PRG Documentation

__init__(self, g, p):

Input variables: g, p

- g and p are the prime numbers required for discrete logarithm

binstring(self, g, p):

Input variables: x

- Takes a number x and outputs it's corresponding binary representation in the form of a string
- It's a helper function

dlp(self,x):

Input variables: x

- g and p are the prime numbers required for discrete logarithm
- Returns (g^(x))%p

msb(self,x):

Input variables: x

- Returns the most significant bit of the number x

prg_1(self, s):

Input variables: s

- Implements a (l+1) expansion factor PRG by calling DLP and MSB

encrypt(self, x, expFactor):

Input variables: x, expFactor

- Implements a variable-length output PRG by using prg_1