CADT
IDT វិទ្យាស្ថានបច្ចេកវិទ្យាឌីជីថល
Institute of Digital Technology

DEPARTMENT OF TELECOMS AND NETWORKING

COURSE: CRYPTOGRAPHY

TERM 1 | YEAR 3

PROJECT: RSA CRACKER

LECTURER: MR. MEAS SOTHEARATH

SUBMIT DATE: NOVEMBER 29, 2025

Name: Vong Soukorng

ID: IDTB100251

Group: 2

Table of Contents

I. Introduction

a. Overview

In modern cybersecurity, cryptography plays a crucial role in securing communication and protecting sensitive information. Among many cryptographic systems, RSA remains one of the most widely used public-key encryption methods in web security, digital signatures, and secure data transmission. Despite its widespread use, understanding RSA can be challenging for beginners due to its reliance on number theory.

However, RSA also introduces a learning challenge of understanding how the security depends on large number factorization and how vulnerabilities allow encrypted data to be recovered.

This project presents a graphical decryption tool designed to assist cybersecurity students in understanding RSA internals while solving CTF (Capture The Flag) cryptography challenges.

b. Problem

In CTF competitions, RSA challenges often provide limited information such as:

- n (modular)
- e (public exponent)
- c (ciphertext)

Beginner struggles because they require knowledge of number theory such as factoring the modulus n, computing the private exponent through modular inverse, and correctly applying the RSA decryption formula. Most existing tools require command-line usage or manual calculations, which can be overwhelming for students who are still developing programming skills. Additionally, once decrypted, RSA output may appear in formats such as hexadecimal or raw integers, making it difficult for beginners to interpret and convert into readable text like UTF-8. Some tools also fail silently or do not show any results when the input values are incorrect, leaving users confused and unsure whether they are making progress. These difficulties create a significant learning barrier and reduce efficiency during timed CTF competitions.

c. Solution

This RSA Cracker Project delivered a user-friendly GUI allowing user to:

- Input any given RSA values (n, e, c)
- Automatically factor n into p and q
- Computing private key exponent d
- Decrypt the ciphertext
- Display results in Hex, Integer, and UTF-8 formats
- Always show output even if the plaintext is invalid

This tool doesn’t need command lines, making it suitable for CTF beginners and cryptography learners.

d. Motivation

The motivation behind this project is to help students understand how RSA works and make it easier for them to solve RSA challenges in CTF competitions. The tool allows learners to test and practice decryption without only relying on theory. It also shows how weak keys or small numbers can make RSA vulnerable. Using this tool, beginners can build confidence and improve their practical skills in cryptography, especially in CTF competitions.