Vivekanand Education Society's Institute of Technology

Department of AI & DS Engineering

Subject: Cryptography and System Security

Class: D11AD

Roll No: 46	**Name: Ashish Patil**
Practical No:10	**Title:Digital Signature**
DOP:	**DOS:**
Grades:	**LOs Mapped:**
Signature:	

Title: Digital Signature
DOP: /3/24
DOS: /3/24

(Attach output screenshots)

Aim: To demonstrate RSA Digital Signature scheme.

Theory:

A digital signature is a cryptographic technique used to verify the authenticity and integrity of a digital message, document, or data. It serves as the electronic equivalent of a handwritten signature or a stamped seal, providing assurance that the message was created by a particular sender and has not been altered or tampered with during transmission.

The concept of digital signatures relies on public key cryptography, a branch of cryptography that involves the use of key pairs: a public key and a private key. In digital signature schemes, a sender uses their private key to create a unique digital signature for the message, and the recipient can use the sender's public key to verify the signature. If the signature is valid, it confirms that the message was indeed sent by the claimed sender and that it has not been modified since the signature was created.

RSA (Rivest-Shamir-Adleman) is one of the most widely used public key cryptosystems, named after its inventors. In RSA digital signatures, the signing process involves the following steps:

1. Key Generation : The sender generates an RSA key pair consisting of a private key and a corresponding public key. The private key is kept secret and used for signing, while the public key is distributed to potential message recipients for signature verification.

2. Signing : To sign a message, the sender applies a mathematical operation involving their private key and a cryptographic hash function to the message. The result is the digital signature, which is unique to both the message and the private key.

3. Verification : The recipient of the signed message uses the sender's public key to verify the signature. This involves applying the same cryptographic hash function

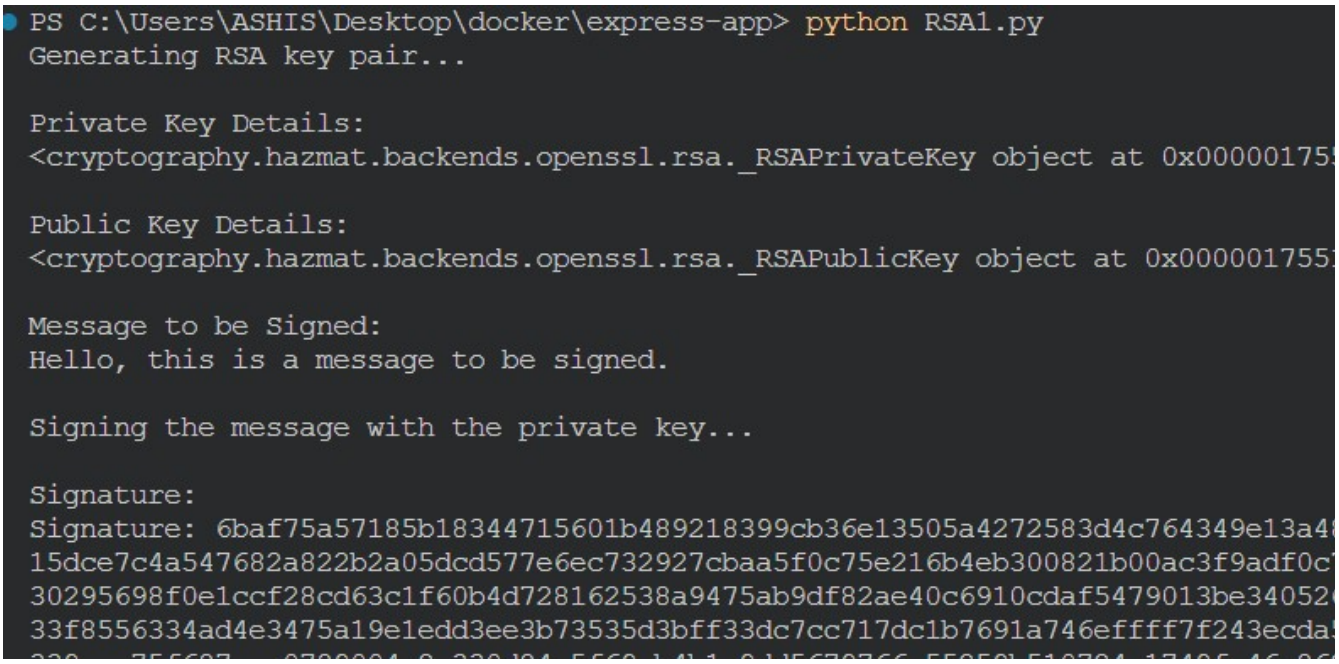
to the message and comparing the computed hash value with the decrypted signature obtained by applying the public key operation. If the computed hash matches the decrypted signature, the signature is considered valid, indicating that the message was indeed signed by the claimed sender and has not been altered.

RSA digital signatures provide several important properties:

- **Authentication : The recipient can verify the identity of the sender by confirming that the signature matches the sender's public key.**
- **Integrity : The recipient can verify that the message has not been altered since it was signed, as any modification would result in an invalid signature.**
- **Non-repudiation : The sender cannot deny having signed the message, as only they possess the private key required to create the signature.**

Overall, RSA digital signatures play a crucial role in ensuring the security and trustworthiness of electronic communications and transactions in various domains, including email, digital documents, software distribution, and online transactions.

Output Screenshot:



Conclusion: We have successfully implemented RSA algorithm and understood the concept of digital signature.