Module `crypto-lib.cpa_secure.cpa_secure`

Classes

```
class CPA
```

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

Methods

```
def decrypt(self, cipher, key)
```

Given a ciphertext and the key, generate the message which was encrypted.

```
def encrypt(self, message, key)
```

Given a message and a key, return the encrypted cipher text.

```
def key_gen(self, n)
```

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