CPA Secure Documentation

This contains 2 classes, one to encrypt using a CPA secure encryption scheme and one to decrypt using a CPA secure decryption scheme.

CPA_secure_encrypt:

init:

Params:
p: prime number
n: number of bits

get_key:

Returns:
Retrieves the key value

update_key:

Generates a new key taking the previous key as a seed.

encrypt:

Params:
message: the message to be passed. Is of fixed length, the same as the prime number bit_length.

Returns:
Encrypted message

Takes a random bit string of n size, computes its PRF, takes a xor with the message and then concatenates this to the random bit string to form the cipher text.

CPA_secure_decrypt:

init:

Params:
p: prime number
n: number of bits

decrypt:

Params:
cipher: cipher text
key: private key for CPA security.

Returns:
Decrypted message

Breaks the cipher text into 2. Computes the PRF of the random bit string, computes the xor again with the second half and retrieves the original message.