# FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING Department of Computer Engineering

# 1. Course , Subject & Experiment Details

Academic Year	2018-19	<b>Estimated Time</b>	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:	3
Title:	Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA.
Date of Performance:	
Date of Submission:	
Roll No:	
Name of the Student:	

## **Evaluation:**

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

Signature of	f the T	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:**

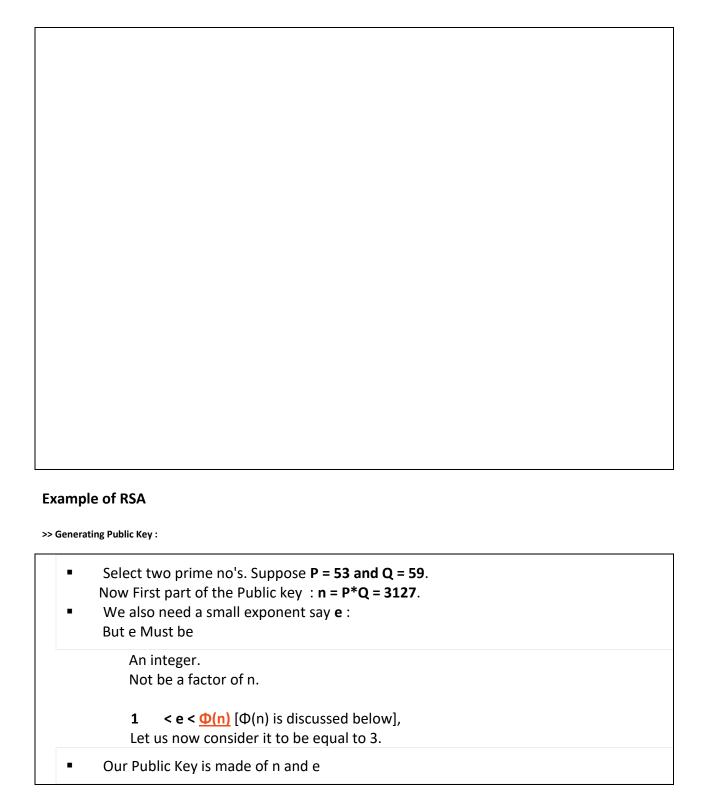
To overcome the problems faced in symmetric key algorithms, people have chosen Asymmetric Key algorithms for communication. Communication with Asymmetric algorithms will give us transmission of information without exchanging the key.

**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			



>> Generating Private Key:

We need to calculate Φ(n) :

Such that  $\Phi(n) = (P-1)(Q-1)$ 

so,  $\Phi(n) = 3016$ 

■ Now calculate Private Key, **d**:

 $d = (k*\Phi(n) + 1) / e$  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 = 89e mod n.

Thus our Encrypted Data comes out to be 1394

Now we will decrypt 1349:

■ Decrypted Data = c<sup>d</sup> mod n.

Thus our Encrypted Data comes out to be 89

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

#### **Conclusion:**

The program was tested for different sets of inputs.

Program is working SATISFACTORY NOT SATISFACTORY

(Tick appropriate outcome)

### **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.