Name	Atharva Tamhankar
UID no.	2022300127
Experiment No.	3

AIM:	To implement RSA public-key cryptosystem including key generation, encryption, and decryption.
THEORY:	**Concept**: RSA is an asymmetric cryptographic algorithm. It uses two keys: - Public key (e, n) for encryption - Private key (d, n) for decryption The security relies on the difficulty of factoring $n = p \times q$. **Steps**: 1. Choose two large prime numbers p and q. 2. Compute $n = p \times q$ and Euler's totient $\varphi(n) = (p-1)(q-1)$. 3. Select e such that $\gcd(e, \varphi(n)) = 1$. 4. Compute $d \equiv e^{-1} \bmod \varphi(n)$. 5. Encryption: c ≡ m^e mod n 6. Decryption: m ≡ c^d mod n **Key Points:** - Prime generation is done using random numbers and primality testing. - The totient function ensures the number of coprimes with n. - Modular inverse ensures correct decryption key. - Security depends on prime size (lab demo uses small primes, real systems use ≥2048 bits).
CONCLUSION:	RSA successfully demonstrates public-key cryptography with asymmetric keys. The implementation shows end-to-end working: key generation → encryption → decryption. It highlights the importance of prime generation, modular arithmetic, and number theory in modern cryptography.