**FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING**

**Department of Computer Engineering**

**1. Course , Subject & Experiment Details**

| | | | |
|---|---|---|---|
| **Academic Year** | **2021-22** | **Estimated Time** | **03 - Hours** |
| **Course & Semester** | **T.E. (CMPN)- Sem VI** | **Subject Name & Code** | **CSS - (CPC702)** |
| **Chapter No.** | **02 – Mapped to CO- 1** | **Chapter Title** | **Basics of Cryptography** |

| | |
|---|---|
| **Practical No:** | 4 |
| **Title:** | Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA. |
| **Date of Performance:** | **21/02/2022** |
| **Date of Submission:** | **19/03/2022** |
| **Roll No:** | **8940** |
| **Name of the Student:** | **Warren Fernandes** |

**Evaluation:**

| Sr. No | Rubric | Grade |
|---|---|---|
| 1 | On time submission Or completion (2) | |
| 2 | Preparedness(2) | |
| 3 | Skill (4) | |
| 4 | Output (2) | |

**Signature of the Teacher:**

**Date:**

**MNS**

**Title:** Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA/ElGamal.

**Lab Objective**:

This lab provides insight into:

· How the public-key algorithms work and understand the working of RSA.

**Reference** : "Cryptography and Network Security" B. A. Forouzan
"Information Security Principles and Practice" Mark Stamp
"Cryptography and Network Security" Atul Kahate

**Prerequisite :** Any programming language and Knowledge of Ciphering .

**Theory:**

To overcome the problems faced in symmetric key algorithms, people have chosen Asymmetric Key algorithms for communication. Communication with Asymmetric algorithms will give us transmission of information without exchanging the key.

**Public-key cryptography** refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Public-key cryptography is widely used. It is an approach used by many cryptographic algorithms and cryptosystems. It underpins such Internet standards as Transport Layer Security(TLS), PGP, and GPG. RSA and Diffie–Hellman key exchange are the most widely used public key distribution systems, while the Digital Signature Algorithm is the most widely used digital signature system. Asymmetric algorithms which are mostly used are RSA cryptosystem and ElGamal Cryptosystem.

**The RSA algorithm** is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape.RSA is an algorithm for public key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem.The RSA algorithm involves threesteps: key generation, encryption and decryption.

**ElGamal System** is a public-key cryptosystem based on the discrete logarithm problem. It consists of both encryption and Signature algorithms. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. ElGamal encryption consists of three components: the key generator, the encryptionalgorithm, and the decryption algorithm.

**ALGORITHM**

**RSA**

**Example of RSA**

**>> Generating Public Key :**

- Select two prime no's. Suppose **P = 53 and Q = 59**.
  Now First part of the Public key : **n = P*Q = 3127**.
- We also need a small exponent say **e** :
  But e Must be

  An integer.
  Not be a factor of n.

  **1 < e <** Φ(n) [Φ(n) is discussed below],

  Let us now consider it to be equal to 3.

- Our Public Key is made of n and e

**>> Generating Private Key :**

**MNS**

- We need to calculate Φ(n) :

  Such that **Φ(n) = (P-1)(Q-1)**

  so, Φ(n) = 3016

- Now calculate Private Key, **d** :
  **d = (k*Φ(n) + 1) / e** for some integer k
  For k = 2, value of d is 201

Now we are ready with our – Public Key ( n = 3127 and e = 3) and Private Key(d = 2011)

Now we will encrypt **"HI"** :

- Convert letters to numbers : H = 8 and I = 9
- Thus **Encrypted Data c = $89^e$ mod n**.

  Thus our Encrypted Data comes out to be 1394

Now we will decrypt **1349** :

- **Decrypted Data = $c^d$ mod n**.

  Thus our Encrypted Data comes out to be 89

**8 = H and I = 9 i.e. "HI".**

## Code:

In [3]:

```
import random
import math
p = int(input("Enter the value of p = "))
q = int(input("Enter the value of q = "))
n = p * q
toitent = (p-1) * (q-1)
print("\nThe value of toitent = ", toitent)
e = 0
for i in range(2, toitent):
    if math.gcd(i, toitent) == 1:
        e = i
        break
print("\nThe value of e = ", e)
#k = 2
k = int(input("\nEnter the value of k = "))
d = int((k*toitent +1)/e)
print("The private key (d) = ", d)
c = (p**e)%n
print("\nThe value of c (encrypted data) = ", c)
p = (c**d)%n
print("The value of p (decrypted data) = ", p)
```

## Output:

```
Enter the value of p = 3
Enter the value of q = 7

The value of toitent =  12

The value of e =  5

Enter the value of k = 2
The private key (d) =  5

The value of c (encrypted data) =  12
The value of p (decrypted data) =  3
```

**Conclusion:**

The program was tested for different sets of inputs.
Program is working SATISFACTORY

**Post Lab Assignment:**

Test above an experiment to estimate the amount of time
to i) Generate key pair (RSA ) ii) Encrypt n bit message (RSA)
iii) Decrypt n bit message (RSA)
As function of key size, experiment with different n-bit messages. Summarize your Conclusion.

**Answer:**
From the above experiment we can estimate the time complexity of each method in RSA algorithm:
Generate key pair: O((log(n)/log(2))^3)
Encrypt n bit message: O(n^2)
Decryption n bit message: O(n^3)
Where n is key size.