

# Lab 6 - Hiding in Plain Sight b3lgYW0gSQ==

CSEC 2324 - Network Security  
Lab Guide v1.0

William Cox, M.S.  
Visiting Assistant Professor  
wcox@ualr.edu or wcox@uaptc.edu

January 2023




# Contents

Lab Guide Instructions . . . . .	4
Lab File Formatting . . . . .	4
Markdown How-To . . . . .	5
Suggested Setup . . . . .	5
Lab Assignment 6 - Hiding in Plain Sight b3lgYW0gSQ== . . . . .	5
Overview . . . . .	5
Lab Artifacts . . . . .	6
Lab Software . . . . .	6
Part 1: Using GPG . . . . .	6
Introduction . . . . .	6
Asymmetric Encryption . . . . .	6
Creating Public & Private Key . . . . .	7
Export your Public Key . . . . .	7
Import Public Key . . . . .	8
Encrypt a File . . . . .	9
Decrypt a File . . . . .	10
List your keys . . . . .	11
Revoke a key . . . . .	12
Reflection . . . . .	13

## Lab Guide Instructions

The labs included in this guide will help you understand the principles of Network Security.

When you see a  you will be required to take a screenshot of that step.

Included is the requirement for a Lab Report file.

Follow the formatting instructions for full credit.

*Note: Using Markdown is only required for the first lab.*

## Lab File Formatting

When completing your labs please follow these instructions.

1. All Labs created using Markdown & will use the Eisvogel template. Labs files created in another word processing program will use Times New Roman, 12 Font, Double Space.  
Get Eisvogel here: <https://github.com/Wandmalfarbe/pandoc-latex-template>
2. Create a title page with the following details:
  1. Title of the Lab
  2. Class Name
  3. Your name
  4. Date
3. Section 2 will have all screenshots and questions/answers for the lab.
  1. Each question must be listed with its question number.
  2. Answers will be indented on the next line and start with an "a."
  3. If answer includes a picture, make sure picture is big enough for your instructor to interpret, but not too big to distract from the quality of your work.
4. Section 3 will be labeled Reflection.
  1. This is where you add any reflections needed.
  2. Make sure to quote your sources with parenthetical citations.
  3. Do not use quotes, but instead rewrite the quote in your own words. *Remember to still give credit to the author.*
5. Section 4 will be References
  1. All references should be in alphabetical order
  2. Use either APA or IEEE formatting

## Markdown How-To

Below you will find a quick reference on how to use Markdown. This is not all inclusive and you may need to research steps that are particular to your situation. IE. Operating System, IDE, etc...

## Suggested Setup

*(You don't need to follow if you know Markdown)*

1. Download and install following programs:
  1. VSCode Download
  2. Pandoc Install Instructions **Note: make sure to install all of the required dependencies**
  3. Eisvogel Template Download
2. Once you have downloaded and installed the required applications, you will need to set up your template and environments.
  1. VSCode Setup - Install following extensions:
    1. Markdown All in One, Author: Yu Zhang
    2. Dictionary Completion, Author: Yu Zhang
    3. markdownlint, Author: David Anson
  2. Setup Pandoc template Eisvogel Install Instructions
3. Basic Markdown syntax can be found at Markdown Guide
4. Convert Markdown to PDF syntax
  1. Open terminal and navigate to your markdown location
  2. Execute the following command replacing the file names with your information.

```
1 pandoc filename.md -o filename.pdf --from markdown --template  
   eisvogel --listings
```

## Lab Assignment 6 - Hiding in Plain Sight b3IgYW0gSQ==

### Overview

This lab will introduce you to encryption techniques. Don't just go through the motions in this lab, but try to understand what you are doing and how you could defend against these attacks.

## Lab Artifacts

Build a Lab report file with the requested answers or screenshots presented in this lab. Follow the Lab file format found in the beginning of the Lab Guide Manual.

## Lab Software

**Programs:** GPG, Email Client

**Operating System:** Linux

**Terminal Emulator:** bash, zsh, CMD

## Part 1: Using GPG

### Introduction

GPG, or GNU Privacy Guard, is a free and open-source implementation of the OpenPGP standard for encrypting and signing files and messages. In this lab guide, you will learn how to use GPG to encrypt and decrypt files and messages, as well as how to create and manage GPG keys.

