20CYS205 – MODERN CRYPTOGRAPHY

RSA & ELGAMAL ENCRYPTION SCHEMES

Submitted by

KAUSHIK M – CB.EN.U4CYS22035
LOGESH R – CB.EN.U4CYS22036
LALITHA K – CB.EN.U4CYS22037
SAI TEJAS MAREDDY – CB.EN.U4CYS22038

Under the guidance of

Mr. Aravind Vishnu,
Assistant Professor,
Amrita Vishwa
Vidyapeetham
Coimbatore.

TIFAC-CORE IN CYBER SECURITY
AMRITA SCHOOL OF
ENGINEERIN

AMRITA VISHWA VIDYAPEETHAM

COIMBATORE - 641 112

2023

Acknowledgement

First of all, we would like to express our gratitude to our Mentor, Aravind Vishnu, Assistant Professors, TIFAC-CORE inCyber Security, Amrita Vishwa Vidyapeetham, Coimbatore, for their valuable suggestions and timely feedbacks during the course of this major project. It was indeed a great support from them that helped me successfully fulfill this work

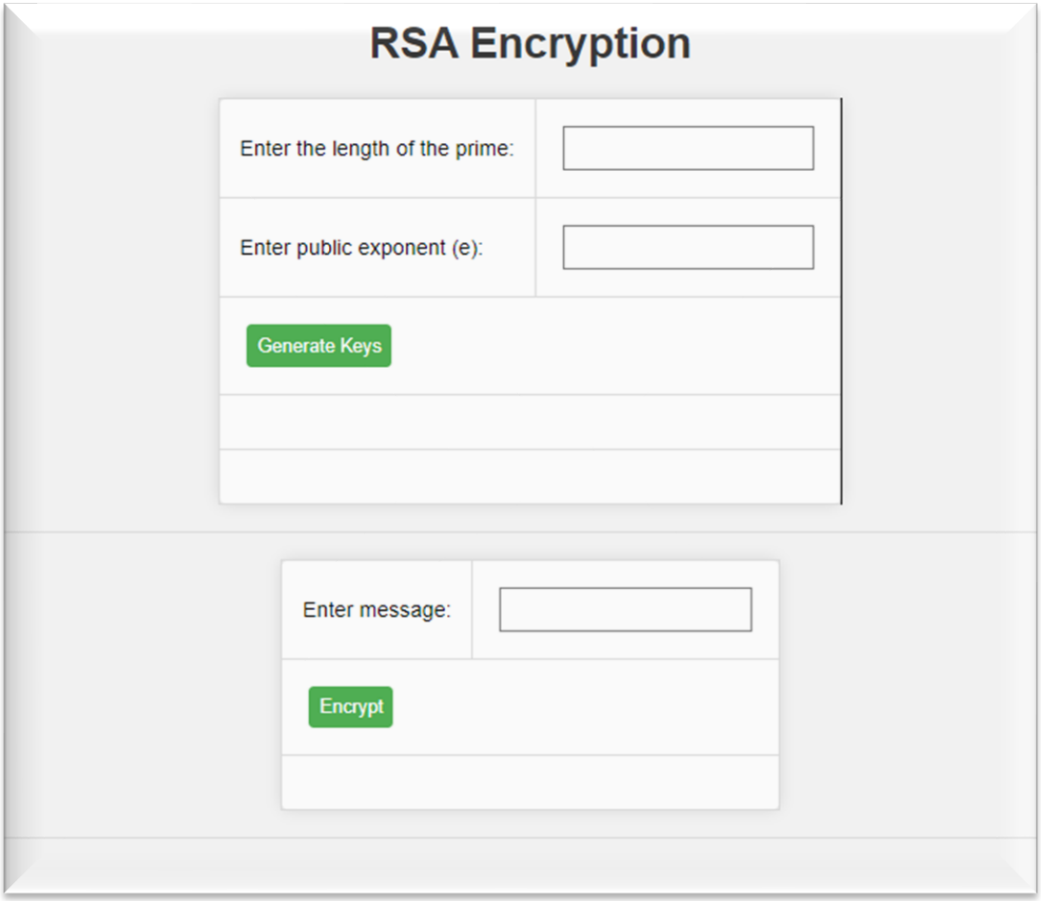
I would like to thank **Dr. M. Sethumadhavan**, Professor and Head of Department, TIFAC-CORE in Cyber Security, for his constant encouragement and guidance through-out the progress of this major project.

