MD Hash Documentation

This class implements the Merkle-Damgard Transform Hash Function.

init:

Params:
p: prime number
bit_length: the bit length of each block

find_hash:

Params:
x: variable length input
size: size of x in bits

Returns:
Hash of the input using the Merkle Damgard Transform

sBreaks the input into blocks of at most bit_length size. First block is input into a DLP Hash with an initialisation vector that is initialised to 0^bit_length. Next block is then input along with the output of the DLP Hash map to form a new output. This is done iteratively to reach a bit_length size hash of the input.