Cairo University
Faculty of Engineering

Cryptography and Network Security
Spring 2022

Computer Engineering Department

Security Project: Implementing and Breaking RSA!

Project Objectives:

1. **Apply security concepts you study in the course.**
2. **Enhance student's understanding of encryption algorithms.**
3. **Have experience with code breaking.**
4. **Implement RSA algorithm, one of asymmetric key encryption algorithms.**

Project Requirement:

1. Implement the RSA algorithm (encryption and decryption).

2. Implement a simple program sending and receiving a text message, the sender should encrypt the message using the receiver's public key, then the receiver will decrypt it using his own private key and display it. Your program should support any text message containing alphabetical and numeric characters not only numbers.

3. Try to use different key lengths for RSA (in terms of the size of n), and calculate efficiency in terms of encryption time using RSA for each key length, plot a graph of RSA encryption time vs. Key length.

4. Implement brute force (mathematical attack) on RSA algorithm using different values for n, plot a graph of Time to break the private key (in seconds) versus value of n. Discuss the results you obtain.

5. Implement the Chosen Cipher Text attack for RSA and justify why it happens in your report.

Important Notes

- **Implement all the required algorithms (RSA, and breaking the code) and all the tasks by yourself.**
- **Copied projects from each other or from the internet will not be accepted. Before marking a plagiarism checking program will check your project against each other and against the internet.**
- **The sender and receiver should be two separate modules (2 programs). Communication can be done using files, or network (socket programming).**
- **Use any programming language of your choice such as: Python, Java, C++, C#,..etc.**
- **All students should submit their own-written code without the help of any external source.**

Deliverables:

- **You should deliver all your code and a detailed report about your project, how you implemented it and the analysis results and your conclusions.**
- **You should submit a zipped folder containing the FOLLOWING:**
  - **Project source files**
  - **Sample input files test cases that were used for testing.**
  - **Sample output files when executing the test cases.**
  - **A detailed report about your project, how you implemented it and the analysis results and your conclusions.**
  - **All projects will be tested by another set of data.**

Project Due Date: **21 May 2022 at 11:59 p.m.**