

Filename: hmac.py

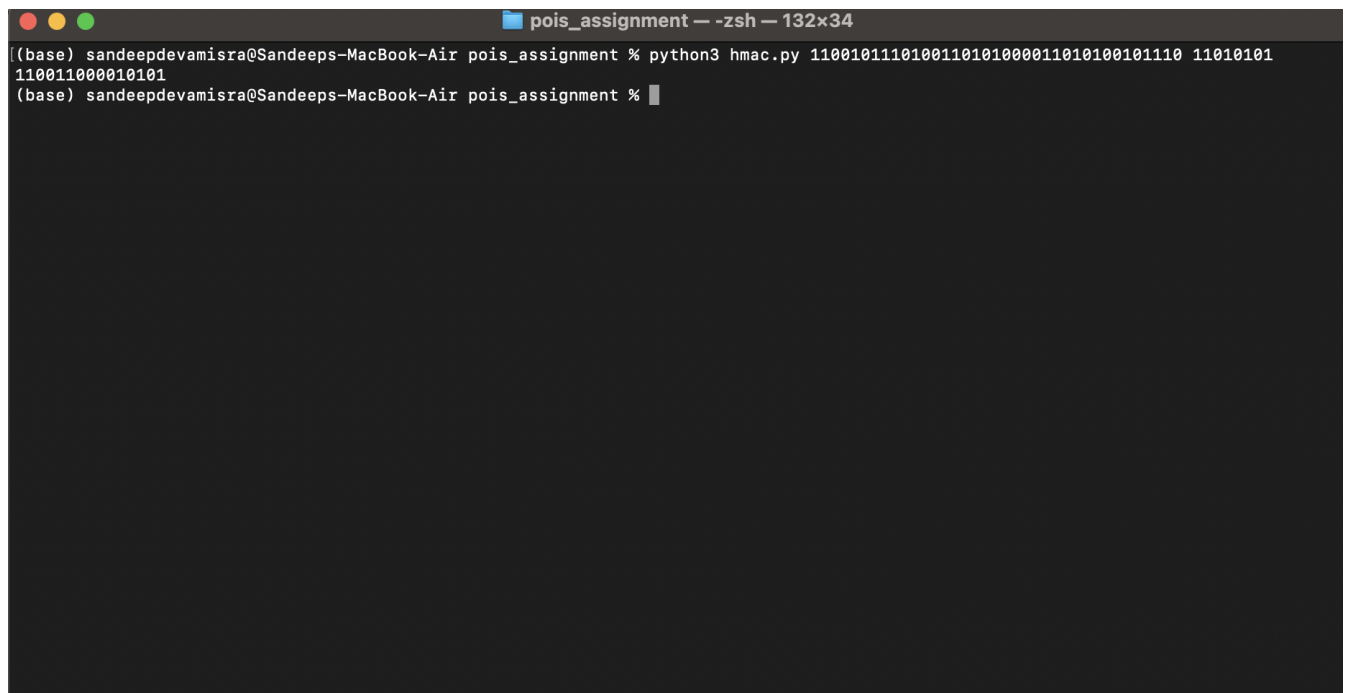
Running instruction: `python3 hmac.py <plaintext> <seed>`

Input: plaintext, seed

Class: HMAC

Function: generate

The DLP\_HASH class is imported and used here directly. The ipad and opad will be initialised according to the standard values. The generate function will first pad these ipad and opad values by repeating their values as many times as required and then calculate the XOR of seed and the ipad. The XORed value and an initialisation vector will be given as input to the DLP\_HASH object. Inside a loop, a block of plaintext will be extracted and will be given as input to the DLP\_HASH object along with the previous output. The output will be obtained and again this output and another block of plaintext will be given to the DLP\_HASH to obtain an output. After the loop terminates, the length of the message(encoded as bit string) and the output will again be given to the DLP\_HASH. Let's call the output now generated as output1. Another output, called output2 will be obtained by giving the output1 and the initialisation vector to the DLP\_HASH object. Finally these output1 and output2 will be given as input again to another DLP\_HASH object to obtain the final output.

A terminal window titled "pois\_assignment --zsh-- 132x34" is shown. The prompt is "(base) sandeepdevamisra@Sandeeps-MacBook-Air". The user enters the command "python3 hmac.py 11001011110100110101000011010100101110 11010101110011000010101". The prompt changes to "(base) sandeepdevamisra@Sandeeps-MacBook-Air" and the user enters "pois\_assignment %". The terminal background is dark, and the text is white. The window has standard macOS window controls (red, yellow, green buttons) in the top left corner.

```
(base) sandeepdevamisra@Sandeeps-MacBook-Air pois_assignment % python3 hmac.py 11001011110100110101000011010100101110 11010101110011000010101
(base) sandeepdevamisra@Sandeeps-MacBook-Air pois_assignment %
```