

Filename: prf.py

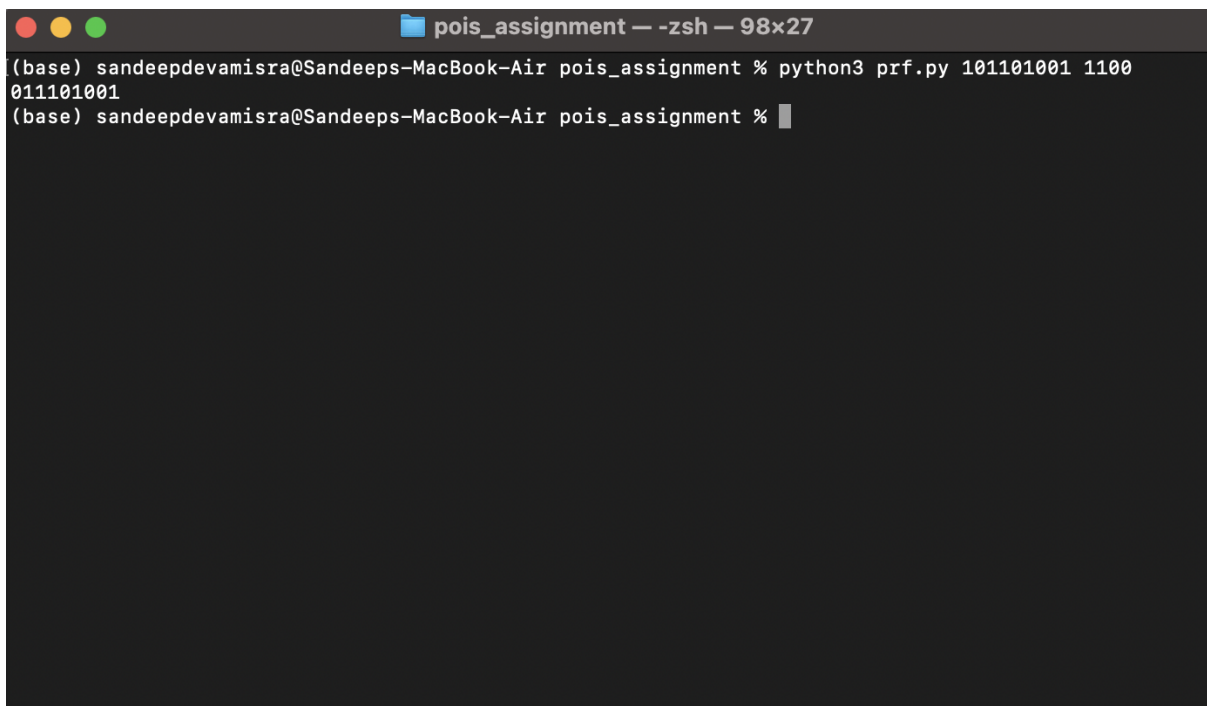
Running instruction: `python3 prf.py <seed> <input_bit>`

Input: seed, input_bit

Class: PRF

Function: l_func, h_func, g_func, print, generate

The implementation of h_func, and g_func is similar to that of the PRG. In l_func we have used a polynomial different from that of PRG. The only difference here is that there is an additional generate function that has a loop which iterates through the inp_bit. It first obtains the PRG based on the input seed. Then if the inp_bit is 0, it returns the left half of the PRG, and the right half. Also the seed is reinitialised with this new output value. After the end of the iteration, we can obtain the output.



```
pois_assignment — -zsh — 98x27
(base) sandeepdevamisra@Sandeeps-MacBook-Air pois_assignment % python3 prf.py 101101001 1100011101001
(base) sandeepdevamisra@Sandeeps-MacBook-Air pois_assignment %
```