

Cairo University

Faculty of Engineering

Computer Engineering Department

Third Year

**Cryptography and Security CMP3050**

**RSA Project**

**Delivery Document**

Ahmed Ihab sec: 1 BN: 2

Ahmed Gamal AbdelSamie sec: 1 BN: 3

Fall 2022

Overview

We have implemented the RSA encryption algorithm using a mixture of Python scripts (.py) and Python Interactive Notebooks (.ipynb). The project is divided into utility functions, chat module using sockets, RSA encryption and decryption, brute force attack, key length vs. time, and chosen ciphertext attack.

How to Run

We have used vscode with python and python notebook extensions installed. Any IDE or code editor will be able to run the .py scripts, and the .ipynb files may be run using Google Collab, Jupyter, Kaggle, etc.

Directions and Explanation