|  |  |  |  |
| --- | --- | --- | --- |
| **Course Name:** | **Information Security (116U01L602)** | **Semester:** | **VI** |
| **Date of Performance:** | **21/01/2025** | **DIV/ Batch No:** | **B2** |
| **Student Name:** | **Akshat** | **Roll No:** | **16010122221** |

|  |
| --- |
| **Title: Application of RSA Algorithm for various security services like confidentiality, authentication, signature, non-repudiation and integrity** |

|  |
| --- |
| **Objectives:** |
| To apply RSA Algorithm for various security services. |

|  |
| --- |
| **Expected Outcome of Experiment:**  CO1 Explain various security goals, threats, vulnerabilities and controls  CO2 Apply various cryptographic algorithms for software security |

|  |
| --- |
| **Books/ Journals/ Websites referred:** |
| <https://www.openssl.org/>  <https://sandilands.info/sgordon/simple-introduction-to-using-openssl-on-command-line> |

|  |
| --- |
| **Abstract:** |
| The RSA algorithm is a widely used asymmetric cryptographic technique that provides security services such as encryption, digital signatures, and key exchange. OpenSSL, an open-source cryptographic library, enables the implementation of RSA for various security applications via command-line operations. This experiment demonstrates key pair generation, encryption and decryption, digital signature creation and verification, and certificate handling using OpenSSL. The results validate the effectiveness of RSA in securing communications and ensuring data integrity in modern cryptographic systems. |

|  |
| --- |
| **Related Theory:** |
| **RSA Algorithm**  The RSA algorithm, developed by Ron Rivest, Adi Shamir, and Leonard Adleman, is a public-key cryptographic method based on the mathematical difficulty of factoring large prime numbers. It involves three key steps:   1. **Key Generation**: Two large prime numbers are chosen to generate a public-private key pair. 2. **Encryption and Decryption**: The public key is used to encrypt data, while the private key is used to decrypt it. 3. **Digital Signatures**: A sender can sign a message using their private key, and the receiver can verify it using the sender's public key. |

|  |
| --- |
| **Implementation Details:** |
| 1. **Public and Private Key Generation**              1. **Encryption & Decryption**          1. **Hash Function**   **Initial Hash**    **Initial Message**    **Changed Hashed Message**    **Changed Message**     1. **Digital Signature**      1. **Digital Certificate** |
|  |

|  |
| --- |
| **Results/Output:** |
| The OpenSSL commands were executed successfully to generate RSA key pairs, encrypt and decrypt messages, and create digital signatures. The encrypted message was unreadable without the private key, proving the security of RSA encryption. The digital signature verification confirmed the authenticity and integrity of the signed message. This validates the effectiveness of RSA for secure communication. |

|  |
| --- |
| **Conclusion:**  We have Successfully completed the experiment and implemented Application of RSA Algorithm |