I convey special thanks to our friends for listening to our ideas and contributing their thoughts concerning the project. All those simple doubts from their part have also made us think deeper and understand about this work.

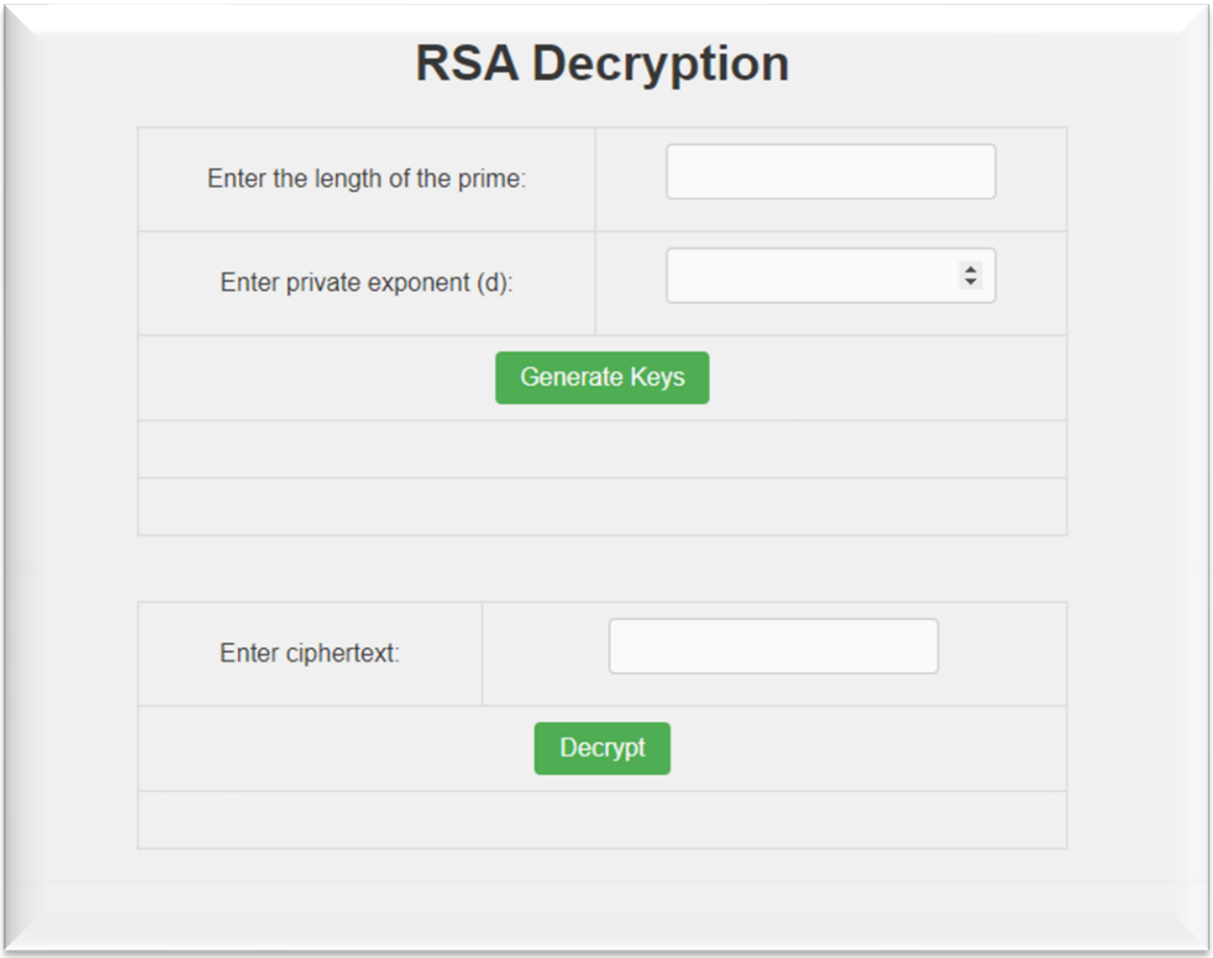
In particular, we would like also like to extend our gratitude to all the other faculties of TIFAC-CORE in Cyber Security and all those people who have helped us in many ways for the successful completion of this project.

