FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING Department of Computer Engineering

1. Course , Subject & Experiment Details

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

Practical No:	4
Title:	Implementation and analysis of ElGamal cryptosystem and Digital signature scheme using ElGamal.
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 the	Teac	her:
-----------	--------	------	------

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:

ALCODITHM

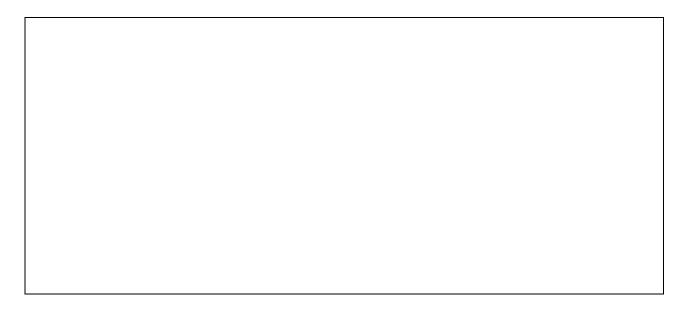
To overcome the problems faced in symmetric key algorithms, people have chosen Asymmetric Key algorithms for communication. Communication with Asymmetric algorithms will give us transmission of information without exchanging the key.

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	ElGamal Encryption Algorithm		



Example of ElGamal

Consider P=71, G=33, x=62, M=15 and y=31 $h = g^x \mod 71 = 10$ Public key= p=71,g=33,h=10

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

CT= (62,18)

62⁻¹ mod 71 = 63
PT=18.63⁶² mod 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

As fu	ecrypt n bit message (ElGamal) Inction of key size, experiment with different n-bit messages. Summarize your Clusion.
2.	Perform comparison analysis of RSA with ElGamal .