

Filename: cpa.py

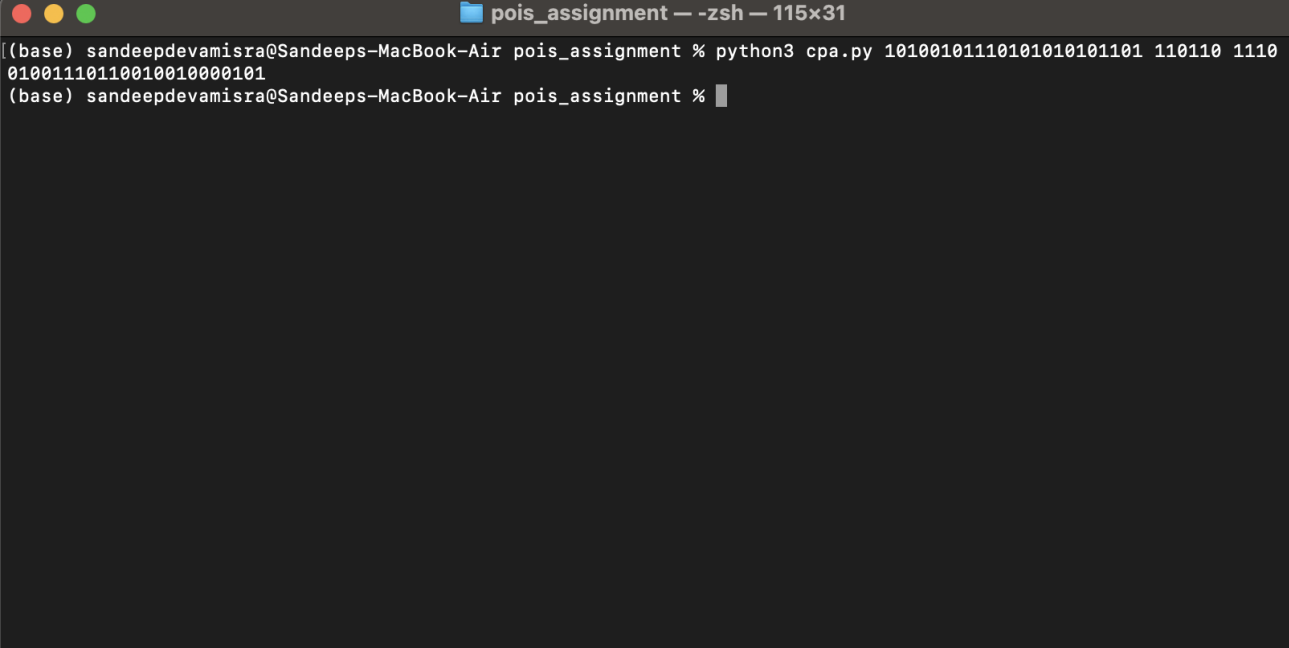
Running instruction: `python3 cpa.py <plaintext> <seed> <counter>`

Input: plaintext, seed, counter

Class: CPA

Function: generate

The PRF class is imported and used here directly. Inside the generate class, a loop is run till that length of the input plaintext. The counter value is incremented by 1. A block of plaintext is extracted, the size of which is initialised beforehand. The seed and the counter are given as input to the PRF object which generates the PRF value. The PRF obtained and the block bits are XORed and the result obtained is appended to the final result.



```
pois_assignment — zsh — 115x31
(base) sandeepdevamisra@Sandeeps-MacBook-Air pois_assignment % python3 cpa.py 101001011101010101101 110110 1110
01001110110010010000101
(base) sandeepdevamisra@Sandeeps-MacBook-Air pois_assignment %
```