**Network Security**

Assignment 4: Project **0**

**Herschelle Gupta 2019045 | Ritik Vatsal 2019321**

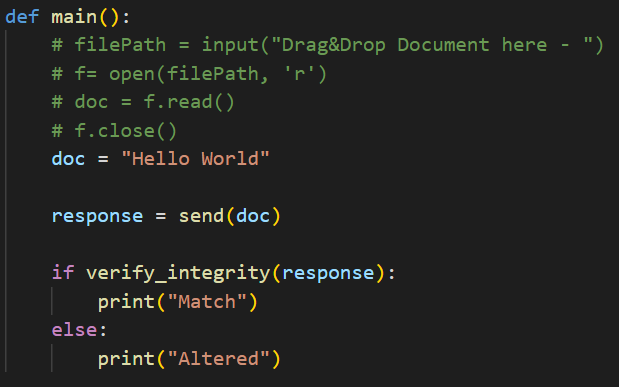
**Setup**

For execution, first launch ***server.py*** and then ***client.py.***

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

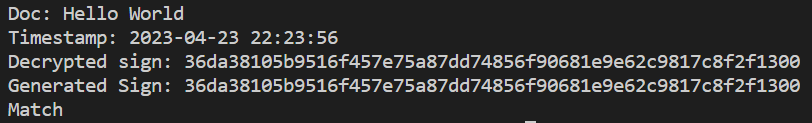
**Input/Output**

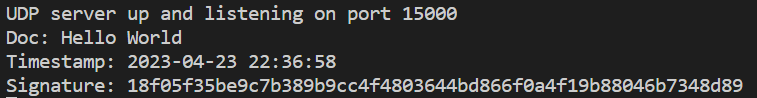
Input

In the client file, modify the doc variable.  


Output  
  
Client ~ Timestamp and Decrypted signature - received from the server

~ Generated signature - calculated using doc and timestamp received



Server - Current Timestamp and generated signature  


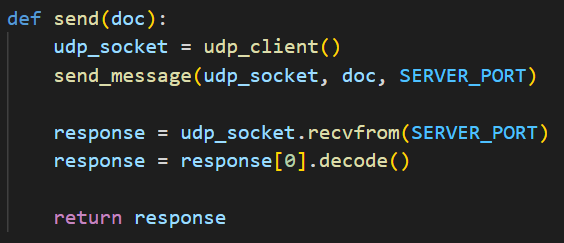
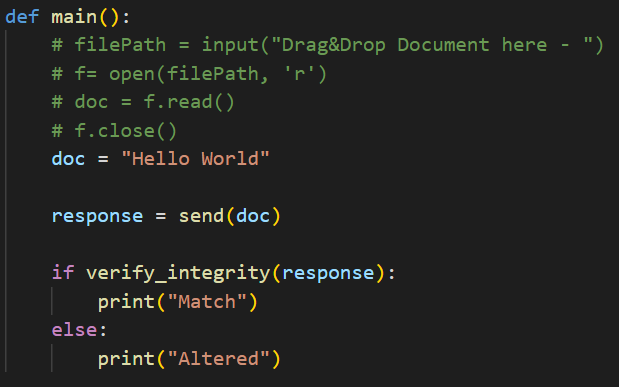
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

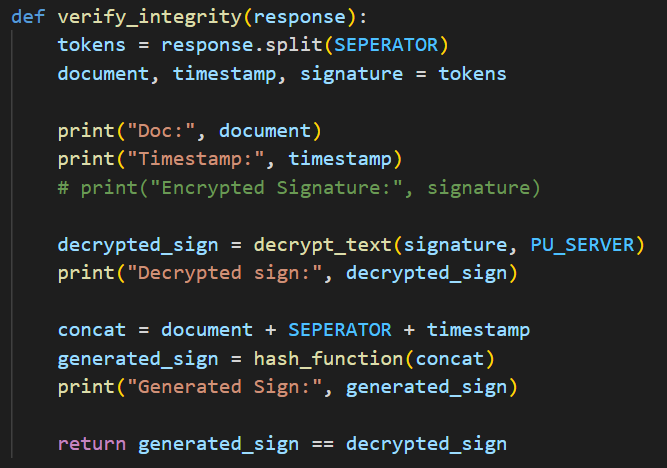
**Current Time-**

We are using Python's inbuilt datetime library to get the time from the system. The system time is synced automatically at regular intervals using the Network Time Protocol (NTP) server. We then send this time using encryption from our server to the client to ensure security and avoid Man in the middle attacks.  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

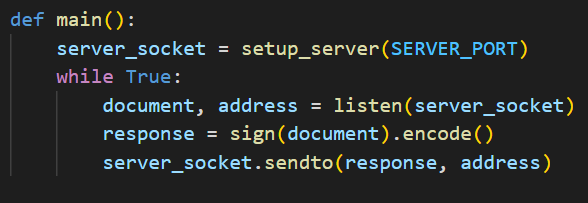
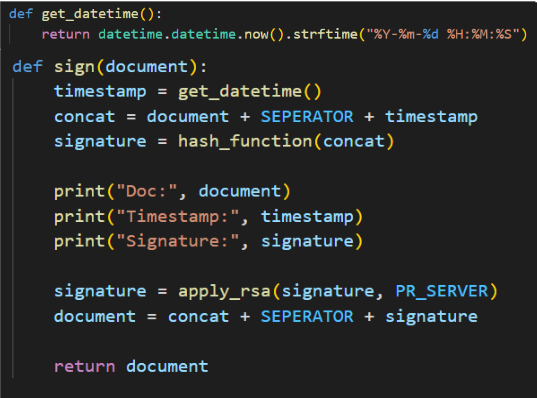
**Working -**

Client

  
 Initialisation Sending Document via UDP to the server

   
Verifying Integrity of messages by comparing the hash received from server with the current hash of the document

Server

  
Setting up UDP server  
  
  
Generating timestamps and using RSA for signature

\*\*\*