Hash Documentation

binstring(self,x):

Input variables: x(int)

- Generates and returns a binary string representation for a given number x

setStrLen(self,s,n):

Input variables: s(str),n(int)

- Returns the given string s set to the given length n

getint(self,s):

Input variables: s(str)

- Returns the integer value of given binary string s

genKey(self,x):

Input variables: n(int)

- Generates a random binary string of length n

getxor(self, s1, s2):

Input variables: s1(str), s2(str)

- Performs xor between to binary strings and returns the outcome in binary string format

G(self,n, num):

Input variables: n(int), num(int)

- Generates a cyclic group G of order q > num -1
- Returns p, order q, generator g, and h which is a random element in G

hash_simple(self, n, x):

Input variables:n(int), x(str)

- Generates a code of length n for a given message x by implementing a fixed-length collision resistant hash function

hash _final(self, x, iv=None, n=None):

Input variables: x(str), iv(int), n(int)

- Takes a message x a number iv and another number n(length of coded block) as input
- Uses hash_simple() to implement a variable-length collision resistant hash function