**Batch: A3 Roll No: 16010121045**

**Experiment No.**

|  |  |
| --- | --- |
| |  | | --- | | **Title:**  **Implementation of Symmetric key cryptography algorithm (DES/AES)** | |

**Objective:**

To write a program implementing RSA Digital Signature showing the application of RSA Algorithm for various security services like confidentiality, authentication, signature, non-repudiation and integrity

**Expected Outcome of Experiment:**

|  |  |
| --- | --- |
| **CO** | **Outcome** |
| **CO3** | |  | | --- | | **Comprehend cryptographic hash functions, Message Authentication Codes and Digital Signatures for Authentication** | |

**Books/ Journals/ Websites referred:**

**Abstract**:-

(*Asymmetric key cryptography*)

**Related theory:**

*Digital signatures, RSA algorithm, RSA signing and verifying process*

**Program:**

*import* math

keyspace="ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&\*()-=\_+"

def publicKey(*p*,*q*):

temp=(*p*-1)\*(*q*-1)

*for* i *in* range(temp-1,2,-1):

*if*(math.gcd(temp,i)==1):

*return* i

def privateKey(*e*,*phin*):

*for* d *in* range(1,*phin*):

*if*((d\**e*)%*phin*==1):

*return* d

p=int(input("Enter value of p (Prime number): "))

q=int(input("Enter value of q (Prime number): "))

n=p\*q

phin=(p-1)\*(q-1)

e=publicKey(p,q)

print("Public key <e,n> = <%d,%d> "%(e,n))

d=privateKey(e,phin)

print("Private key <d,n> = <%d,%d> "%(d,n))

plaintext=input("Enter plain text: ")

print("Encrypted text: ",*end*="")

encTxt=[]

*for* i *in* plaintext:

x=int(keyspace.find(i))

encTxt.append(((x+2)\*\*e)%n)

print(encTxt)

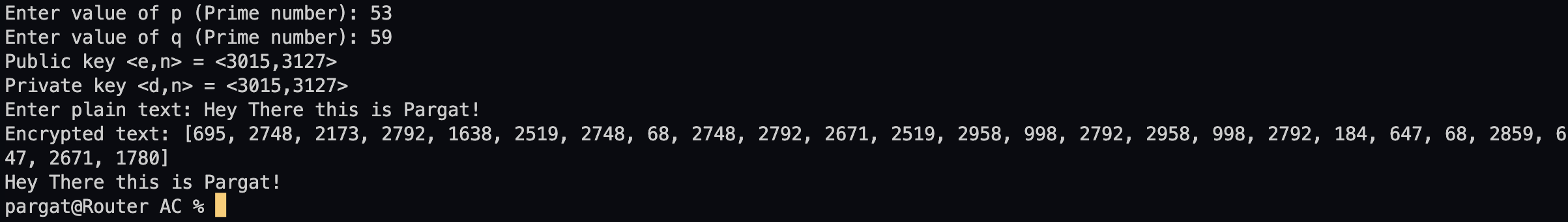
decTxt=""

*for* i *in* encTxt:

decTxt+=keyspace[((i\*\*d)%n)-2]

print(decTxt)

**Output Screenshots:**

****

**Text

Description automatically generated**

**Text

Description automatically generatedConclusion:-**

In this experiment, we learnt about the RSA algorithm and how to implement it in the real world. Successfully implemented the given task with detailed steps shown in the output.

**Postlab questions:**

1. **Comment on strengths and weaknesses of asymmetric key cryptosystem.**

Strengths:

• In asymmetric or public key, cryptography there is no need for exchanging keys, thus eliminating the key distribution problem.

• The primary advantage of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone.

• Can provide digital signatures that can be repudiated.

Weakness:

* A disadvantage of using public-key cryptography for encryption is speed there are popular secret-key encryption methods which are significantly faster than any currently available public-key encryption method.
* If a key is leaked, the protocol is destroyed.
* It needs a whole separate secure protocol for sharing the final key.

1. **Discuss strengths and weaknesses of RSA, comment on solutions over the lacunas.**

Strengths

* RSA is stronger than any other symmetric key algorithm.
* If initial prime number values are large, then near to impossible to preform brute force attacks.
* RSA has overcome the weakness of symmetric algorithm i.e. authenticity and confidentiality.

Weakness

* RSA has too much computation.
* If a key is leaked, the protocol is destroyed.
* It needs a whole separate secure protocol for sharing the final key.
* Is very resource and hardware intensive.