

HASHING FUNCTION:

1. variableLengthHash-

Function to generate variable length hash from fixed length hash using Merkle-Damgard Transform

Parameters	Datatype	Description
msg	str	Input whose hash is to be generated
initial_vector	str	Random chosen noise
g	int	A primitive root of p
h	int	Another primitive root of p
p	int	Prime number p to use in DLP
fixed_length	int	Length of fixed hash output

Return:

(str) : Binary hash of size half of that of input

Called by:

Main code

Caller of:

- fixedLengthHash
- decimalToBinary