Network Security

Programming Exercise-4

Algorithm to Pick the Project

k=(A1+A2)%3
k=(1019+1039)%3=0

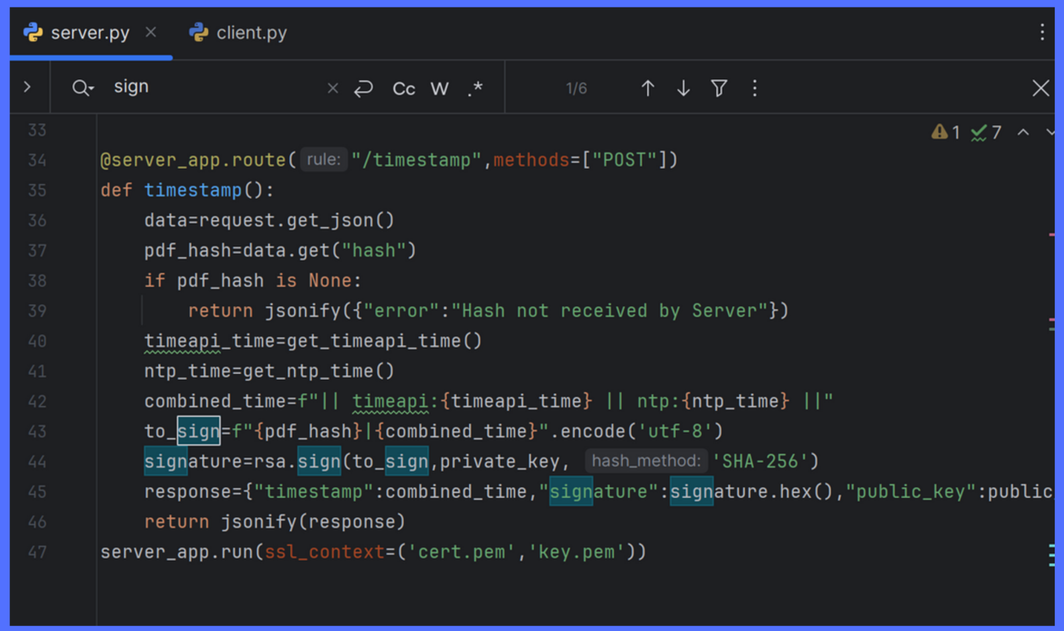
Assigned Project:- Securely time-stamping a document

Arnav Singh (2021019) Dharani Kumar S. (2021039)

Objectives

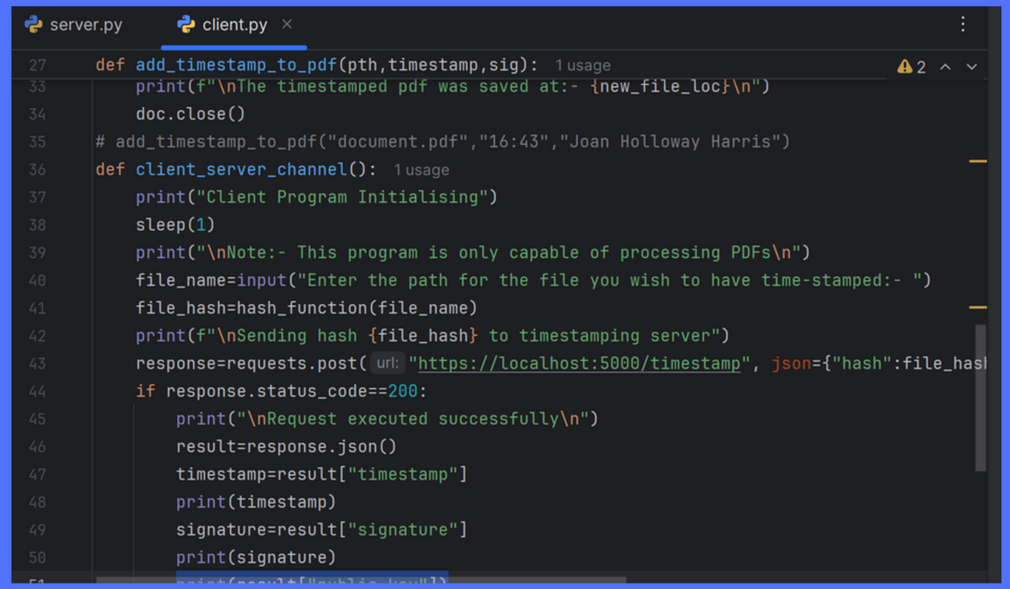
- Issue and verify time-stamped PDF files.
- Allow secure exchange of messages.
- Ensure that the CIA triad and non repudiation are maintained

Server



- Retrieves GMT time from timeapi.io (HTTPS) and time.nist.gov (NTP) upon receiving a document hash.
- Combines the hash with the timestamp, signs it with a 2048-bit RSA private key using SHA-256.
- Sends the timestamp, signature hex str, and RSA public key to the client over HTTPS.

