DLP Hash Documentation

This class implements the DLP Hash function

init:

Params:

p: prime number

bit_length: number of bits in prime number

prime_factors:

Params:

number: any positive integer

Returns:

A list of prime factors of the input positive integer

find_primitive_root:

Returns:

The primitive root of the prime number p.

Checks for all numbers below p, if the modular exponent is 1. If so, return such number, else return -1

find_hash:

Params:

x1: first half of the 2*n bit string

x2: second half of the 2*n bit string

Returns:

The modular exponent of the form (g^x1*h^x2)mod p