

PRG FUNCTIONS:

1. hc-

Function to get hardcore predicate bit using Goldreich-Levin Theorem

Parameters	Datatype	Description
x	str	Input of one-way function

Return:

(str): 1 bit hardcore predicate of x

Called by:

- PRG

Caller of:

None

2. owf-

One-way function with candidate as Discrete Log Problem

Parameters	Datatype	Description
x	int	Input of one-way function
g	int	Generator
p	int	Prime

Return:

(int): Dlp function output

Called by:

- PRG
- fixedLengthHash

Caller of:

None

3. PRG-

Function to generate pseudo-random output from a seed

Parameters	Datatype	Description
seed	str	Binary input seed
l	int	Length to which to expand
g	int	Generator
p	int	Prime

Return:

(str): pseudo-randomly generated number of l length

Called by:

- PRF

Caller of:

- hc