CSCD 437
Lab 6
Cryptography

SPECIFICATIONS

Most of the time we cover the cryptography algorithms, but we don't actually write any code. This is no longer the case. In this lab we will practice encrypting/decrypting messages. There are three separate related parts for this lab.

NOTE: There will be a single PDF with appropriately marked parts that will be submitted with Java code for this lab.

This is lab will be completed in groups of three, (the team of two I will be your third team member) using the same three students from your project team. Each member will complete each part and submit a single PDF. The reason for groups of three are so you have someone to exchange your encrypted messages.

For 70% of the grade complete Part 1
For 85% of the grade complete Part 1 and Part 2
For 100% of the grade complete Part 1, Part 2 and Part 3

It is possible that one team member will only complete Part 1 and the other two complete all the other parts. Please denote any shortcomings by yourself or any teammate for each part.

PART 1 – PGP Basics

Using your AWS VM

1) Install PGP
2) Generate your public and private keys. Use your EWU email set the expiration date for 1 month
3) Download your public key, and upload it to https://keys.openpgp.org/
    a. Enter your email and verify your key
    b. You must use your EWU email
4) Your teammates will grab your verified public key from the above website.
5) Encrypt an appropriate clean message to your teammates using their public keys (Each message should be unique per teammate).
6) Send them the encrypted message and have them decrypt it.
7) Capture each team members encryption/decryption including the original/decrypted message into the single PDF. Label which teammate you are encrypting messages to.
8) Add your decrypted teammate messages to your PDF. Ensure you capture all commands and the message.

PART 2 – Java Cryptography – This part is by each individual

I have provided a Java main, and Javadoc of a Java class. Your task is to write the Java class. This Java class is meant to simulate the basics similar to PGP.

1) Write the CSCD437Crypto.java code based on the Javadoc specifications. NOTE: the code is within a package.
2) Using the message.txt file execute CSCD437Lab6Tester.java and capture the output.
3) Capture the output and place the output in the single PDF

PART 3 – Java Cryptography – This part is by each individual sending/receiving from each teammate

1) Repeat Part 1 with your teammates, meaning send your teammates encoded messages and decoded their messages they send you.
    a. You will create both public and private keys
    b. You will send your public key to your teammates
    c. You will also send your teammates what algorithm you used (SHA256withRSA)
    d. You must you a different algorithm for each teammate.
    e. Load your teammate's public key
    f. Create and encode a message for your teammate
    g. Send your teammate the encoded message
    h. Decode the message from your teammate
    i. Don't over complicate this. It really is a repeat of Part 1 just using Java
2) Create a main in the lab6 package named CSCD437Lab6Part3TM1.java and CSCD437Lab6Part3TM2.java
3) Run your code for each teammate's message
4) Capture the output for each teammate and place the output in the single PDF – Note your teammates first and last name for each message

WHAT TO TURN IN:

Your group will submit a single zip containing:

- The single PDF
- All Java code inside the lab6 folder.

Name your zip your last name first letter of your first nameTL-lab6.zip (Example: steiners-lab6.zip)