2021201041
NVSS Maneesh Gupta

Utility Functions

Function: dec_to_bin

Input arguments:

x = integer base 10

Output

A string in binary of the input x

Logic

Simple conversion of integer base 10 to integer base 2 and then to a string

Usage

This is used when the input is required in binary string format but we have an integer

Function hardcore_predicate

Input Arguments

S = binary string

Output

Returns either 0 or 1 basing on the input

Logic

MSB is the hardcore predicate for the discrete logarithm

For the value s if $msb(s) = \begin{cases} 0 \; if \; s < p/2 \\ 1 \; if \; s > p/2 \end{cases}$

Usage

This is used to generate the MSB of the input S

Function one_way_function

Input Arguments

X= binary string

Output

Binary string

Logic

We consider discrete logarithm as a one-way function. $f_{p,g}(x) = g^x \ mod \ p$

The above implemented consider p being a prime and g is the generator

Usage

This is used in Pseudo Random Generator, Fixed length hash function

Function function_G

Input Arguments

X = binary string

Output

Binary string

Logic

Here the functions hardcore_predicate and one_way_function are called.

The function outputs are concatenated and then sent as the output

Usage

This function is called multiple times in the Pseudo Random Generator

Function prg

Input Arguments

X = binary string

Length=integer

Output

A binary string of length is equals to input argument length

Logic

Using the function_G output, the last character is taken and the remaining output is again given as input for the function_G. This is repeated length times.

Usage

This is the basic function used in pseudo random function (PRF).