Client



- Reads a user-selected PDF using PyMuPDF, extracts text, and computes a SHA-256 hash.
- Sends the hash to the server at /timestamp via HTTPS, verifies the server’s certificate, and receives the timestamp, RSA signature, and public key.
- Verifies the signature, then embeds the timestamp and signature into the PDF, saving it as a new file.

Q&A

1. How and where do you get the correct GMT date and time? Your laptop or the local Linux server is not good enough.
We get the correct GMT date and time from timeapi.io and UTC time from NTP. There are minor differences between the two, but all in all they return roughly the same time, and the end user can use whichever they trust more. timeapi.io is secured by HTTPS but is not authoritative, and the opposite can be said about NTP.

2. When is the correct GMT date/time obtained?
The correct GMT date/time is obtained once the server receives the document hash from the client

3. Is the source reliable? Is the GMT date and time obtained in a secure manner? The term ‘obtained’ refers to security of communication.
Yes and No. The timeapi.io time is obtained securely, but the NTP time is not, so it is susceptible to MITM attacks. Though one can make the claim that malicious actors could similarly cast aspersions on the validity of timeapi.io’s info but to us, it seemed that it’d be best to refer to multiple sources to reduce the possibility of being affected by such attacks.

4. How do you ensure privacy, in that the server does not see/keep the original document?
We only share the document’s SHA256 hash with the server

5. How do you share the document with third parties in a secure manner with the GMT date/time preserved, and its integrity un-disturbed?
We can share the original document, the timestamped document, and the server's public key to third parties in a secure fashion, so as to ensure that they have the ability to validate the contents of the files independently by verifying the timestamp and document integrity by recomputing the SHA-256 hash of the original document's text, extracting the timestamp and signature from the timestamped document, and verifying the signature using the public key.

6. How does one ensure that the user (both the owner and anyone else verifying the date/time) uses the correct "public-key" of the server stamping/signing the "GMT date/time".)
The owner receives the correct public key from the server over TLS, secured by a self-signed certificate verified by the client, ensuring authenticity in a trusted environment. For third parties, the owner shares the public key via secure channels, such as TLS-secured websites, encrypted email, or physical media. Third parties must trust the owner or a known server operator to provide the correct key, and they can verify its correctness by successfully validating the RSA signature on the timestamped document.

7. Which of these, viz. confidentiality, authentication, integrity and non-repudiation is/are Relevant?
According to us, All of these properties are met in our project, and are absolutely necessary to ensure secure multi-party communication. Each of these requirements are addressed as showcased below:-
Confidentiality: Only the SHA-256 hash of the PDF is sent to the server, and communication is secured via TLS.
Authentication: The server's identity is verified via TLS, ensuring the client communicates with the legitimate server.
Integrity: The RSA signature signs the document hash and timestamp, ensuring they are unaltered.
Non-Repudiation: The server's RSA signature, verifiable with its public key, proves the timestamp's origin and authenticity.

Note: Ideally we'd like to add the public key in the modified document itself to make comms with third parties more convenient but since that wasn't explicitly allowed, we've chosen to send it over separately if and when required by the third party

Output

STERLING COOPER & PARTNERS LLC.

5 MADISON AVENUE, NEW YORK

Lease Agreement for Mayfair Studios, Pasadena

As part of the expansion out west, The firm has decided to set base at the Mayfair Studios' Greenwich location for the employees working on the Ocean Spray Account and for the finance department to host representatives from the Martin Marietta Company for the Annual Defence Contractors' Tete-a-tete in Burbank. Partners Peter Campbell and Ted Chaough are to fly out to LAX on Monday, August 25, 1968, to take positions as the heads of the Accounts and Creative departments respectively, and to finally ratify this agreement in the presence of representatives from Dreyfuss, Rothberg, and Schlitz.

Passed with 5 Ayes, 2 Nays, and 1 Abstention.

All Partners in Attendance

STERLING COOPER AND PARTNERS
1969

STERLING COOPER & PARTNERS LLC.

5 MADISON AVENUE, NEW YORK

Lease Agreement for Mayfair Studios, Pasadena

As part of the expansion out west, The firm has decided to set base at the Mayfair Studios' Greenwich location for the employees working on the Ocean Spray Account and for the finance department to host representatives from the Martin Marietta Company for the Annual Defence Contractors' Tete-a-tete in Burbank. Partners Peter Campbell and Ted Chaough are to fly out to LAX on Monday, August 25, 1968, to take positions as the heads of the Accounts and Creative departments respectively, and to finally ratify this agreement in the presence of representatives from Dreyfuss, Rothberg, and Schlitz.

Passed with 5 Ayes, 2 Nays, and 1 Abstention.

All Partners in Attendance

STERLING COOPER AND PARTNERS
1969