USER MANUAL

RSA ENCRYPTION AND DECRYPTION:

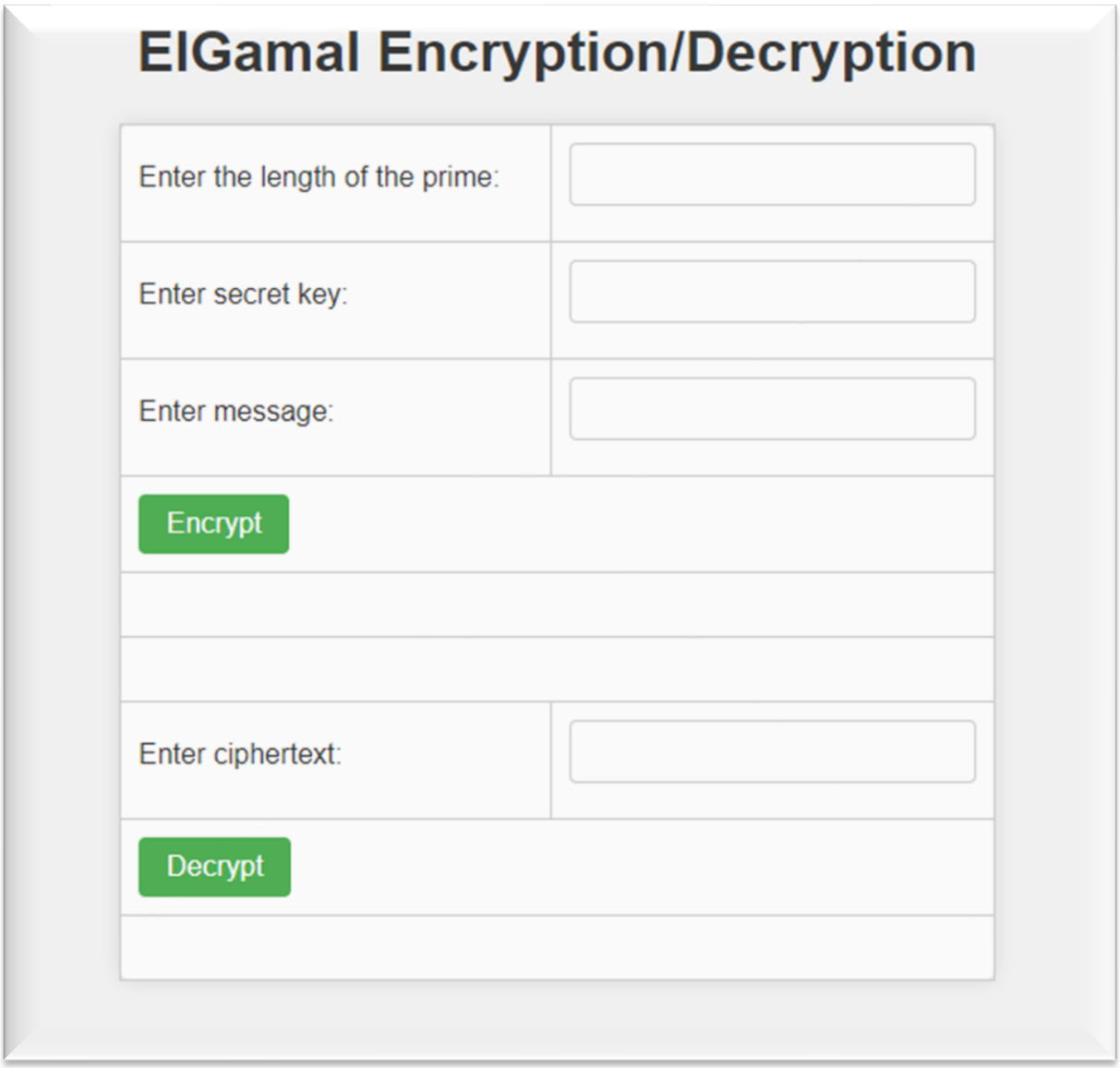


Here as soon as we enter the length of the primes we require (p and q) it will generate them and then we enter the public exponent e it will automatically calculate the private exponent d.
After we enter the message it will generate its cipher text and give us.



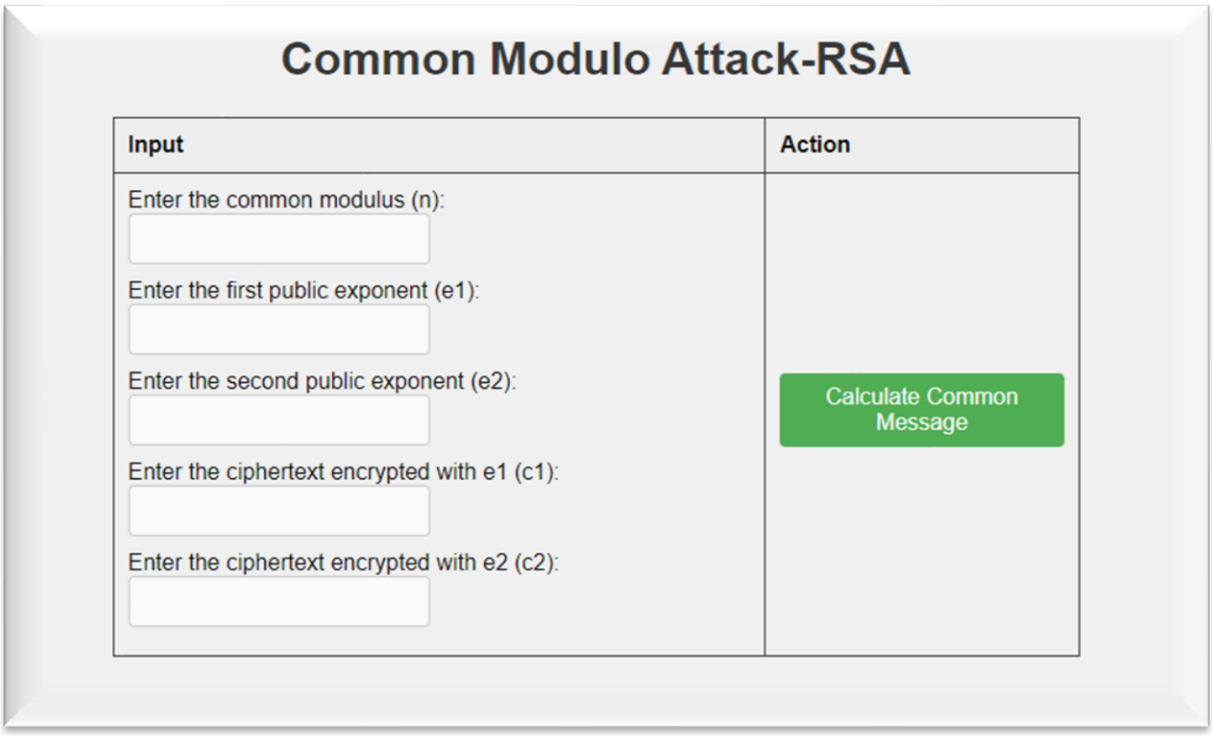
Here, Decryption also works in the same manner and provides the plain text when the cipher text is entered.

ELGAMEL ENCRYPTION AND DECRYPTION:



After we enter the asked information and the message, the cipher text will be provided and parallelly we can check decryption for which when the cipher text is entered, the plain text is returned.

RSA COMMON MODULO ATTACK:



Here after we enter the required details, it calculates the common message.