Implementation of RSA Cryptosystem

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

Assignment by,
Panchananam Lakshmi Srinivas
(CS22B1040)

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

Keyspace & Security Complexity:

- **Keyspace Size**: Determined by the size of nnn; modern RSA typically uses key sizes of 2048 to 4096 bits.
- **Security**: Relies on the intractability of factoring large semi-primes.
- **Complexity**: Factoring a 2048-bit number has sub-exponential time complexity (using General Number Field Sieve).
- RSA's security is theoretically vulnerable to **Shor's algorithm** on a quantum computer, but remains strong against classical attacks.

Result :

```
PS E:\NitPY_B-Tech\Sem6\NS> & "C:/Program Files/Python311/python.exe" e:/NitPY_B-Tech/Sem6/NS/Assignment.py
Welcome to the RSA Encryption Program!

RSA Key Pair Generated!
Public Key (e, n): (121928205281, 520474379057)
Private Key (d, n): (83245416221, 520474379057)

Please enter the message you want to encrypt (plaintext):
 RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem used for secure data transmission. It relies on the mathematical difficulty of factoring large prime numbers. The system involves a pair of keys: a public key for encryption and a private key for decryption. RSA is widely used for securing communications and digital signatures.

Encrypted message (ciphertext):
 [4413452766, 377873629975, 162042864908, 84981429572, 210555317595, 13499645872, 93014828400, 496271914201, 260830159352, 211925469886, 428592664134, 215987652240, 462376415321, 56408539123, 246898752456, 461911561336, 509079834847, 173787946924, 211841650752, 288267283317, 459556263852, 63617979, 244175880005, 93425061221, 133566141616, 141106788869, 215350739315, 149080643396, 339491316218, 282037871628, 500442555760, 271552517078, 45233898680, 361496169469, 191246977491, 311630663911, 186252083297, 311630663911, 59904065567, 136213348474, 216198338973, 496456654103, 322142833503, 516188271569, 516664557407, 382079411738, 133204787544, 355718921015, 284633909797, 248203309642, 193909063650, 444693399130, 438434514074, 245830859261, 308113780584, 76540688027, 382942512507, 189304998291, 480554758467, 39283124230, 290758441390, 202080101659, 428592664134, 130331372792, 91536596383, 32781696375, 39635334795, 132468370923, 365044319055, 438794888078, 365338743876, 123169253448, 227923364880, 345699371462, 296538705605, 19951871529, 191246977491, 102654490349, 428592664134, 313431233039, 175316889463, 136497225701, 123169253448, 227923364880, 134340726833, 296538705605, 19951871529, 100281774639, 465486508959, 346266691663, 243357798168, 124609862016, 20458104189, 288267283317, 459556263852, 63617979, 244175880005, 250272713856, 193738066258, 23133653436, 274125939779, 136213348474, 159918918160, 476944296631, 102654490349, 418071319635, 385197737857, 417466875269, 7184023546, 229401718315, 93425061221, 35295374577]


Decrypted message:
 RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem used for secure data transmission. It relies on the mathematical difficulty of factoring large prime numbers. The system involves a pair of keys: a public key for encryption and a private key for decryption. RSA is widely used for securing communications and digital signatures.
```

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.