**CSCI 3500**

**Ethan Walton**

**September 13, 2025**

**Instructor: Ms. Emond**

**PGP / Encryption**

## **Lab Purpose (In Your Own Words)**

This lab introduces students to the fundamentals of public key cryptography using GPG software. The goal is to understand how asymmetric encryption works by generating key pairs, exchanging public keys, and securely sending encrypted messages. Through hands-on experience, students learn how to protect sensitive data and verify identities using digital signatures. The lab also emphasizes the importance of key management and secure communication practices.

## **Tools & Resources Required**

* + Gpg4win (Kleopatra): A Windows-based software suite for managing OpenPGP keys and encrypting/decrypting messages.
  + Windows Host Machine: Required for running Gpg4win; Mac users may need to use lab computers.
  + Notepad++: Used to create and save messages and public key files.
  + D2L Discussion Board: Platform for sharing public keys with lab partners.
  + Email Client: Used to send and receive encrypted messages.

## **Lab Procedures (Minimum of 1 Page)**

To begin the lab, I downloaded the Gpg4win software from the official website and selected the full version, opting for a $0 donation. After running the installer, I chose English as the installation language and proceeded through the setup by accepting the EULA and installing the default components. Once the installation was complete, Kleopatra launched automatically. I then created a new OpenPGP key pair by selecting “Create a Personal” format and entering my name and email address. I enabled passphrase protection and accessed the advanced settings to set the key material to RSA4096 and the expiration date to one day ahead. After confirming the settings, I used “password” as the passphrase, acknowledged the insecure password warning, and finalized the key creation.

Next, I exported my public key by right-clicking the newly created key in Kleopatra and saving it as a file. I uploaded this file to the D2L discussion board to share with my lab partner. To receive my partner’s public key, I downloaded their file from D2L and saved it as a .gpg file using Notepad++. I then imported the certificate into Kleopatra and verified it. For message encryption, I typed a short message in Notepad++, copied it, and pasted it into Kleopatra’s Notepad. I selected my partner’s public key under “Encrypt for others” and my own key under “Sign as,” then clicked “Sign/Encrypt Notepad.” After entering my passphrase, the encrypted message appeared, which I copied and sent via email to my partner.

To decrypt the message I received, I copied the entire encrypted text—including the PGP headers—and pasted it into Kleopatra’s Notepad. I clicked “Decrypt,” entered my passphrase, and successfully viewed the decrypted message. This completed the full cycle of public key encryption and decryption between lab partners.

## **­­­Observations (Minimum of ½ a Page)**

This lab provided a practical understanding of how public key cryptography works in real-world applications. I learned how to generate secure key pairs and the importance of protecting private keys with strong passphrases. The process of encrypting and signing messages demonstrated how confidentiality and authenticity can be achieved simultaneously. Importing and verifying public keys emphasized the need for trust and validation in secure communications. One surprising insight was how easy it is to encrypt and decrypt messages once the keys are properly exchanged and verified—making secure communication accessible even to non-experts.

## **Reflection Questions**

**1. What is the purpose of using public key cryptography?** To enable secure communication by using asymmetric keys—one for encryption (public) and one for decryption (private)—ensuring confidentiality and authenticity.

**2. Why is it important to protect your private key with a strong passphrase?** A strong passphrase prevents unauthorized access to your private key, which could otherwise be used to decrypt sensitive messages or impersonate you.

**3. What does signing a message do?** It verifies the sender’s identity and ensures the message hasn’t been altered, providing integrity and authenticity.

**4. Why is it important to verify a public key before using it?** To confirm the key belongs to the intended recipient and hasn’t been tampered with, preventing man-in-the-middle attacks.

**5. What would you do differently if this were a real-world encryption scenario?** Use a complex passphrase, securely store the private key (e.g., encrypted USB in a safe), verify public keys through trusted channels, and rotate keys periodically.