**Course – Cryptography and System Security (CSS)**

|  |  |
| --- | --- |
| **UID** | 2021300038 |
| **Name** | Atharva Gite |
| **Class and Batch** | BE Computer Engineering - Batch VIII |
| **Date** | 12/09/2024 |
| **Lab #** | 3 |
| **Aim** | Implement RSA algorithm. |
| **Problem Definition** | The experiment uses asymmetric and symmetric cryptosystem to provide two security services. First, this experiment covers key distribution problem using asymmetric cryptosystem. The asymmetric cryptosystems allows sharing secret key between sender and receiver through a third party entity. Second, symmetric cryptosystem covers sending large message from the sender to the receiver using the secret key shared in the first step. |
| **Theory** | Public-key cryptography, or asymmetric cryptosystem, is the field of cryptographic systems that use pairs of related keys. Each key pair consists of a public key and a corresponding private key. Key pairs are generated with cryptographic algorithms based on mathematical problems termed one-way functions. Security of public-key cryptography depends on keeping the private key secret; the public key can be openly distributed without compromising security. |
| **Output** |  |