|  |  |
| --- | --- |
| 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 RSA algorithm for generating public and private key



**Explanation:**

1. Definition: A public-key cryptosystem, also known as asymmetric cryptography, is a cryptographic technique that uses two keys - a public key and a private key - to perform encryption and decryption operations.
2. Key Generation:
   * Public Key: The public key is made freely available to anyone and is used for encryption by other parties.
   * Private Key: The private key is kept secret by its owner and is used for decryption. It must never be shared with others.
3. Encryption and Decryption:
   * Encryption: A message or data is encrypted using the recipient's public key. Only the corresponding private key can decrypt the ciphertext.
   * Decryption: The encrypted message is decrypted using the recipient's private key, ensuring that only the intended recipient can access the original plaintext.
4. Security Properties:
   * Confidentiality: Public-key cryptosystems provide confidentiality by ensuring that only the intended recipient, who possesses the corresponding private key, can decrypt and access the original message.
   * Authentication: Public-key cryptosystems enable authentication by allowing users to digitally sign messages using their private keys, which can be verified by anyone using the corresponding public key.
   * Integrity: Digital signatures generated using public-key cryptography also ensure data integrity, as any tampering with the message will result in an invalid signature.
   * Non-repudiation: Public-key cryptosystems provide non-repudiation, meaning that a user cannot deny sending a message or creating a digital signature once it has been verified using their public key.
5. Applications:
   * Secure Communication: Public-key cryptosystems are used to establish secure communication channels over insecure networks, such as the internet. Examples include HTTPS for secure web browsing and S/MIME for secure email communication.
   * Digital Signatures: Public-key cryptography is used to generate and verify digital signatures, ensuring the authenticity and integrity of electronic documents, transactions, and messages.
   * Key Exchange: Public-key cryptosystems facilitate secure key exchange protocols, such as Diffie-Hellman key exchange, which allows parties to establish a shared secret key over an insecure channel.
6. Security Considerations:
   * Key Management: Proper key management practices, including key generation, distribution, storage, and revocation, are crucial for the security of public-key cryptosystems.
   * Key Sizes: The security of public-key cryptosystems depends on the size of the keys used. Larger key sizes provide stronger security but may impact performance.
   * Algorithm Selection: Choosing secure and widely-accepted cryptographic algorithms, such as RSA, ECC, or ElGamal, is essential to ensure the security and interoperability of public-key cryptosystems.



**Result:**

**A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated**



**Conclusion:**

By understanding these theoretical aspects of public-key cryptosystems, students can gain insights into their principles, functionalities, and applications in cryptography and system security. Lab exercises can involve implementing encryption, decryption, digital signature generation and verification, key exchange protocols, and exploring real-world use cases to reinforce learning and understanding.