Cairo University
Faculty of Engineering

Computer Engineering Department

Cryptography and Network Security- CMP N/426
Fall 2018

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 RSA algorithm by yourself.

2. Try to use different key lengths for RSA, and calculate efficiency in terms of encryption time using RSA for each key length, plot a graph of RSA encryption time vs. Key length.

3. 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.

4. Implement the Chosen Cipher Text attack for RSA.

Important Notes

- **Copied projects from each other/from the internet will get zero!**
- Implement all required algorithms (RSA, and breaking the code) and all the tasks by yourself.
- You should work in group of size 2 students.

Project Due Date:

Tuesday, February 12th, 2019.