CSCD 437
Lab 5
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.

PART 1 – PGP Basics

Using your Ubuntu VM (Windows Subsystem Linux works fine for this too)

1) Install PGP
2) Generate your public and private keys. Use your EWU email set the expiration date for 1 week
3) Exchange your public key with your teammates.
4) Encrypt an appropriate clean message to your teammates using their public keys (Each message should be unique per teammate).
5) Send them the encrypted message and have them decrypt it.
6) Capture each team members encryption/decryption including the original/decrypted message into the single PDF.

PART 2 – PGP Symmetric Mode

If you don't have a person's public key, you can still send them a message. To send another person a message, without their public key you need to use symmetric mode. Using symmetric mode means you have a single shared key that is used to encrypt and decrypt.

1) In canvas is a symmetrically encrypted, by me, file for each team.
2) Choose one person from each team to email me their EWU public key
3) I will encode your team's password for the symmetric file and post it in canvas
4) Grab the encrypted file from canvas and decrypt it with that teammate's private key
5) Retrieve the password from the file
6) Use the password to decrypt your team's symmetrically encrypted file
7) Capture the entire process including the decrypted password and the decrypted symmetrically encrypted file contents into your single PDF.

PART 3 – Java Cryptography

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 CSCD437Lab5Tester.java and capture the output.
3) Capture the output and place the output in the single PDF

WHAT TO TURN IN:

Your group will submit a single zip containing:

- The single PDF
- All Java code inside the lab5 folder, including the message.txt file I provided.

Name your zip your team number lab5.zip (Example: team16lab5.zip)