



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 :-

```

PS C:\Users\sreet> & C:/Users/sreet/AppData/Local/Programs/Python/Python312/python.exe c:/Users/sreet/Downloads/rsa_implementation.py
● Rivest-Shamir-Adleman (RSA) implementation
public key: (65537, 113627473696902699686524277838022893168219182919942796819266877642223549151263774211087793097810060959890955937604005582547813537446854673820951117448396708576729348311194597404467884359799887341183873744564380063759208021969116324399782876266248049502159679038816550213696799016973390389831619958316376661443)
private key: (80980185451900977985847528037300078905168277105173691365755192548260300444147231366667341383026603556061871598908559878298682071097704216704383231497661840967717406575645244534097369292437039226134700219172419834032129873020329990210336820515936378609762948761443193233756126555584192922964062984148345066441, 113627473696902699686524277838022893168219182919942796819266877642223549151263774211087793097810060959890955937604005582547813537446854673820951117448396708576729348311194597404467884359799887341183873744564380063759208021969116324399782876266248049502159679038816550213696799016973390389831619958316376661443)
Enter a message to encrypt:Hey there
Original message: Hey there
Encrypted Message: 97674646360246286032311377201258829331670107444975294043025735578065473753239522587181521643895921633149076744284049856986173942177872437058445808883952832240309957282341732362834225172587386539618224388234045837103011811352055384870252849246769434714838356949238227421291991236470343078299329803581795513035
Decrypted Message: Hey there
PS C:\Users\sreet>

```