Semester	T.E. Semester VI – Computer Engineering
Subject	Cryptography and cyber security
Subject Professor In-charge	Prof. Amit Nerurkar
Assisting Teachers	Prof. Amit Nerurkar
Laboratory	M312B

Student Name	Deep Salunkhe
Roll Number	21102A0014
TE Division	A

Title:

Design and Implementation of Digital Signature

Explanation:

1. Definition: A digital signature is a cryptographic technique used to verify the authenticity and integrity of digital messages or documents. It provides a way for the sender of a message to prove their identity and ensure that the message has not been altered in transit.
2. Components of Digital Signatures:
    - Signing Algorithm: A mathematical algorithm used by the sender to generate the digital signature from the message.
    - Verification Algorithm: A complementary algorithm used by the recipient to verify the authenticity and integrity of the message and signature.
    - Key Pair: Digital signatures are typically based on asymmetric cryptography, where the sender possesses a private key for signing and the recipient uses a corresponding public key for verification.
    - Hash Function: A cryptographic hash function is often used to generate a fixed-size hash value from the message before signing. This hash value ensures that the signature is based on the content of the message and cannot be used to reconstruct the original message.
3. Process of Creating a Digital Signature:
    - The sender computes a hash value of the message using a secure hash function.
    - The sender encrypts the hash value with their private key, generating the digital signature.
    - The sender sends both the original message and the digital signature to the recipient.
4. Process of Verifying a Digital Signature:
    - The recipient computes a hash value of the received message using the same secure hash function used by the sender.

- The recipient decrypts the digital signature using the sender's public key, obtaining the original hash value.
- The recipient compares the computed hash value with the decrypted hash value. If they match, the signature is valid, and the message is authentic and unaltered.

5. Properties of Digital Signatures:
    - Authentication: Digital signatures authenticate the identity of the sender, ensuring that the message originates from a known and trusted source.
    - Integrity: Digital signatures verify that the message has not been altered or tampered with during transmission.
    - Non-repudiation: Digital signatures provide non-repudiation, meaning that the sender cannot deny sending the message once it has been digitally signed and verified.
    - Unforgeability: A valid digital signature cannot be forged by an unauthorized party, as it requires possession of the sender's private key.
6. Applications:
    - Digital signatures are widely used in electronic transactions, digital contracts, secure email communication, software distribution, and other scenarios where authentication and integrity are critical.
    - They are essential for ensuring trust and security in digital environments, especially in situations where physical signatures are impractical or impossible.

Result:

RSA public key

Public exponent (hex, F4=0x10001):

10001

Modulus (hex):

```
a5261939975948bb7a58dffe5ff54e65f0498f9175f5a09288810b8975871e99
af3b5dd94057b0fc07535f5f97444504fa35169d461d0d30cf0192e307727c06
5168c788771c561a9400fb49175e9e6aa4e23fe11af69e9412dd23b0cb6684c4
c2429bce139e848ab26d0829073351f4acd36074eafd036a5eb83359d2a698d3
```

1024 bit | 1024 bit (e=3) | 512 bit | 512 bit (e=3)

Digitally sign the plaintext with Hashed RSA.

Plaintext (string):

test SHA-1

Hash output(hex):

a94a8fe5ccb19ba61c4c0873d391e987982fbbd3

Input to RSA(hex):

a94a8fe5ccb19ba61c4c0873d391e987982fbbd3 Apply RSA

Digital Signature(hex):

```
2576257c9fa21a134f6e82fa9ffced2ff85b629146e77e6d601eb8b97420798d
814e697f7e081a6a3949b31ecdeb008566d420c2e84926b1531bf695c78e5421
1821948b3f3fb9a239ee642298ce4529b4918270d2f18d47de35ec55678ad5c6
f66616727869d79b87102e1126d991be9f23f8da2cbb27a0197ed50d72fdb3c5
```

Digital Signature(base64):

```
JXYlfJ+iGhNPboL6n/ztL/hbYpFG535tYB64uXQgeY2BTml/fggaajlJsx7N6wCF
ZtQgwuhJJrFTG/aVx45UIRghlIs/P7miOe5kIpjORSm0kYJw0vGNR9417FVnitXG
9mYWcnhp15uHEC4RJtmRvp8j+NosuyegGX7VDXL9s8U=
```

Status:

Time: 2ms

Conclusion:

By understanding these theoretical aspects of digital signatures, students can gain insights into their importance, functionality, and applications in cryptography and system security. Lab exercises can involve implementing digital signature algorithms, experimenting with different

parameters and key sizes, and exploring real-world use cases to reinforce learning and understanding.