Module cryptolib.merkle_damgard.merkle_damg ard

Classes

class MerkleDamgard

Class for converting the fixed length hash function to a variable legth one by using a simple chaining method.

Initialize the IV

Methods

def hash(self, message)

Given a message (list of bitstrings), get the hash.