|  |  |
| --- | --- |
| 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:**

**A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated**



**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.