Name of Student			
Lab Experiment No.	2	**Roll No.**	
Date Of Perf.:		**Date Of Sub.:**	
Expt. Title	Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA/El Gamal		
CO Mapping	LO1,LO2		

Aim: Implementation and analysis of RSA cryptosystem and Digital signature scheme using RSA/El Gamal

Objectives of the Experiment: To be able to analyze and implement public key algorithms like RSA and El Gamal

Problem Statement:
Design 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.

Postlab

Explain direct and arbitrated digital signature.
Estimate the encryption and decryption values for the RSA algorithm parameters. P=7, Q=11,and M=8.

The outputs were checked for different sets of inputs.
Program is working is SATISFACTORY NOT SATISFACTORY (Tick appropriate outcome)

Evaluation:

Timeline (2)	Understanding(2)	Performance (4)	Postlab (2)	Total(10)

Date & Signature of teacher: **Students Signature:**