Module `crypto-lib.cca_secure.cca_secure`

Classes

`class CCA (type=1)`

Complete class for performing the complete procedure from key generation, encryption and decryption for a cpa-secure communication. The previously defined MAC, PRG and PRF classes are used. CCA-secure implies that an adversary with access to encryption server and the decryption server cannot break the encryption scheme.

Methods

`def decrypt(self, cipher, key)`

Given a ciphertext and the key, generate the message which was encrypted. Also verify if the cipher and the tag match.

`def encrypt(self, message, key)`

Given a message and a key, return the encrypted cipher text (along with the tag).

`def key_gen(self, n)`

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