# NATIONAL INSTITUTE OF TECHNOLOGY PUDUCHERRY

(An Institution of National Importance under MoE, Govt. of India)

**KARAIKAL – 609 609**

## DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

**Roll Number:** CS22B1057 **Name: Thinnavalli Sree**

**Semester:** 6nd semester **Class:** CSE

**Subject Code:** CS1072 **Subject Name:** Network Security


**Assignment - 1** **Date:** 29-04-2025

## RSA Implementation

**CODE :-**

```
import random
import sympy

def generate_prime(bits=512):
   return sympy.randprime(2**(bits-1), 2**bits)

def compute_keys():
   p = generate_prime()
   q = generate_prime()

   n = p * q
   phi_n = (p - 1) * (q - 1)

   e = 65537  #public exponent
   d=pow(e,-1,phi_n) #private exponent

   return ((e, n), (d, n))

def encrypt(message, public_key):
   e, n = public_key
   message_int=int.from_bytes(message.encode(), 'big')
   cipher_text=pow(message_int,e,n)
   return cipher_text

def decrypt(cipher_text, private_key):
   d, n = private_key
   decrypted_int=pow(cipher_text,d,n)
   decrypted_message=decrypted_int.to_bytes((decrypted_int.bit_length()+7)//8, 'big').decode()
   return decrypted_message

if __name__=='__main__':
   print("Rivest–Shamir–Adleman (RSA) implementation")

   public_key,private_key=compute_keys()
```

```
print(f"public key: {public_key}")
print(f"private key: {private_key}")

msg=input("Enter a message to encrypt:")
print(f"Original message: {msg}")

cipher_text=encrypt(msg,public_key)
print(f"Encrypted Message: {cipher_text}")

decrypt_message=decrypt(cipher_text,private_key)
print(f"Decrypted Message: {decrypt_message}")
```

**Result :-**