

Filename: mac.py

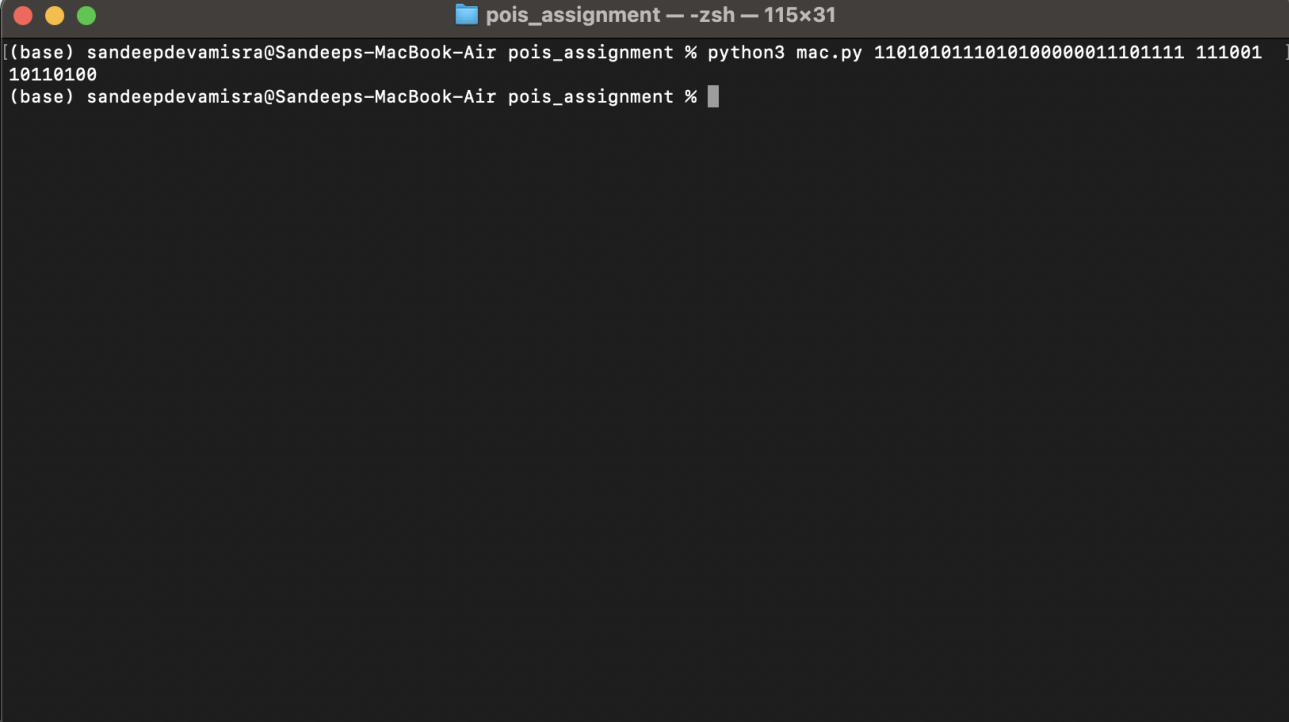
Running instruction: `python3 mac.py <plaintext> <seed>`

Input: plaintext, seed

Class: MAC

Function: generate

The PRF class is imported and used here directly. The length of plaintext is encoded as bit string and then it is used as input, along with the seed to the PRF object to generate the PRF value. We will initialise a variable with this PRF value. A loop is then run till the length of the plaintext, the block of the plaintext is extracted and XOR operation is performed between bits of block and the initial value we calculated. This XORed result is used as input to the PRF object along with the seed. The result obtained is used to reinitialise the initial value. These steps are performed till the loop ends and finally the result is obtained.



```
pois_assignment — zsh — 115x31
(base) sandeepdevamisra@Sandeeps-MacBook-Air pois_assignment % python3 mac.py 1101010111010100000011101111 111001
10110100
(base) sandeepdevamisra@Sandeeps-MacBook-Air pois_assignment %
```