Implementation of RSA Cryptosystem

Supervisor,
Dr. Narendran Rajagopalan,
Associate Professor,
NITPY.

Assignment by,
Mekala Hari Krishna
(CS22B1031)

Overview:

The RSA cryptosystem, named after its inventors Rivest, Shamir, and Adleman, is one of the most widely used public-key encryption algorithms. It forms the backbone of secure data exchange on the internet by allowing encryption and digital signatures using asymmetric keys. RSA ensures data confidentiality, authenticity, and integrity through the use of mathematically linked public and private keys.

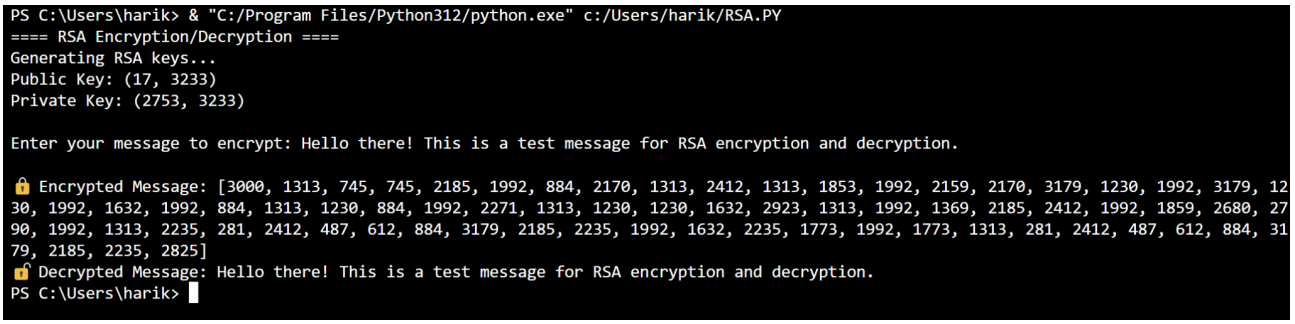
Methodology:

- **Key Generation**
  - Choose two large prime numbers p and q.
  - Compute $n = p \times q$ (modulus).
  - Calculate Euler's totient: $\varphi(n) = (p-1)(q-1)$.
  - Choose an encryption exponent e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
  - Compute decryption exponent d as the modular inverse of e mod $\varphi(n)$.
- **Encryption**
  - Convert the plaintext message to an integer m, such that $m < n$
  - Compute ciphertext: $c = m^e \bmod n$
- **Decryption**
  - Recover plaintext: $m = c^d \bmod n$

Applications:

- Secure Email Communication (e.g., PGP)
- Digital Signatures for authentication
- TLS/SSL protocols for HTTPS websites
- Software licensing and code signing
- Cryptographic wallets and blockchain-based identity systems

Result :



Conclusion :

RSA remains a cornerstone of modern cryptography, enabling secure data transmission and authentication across digital systems. Its strength lies in asymmetric key encryption and the computational difficulty of factoring large integers. Despite the rise of post-quantum cryptography, RSA continues to be a trusted and essential component in digital security infrastructures.