CSCD 434-040 Network Security

Lab 3, RSA- Due, January 31, 2024

January 25, 2024

Overview

The objective of this lab is to learn more about RSA. You'll finish writing a basic RSA python encryption program (given a mostly complete file) and learn how the key size affects the effectiveness of RSA.

Part 1:

Finish implementing the code in `practiceRSA.py` and make sure you can encrypt and decrypt data. Encrypt a message with **both** your pubic and private keys. Code for encrypting with a public key is given, **do not forget to provide code for private encryption**. Include a screen shot of the output in your write up.

Part 2:

Given my `public key`(n,e), decrypt the cipher text C (represented as an integer) created with my public key :

```
C = 39523400271805851137124348723016754985 1
public key = (902125837174791721758566383713256340347,65537)
```

Make a separate python file to calculate your solution to part 2. Explain what you did and how you cracked the cipher text using the public key. Be sure to state the decrypted text in your write up.

Extra credit (5pts for undergrads)

Create keys of increasing size and plot the time required to factor them. Start with the number of bits for each prime number at ~64 and include at least 10 steps, increasing the number of bits. Determine how large the key needs to be for factoring to be too difficult for a modern computer. Include the plot in your turn in along with your evaluation and code.

Extra credit (for all)

Crack:

```
Cipher text = 336581678530946914008894606405291446545818902817979880604699690816617017236 49
public key = (347188330600708164164070159056688356594521214661878139176848543494809610628403,65537)
```

Turn in

You'll create a tarfile to turn in your lab. Make sure to include:

1. A PDF write up answering any questions and requested screen shots.
2. Source code. Your python files **must** be named `lab3-part1.py` and `lab3-part2.py` and your code must run.
3. A detailed `README` so I now how to run your code. The `README` should describe how to run each python file.