CCA Secure Documentation

This implements the CCA secure encryption and decryption classes

CCA_secure_encrypt:

init:

Params:
p: prime number
n: number of bits in block

get_key_cpa:

Returns:
The CPA encryption private key

get_key_vlmac:

Returns:
The Variable Length MAC private key

encrypt:

Params:
message: the message to be encrypted
msg_size: the size of the variable length message to be encrypted

Returns:
cipher_dec: the cipher text in decimal
tag: the tag in decimal
cipher_size: the size of cipher in binary
tag_size: the size of tag in binary

Breaks the message into n size blocks, encrypts them using CPA, then combines them into a bit string, further computes the variable length mac on this combined bit string, and concatenates the CPA encrypted cipher text with this generated tag. These results may be returned in the concatenated for or separated form.

CCA_secure_decrypt:

init:

Params:
p: prime number
n: number of bits in one block

decrypt:

Params:
cipher_dec: cipher text in decimal
tag_dec: tag for the cipher text in decimal
key_cpa: the CPA private key during encryption
key_vlmac: the VLMAC private key during generation of tag

cipher_size: the size of the cipher text in binary bits
tag_size: the size of the tag in binary bits

Returns:
Decrypted message if the message is untampered

The cipher text is verified using VLMAC. If the authenticity is established, the cipher text is broken down into its constituent encrypted blocks. Each of those blocks are decrypted and concatenated to form the final decrypted message.