

Filename: prg.py

Running instruction: `python3 prg.py <seed>`

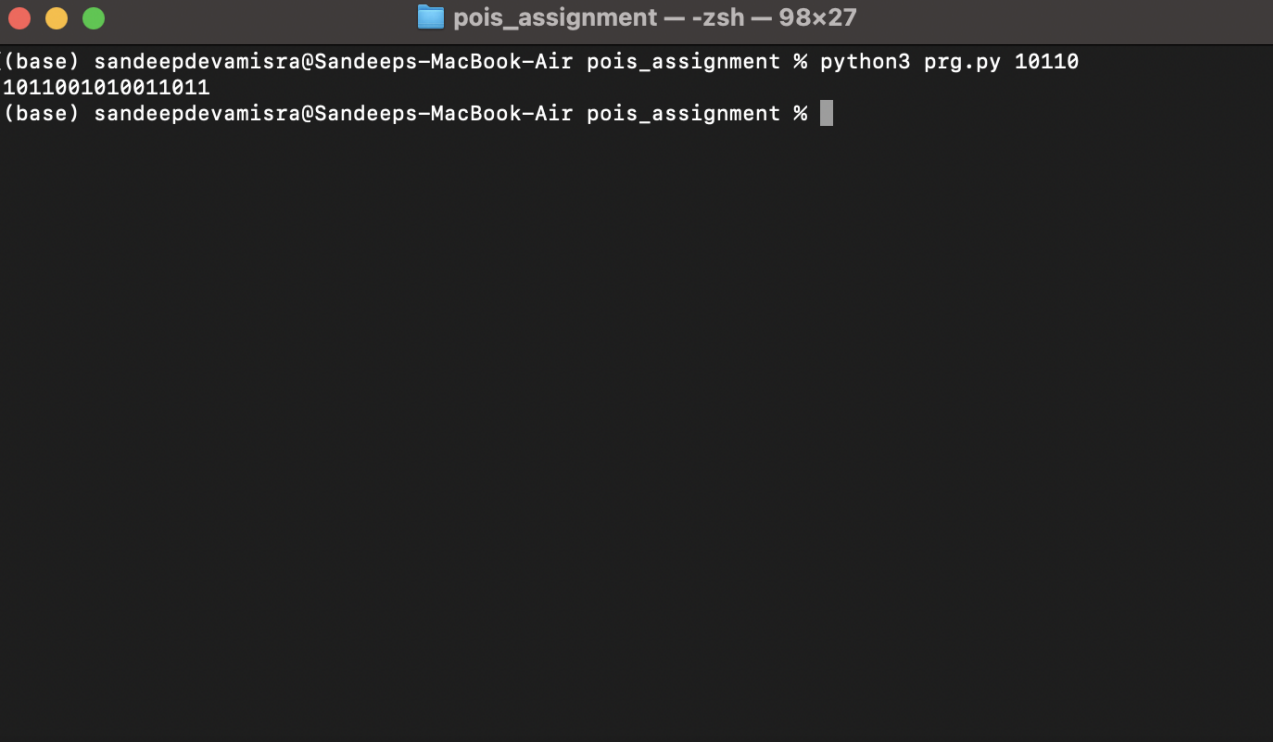
Input: seed

Class: PRG

Function: `l_func`, `h_func`, `g_func`, `print`

There are two primary functions `g_func` and `h_func`. `g_func` takes a bit string as input. It will iterate from $i=0$ to $l(n)-1$, where $l(n)$ is calculated using a helper function `l_func` that takes the seed length as input and returns an integer. Inside the for loop of `g_func` the input string is divided into two equal halves and both the halves are given as input to the `h_func`. The last bit of the output string returned by `h_func` is extracted and appended to the final result and this string (with one-bit lesser) is again used for the next step till the end of the iteration.

The `h_func` calculates the DLP using the left half of the string. Then the hardcore bit is calculated through the usual way, i.e. XOR of (left half & right half bits). A string concatenated by the DLP, right half of the string and the hardcore bit is return by the `h_func`



```
pois_assignment — zsh — 98x27
(base) sandeepdevamisra@Sandeeps-MacBook-Air pois_assignment % python3 prg.py 10110
1011001010011011
(base) sandeepdevamisra@Sandeeps-MacBook-Air pois_assignment %
```