Secure MAC Documentation

This implements fixed length MAC and variable length MAC classes

fixedLengthMAC:

init:

Params:
p: prime number
n: number of bits

get_key:

Returns
Retrieves the key

set_key:

Params
key: Input key

Sets the key to the input value.

generate_tag:

Params:
message: The message to be tagged

Returns:
Tag for the input message

Passes the message through a PRF given the private key to generate the tag.

verify:

Params:
message: the message to be verified
key: the private key at generation time
Tag: the tag generated for the message

Returns:
True if the message and the tag match
False if the message and the tag don't match

Recomputes the tag for the message given the private key. If the tags match returns true. Else false.

variableLengthMAC:

init:

Params:
p: prime number

n: number of bits in one block

Initialises a PRG, a fixed length MAC and a n/4 random bit string

get_key:

Returns:
Returns the key for the fixed length MAC

update_key:

Updates the fixed length MAC key with the random string generated taking the present MAC key as input

get_nby4_bits:

Params:
tag: input tag from which first n/4 bits to be extracted

Returns:
First n/4 bits of input string

generate_tag:

Params:
message: the variable length message to be tagged
msg_size: the length of the variable length message
rby4: used to input preexisting random n/4 bit length string. Used for computation during verification
key: used to input preexisting key. Used for computation during verification.

Returns:
a tag in the decimal form for the message

Breaks the message into various blocks of equal size of n/4 bits and pads with 0 if needed. Later computes the PRF of random n/4 bit string concatenated with number of message blocks encoded into n/4 bits, block number encoded in n/4 bits and the message block of n/4 bits. These PRFs are then concatenated with the random n/4 string and is returned as the final tag.

verify:

Params:
message: the message to be verified
msg_size: size of the variable length message
key: private key at generation time
tag: the tag generated for the message

Returns

True if the message matches to the tag
False if the message doesn’t match to the tag

Recomputes the tag on the message given the private key as well as the random n/4 bit string. If this tag matches the input tag, returns true. Else false.