**Department of Computer Engineering**

**Name of the Student: Parth Das Roll Number: C-111**

**SAP ID: 60004220185 Class: Comps Division: C-2 Batch: 2**

**Subject: Information Security**

**DATE OF PERFORMANCE: 15/02/2025 DATE OF SUBMISION: 15/02/2025**

**EXPERIMENT NO: 4**

**AIM:** To Study and implement RSA Encryption Algorithm

**Theory:**

**SOURCE CODE WITH OUTPUTS:**

import hashlib

p = int(input("Enter P : "))

q = int(input("Enter Q : "))

n = p\*q

phi\_n = (p - 1)\*(q - 1)

def isPrime(ele):

for i in range(2, int(ele\*\*(1/2)) + 1):

if ele%i == 0:

return False

return True

def encrypt(key, plaintext):

d, n = key

cipher = plaintext\*\*d % n

return cipher

def decrypt(key, ciphertext):

e, n = key

decipher = ciphertext\*\*e % n

return decipher

message = "Hello"

message\_hash = int(hashlib.md5(message.encode()).hexdigest(), 16) % n

print(f"\nMessage : {message}")

print(f"Message Digest : {message\_hash}")

for e in range(n-1, 2, -1):

if e!=p and e!=q and isPrime(e):

break

d = 3

while e\*d%phi\_n != 1:

d+=1

print(f"\nPublic Key : {(e, n)}")

print(f"Private Key : {(d, n)}")

signature = encrypt((d, n), message\_hash)

print(f"\nSignature : {signature}")

print(f"Sender Send (Message, Signature) to Receiver : {(message, signature)}")

message\_hash = int(hashlib.md5(message.encode()).hexdigest(), 16) % n

print(f"\nHash of message at Receiver : {message\_hash}")

hashfromsignature = decrypt((e, n), signature)

print(f"Hash from signature : {hashfromsignature}")

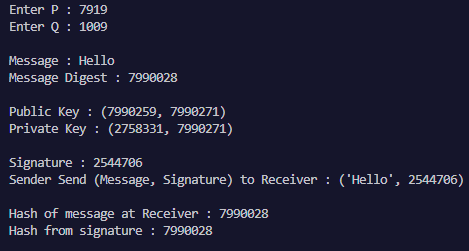
if hashfromsignature == message\_hash:

print("\nVerifed as both hash matches")

else:

print("\nError")

**Output:-**



**CONCLUSION:**

RSA is a powerful asymmetric encryption algorithm that secures data using a public-private key pair. Its security relies on the difficulty of prime factorization, making it resistant to brute-force attacks. While highly secure, RSA is computationally slower than symmetric encryption methods.To enhance efficiency, it is often used in combination with symmetric encryption in hybrid cryptosystems..Despite its challenges, RSA remains a fundamental pillar of secure communication and digital signatures