac, n, m):

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

- Implements a variable length cca for givn block length n and message m

mac_dec(self, prg, prf, cpa, mac, k1,k2, cip, iv_init, m_len):

Input variables: prg(prg obj), prf(prf obj), cpa(cpa obj), mac(mac obj), k1(str), k2(str), iv_init(int), m_len(int)

- Implements the verification step of secure cca scheme