Credit Hours System

CMPN426

Cairo University

Faculty of Engineering

Computer Systems Security Project

Submitted by: Omar Tarek Fahmy Elwakil

ID: 1170331

Date of submission: 24/5/2022

File Structure

Project files are divided into 4 files:

1. rsa_algorithm.py which contains all RSA functions.
2. rsa_performance.py which contains brute force and chosen cipher attack functions.
3. sender.py
4. receiver.py

How to run

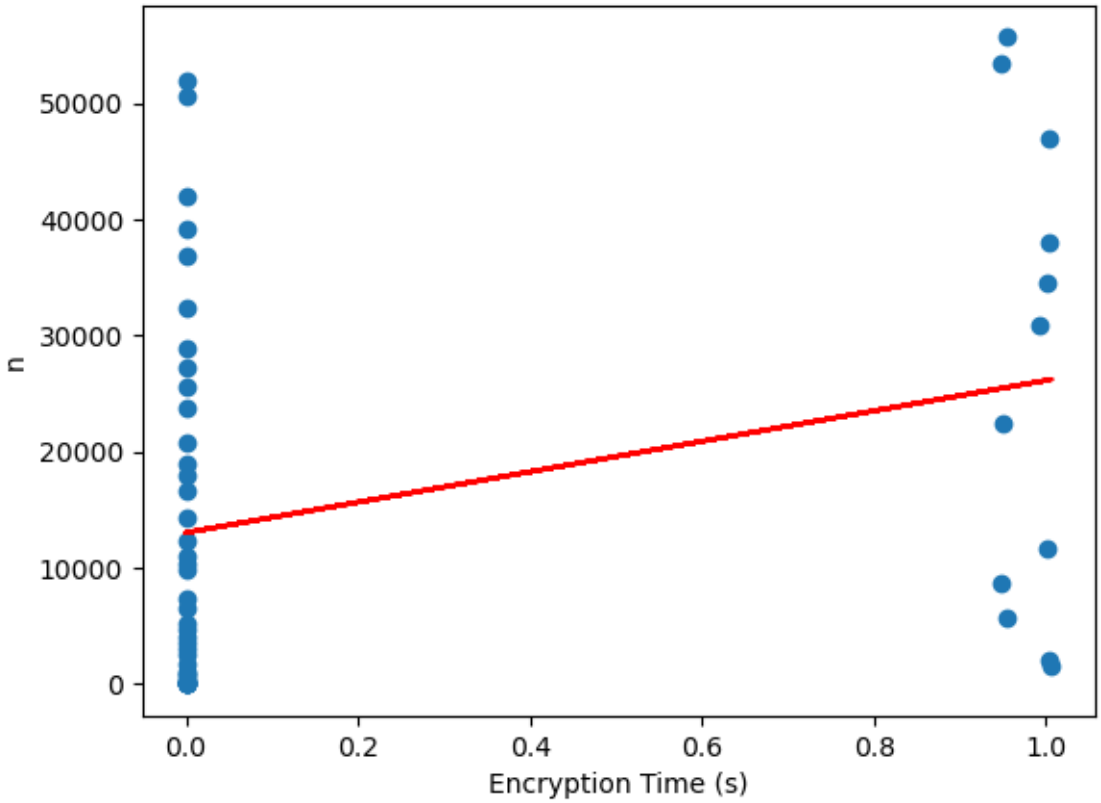
You can run rsa_performance.py. You have to uncomment which part you want to run brute force or chosen cipher attack.
python rsa_performance.py

You can run sender/receiver. You don't need any setups there.
python receiver.py
python sender.py
You have to run receiver.py first then sender.py because receiver is the one who initialize and make key generation and sends to sender.

You can only insert in receiver.py on runtime are p and q values.
You can only insert in sender.py on runtime is the plaintext you want to send.

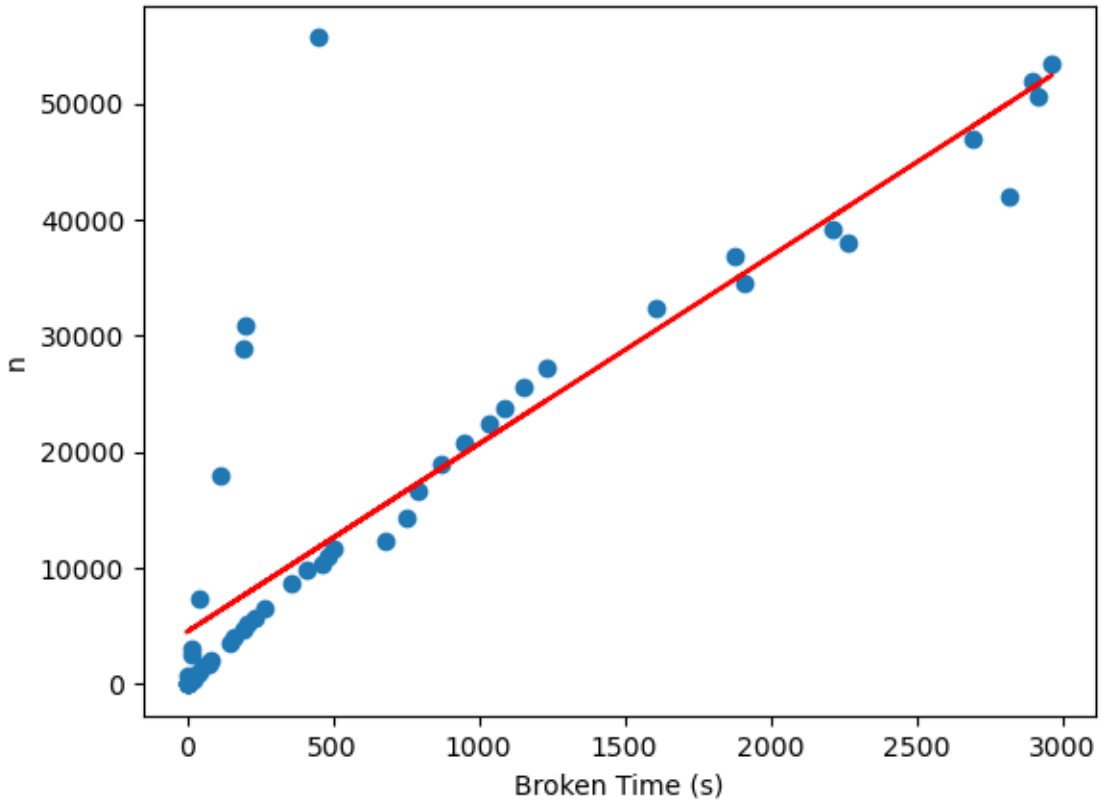
Performance

Encryption time vs n



As you can see from the plot is n value vs encryption time. The highest n value is little more than 50,000

Breaking RSA time vs n



As you can see from this plot. As n increases, broken time increases linearly because there is more than 1 d value that can return the ciphertext back to plaintext correctly. That is why the plot is increasing linearly not exponentially.