

Filename: merkle\_damgard.py

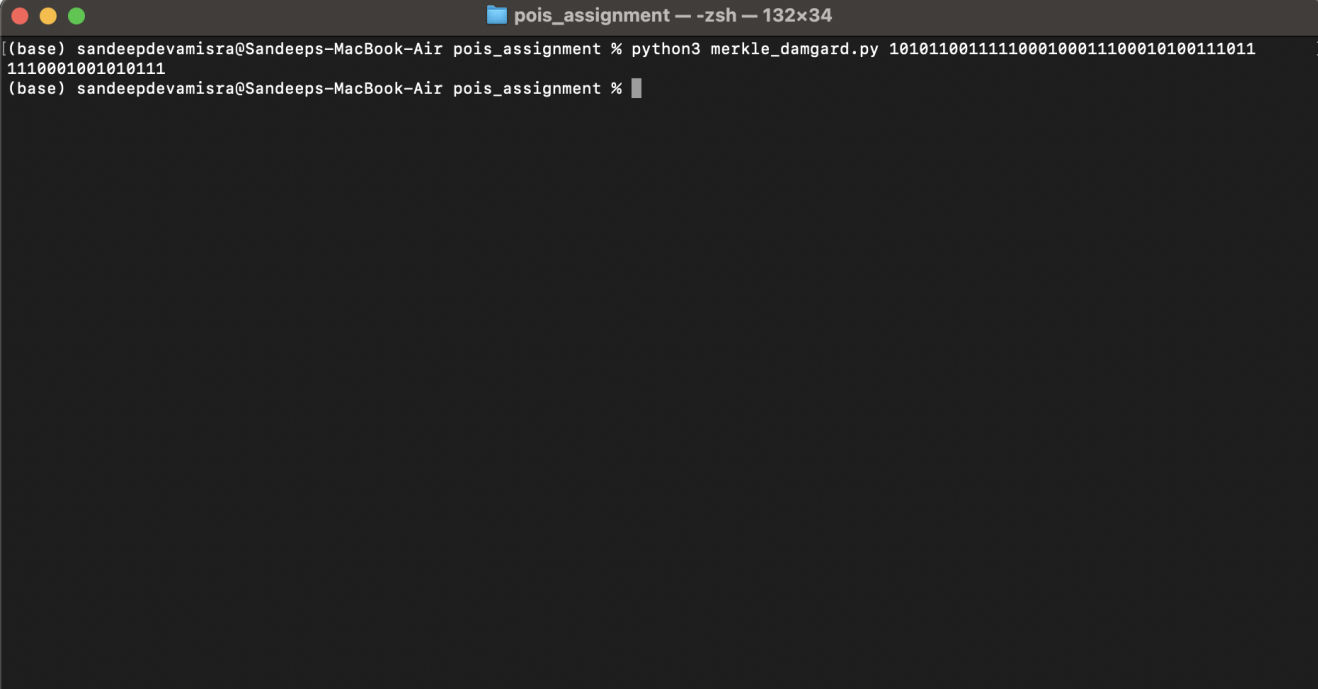
Running instruction: `python3 merkle_damgard.py <plaintext>`

Input: plaintext

Class: MERKLE\_DAMGARD

Function: generate

The DLP\_HASH class is imported and used here directly. The generate function will have a loop that iterates till the length of plaintext. The block of plaintext is extracted and given as input to the DLP\_HASH object along with an initialisation vector containing zeros of length equal to the block size. The output generated will again be given as input to the DLP\_HASH object along with another block of plaintext. After the iteration is over, in the final step, the length of the plaintext is encoded as a bit string and given as input to the DLP\_HASH object along with the output. The output generated after this will be the final output.

A screenshot of a macOS terminal window titled "pois\_assignment - zsh - 132x34". The terminal shows a user prompt "(base) sandeepdevamisra@Sandeeps-MacBook-Air" followed by the command "pois\_assignment % python3 merkle\_damgard.py 101011001111100010001110001010011101110001001010111". The output of the command is displayed on the next line: "1110001001010111". The prompt then changes to "pois\_assignment %" and a cursor is visible.

```
(base) sandeepdevamisra@Sandeeps-MacBook-Air pois_assignment % python3 merkle_damgard.py 101011001111100010001110001010011101110001001010111
1110001001010111
(base) sandeepdevamisra@Sandeeps-MacBook-Air pois_assignment %
```