

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

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

<b>Academic Year</b>	<b>2019-20</b>	<b>Estimated Time</b>	<b>03 - Hours</b>
<b>Course &amp; Semester</b>	<b>T.E. (CMPN)- Sem VI</b>	<b>Subject Name &amp; Code</b>	<b>CSS - (CSL604)</b>
<b>Chapter No.</b>	<b>02 – Mapped to CO- 1</b>	<b>Chapter Title</b>	<b>Symmetric and Asymmetric key Cryptography and key Management</b>

<b>Practical No:</b>	<b>4</b>
<b>Title:</b>	Implementation and analysis of ElGamal cryptosystem and Digital signature scheme using ElGamal.
<b>Date of Performance:</b>	
<b>Date of Submission:</b>	
<b>Roll No:</b>	
<b>Name of the Student:</b>	

**Evaluation:**

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

**Signature of the Teacher:**

**Date:**

MNS

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

**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.

This cryptosystem is based on the difficulty of finding **discrete logarithm** in a cyclic group that is even if we know  $g^a$  and  $g^k$ , it is extremely difficult to compute  $g^{ak}$ .

ElGamal encryption consists of three components: the key generator, the encryption algorithm, and the decryption algorithm.

**ALGORITHM**

**ElGamal Encryption Algorithm**

### Example of ElGamal

Consider  
 $P=71, G=33, x=62, M=15$  and  $y=31$

$h = g^x \bmod 71 = 10$   
Public key=  $p=71, g=33, h=10$

$M=15$   
 $r=31$   
 $(C1, C2) = (62, 18)$

**CT= (62,18)**

$62^{-1} \bmod 71 = 63$   
 $PT=18.63^{62} \bmod 71 = 15$

### Conclusion:

The program was tested for different sets of inputs.

Program is working	SATISFACTORY	NOT SATISFACTORY
( Tick appropriate outcome)		

### Post Lab Assignment:

**1. Test above an experiment to estimate the amount of time to**

- i) Generate key pair (ElGamal)
- ii) Encrypt n bit message (ElGamal)

MNS

iii) Decrypt  $n$  bit message (ElGamal)

As function of key size, experiment with different  $n$ -bit messages. Summarize your Conclusion.

**2. Perform comparison analysis of RSA with ElGamal .**