#### 1. Install GPG

- In order to use GPG, you must first install it on your computer.
- On Windows, you can download and install GPG4Win from <https://www.gpg4win.org/>
- On Mac, you can install GPG Suite from <https://gpgtools.org/>
- On Linux, you can use the package manager of your distribution to install GPG. For example, on Ubuntu, you can use the command:


```
1 sudo apt-get install gnupg
```

## Asymmetric Encryption

Asymmetric encryption uses two keys: a public key and a private key. The public key is used to encrypt data, while the private key is used to decrypt it. Data encrypted with the public key can only be decrypted with the corresponding private key. This method of encryption is considered more secure than symmetric encryption because the private key never needs to be shared. Additionally, anyone can encrypt data with the public key, but only the holder of the private key can decrypt it, providing an extra layer of security.

## Creating Public & Private Key


### Windows

1. Once GPG4Win is installed, you can use Kleopatra to create a GPG key pair
  1. Open Kleopatra, click on the “File” menu, and select “New Certificate”.
  2. Follow the prompts to create your key pair, making sure to enter accurate information and a strong passphrase.
  3. You will be asked to choose the type of key you want to create, the key size, and the expiration date. You can choose RSA and RSA (default) for the type of key, and choose the key size and expiration date that best fits your needs.
  4. You will also be prompted to enter your name, email address, and a passphrase. Make sure to enter accurate information and a strong passphrase.
2. Once you have entered all the information, Kleopatra will generate your key pair.
3. You can view your key pair by going to the “My Certificates” tab in Kleopatra, where you will see your private key and public key listed. 

### Linux/Mac

1. Create a GPG key pair
  - To create a GPG key pair, you can use the command:

```
1 gpg --gen-key
```


- This will prompt you to select the type of key you want to create, the key size, and the expiration date. For most purposes, the default options are fine.
- You will also be prompted to enter your name, email address, and a passphrase. Make sure to enter accurate information and a strong passphrase.
- Once you have entered all the information, GPG will generate your key pair. 

## Export your Public Key

To share your public key with others, you will need to export it.

### Windows


1. In Kleopatra, click on the “My Certificates” tab, select your key, and click on the “Export Certificates” button.

2. Select the location to save the exported certificate and give it a name like `firstlast_pubkey.asc` or `firstlast_public_key.asc`
3. Open File Explorer and go to the location here the file was saved. 
4. You can share this file with others so they can use it to encrypt messages to you or verify your signature on a document.
5. Email the public key to your instructor

## Linux/Mac


1. You can export your public key using the command:

```
1 gpg --export -a "Your Name" > publickey.asc
```

- This will create a file called “publickey.asc” that contains your public key. You can share this file with others so they can use it to encrypt messages to you. 
2. Email the public key to your instructor

## Import Public Key

### Windows

1. To import a public key in Gpg4win, you can use the drag-and-drop feature of the Kleopatra tool.
2. If you haven't done so, download your Professors public key at [https://drive.google.com/drive/folders/1FEePJLk6KZX\\_UT7UKNVX6pO31jbB0YBW?usp=sharing](https://drive.google.com/drive/folders/1FEePJLk6KZX_UT7UKNVX6pO31jbB0YBW?usp=sharing)
3. Drag the public key file(with .asc extension) onto the Kleopatra window.
4. Kleopatra will import the key and add it to your keyring.
5. You can view the imported key by going to the “My Certificates” tab in Kleopatra, where you will see the imported key listed. 

### Note:

- It's important to ensure that you are importing the correct public key, otherwise you will not be able to encrypt messages or files for the intended recipient.
- If you are importing a key that you did not generate, it is recommended to verify the key's fingerprint with the key owner before importing to ensure that you are importing the correct key.

File Name	Hash (SHA 256)
wcox_pubkey.asc	dd972e5cc9e11dbf58e80fb858cb5a9c232dd9c5d54253bb5





**Linux/Mac** To import a public key in GPG on Linux/Mac, you can use the command line.

1. If you haven't done so, download your Professors public key at [https://drive.google.com/drive/folders/1FEePJLk6KZX\\_UT7UKNVX6pO31jbB0YBW?usp=sharing](https://drive.google.com/drive/folders/1FEePJLk6KZX_UT7UKNVX6pO31jbB0YBW?usp=sharing)
2. Open the terminal and use the command:

```
1 gpg --import publickey.asc
```

Replace “publickey.asc” with the name of the public key file you want to import. (wcox\_pubkey.asc)

3. This command will import the public key from the specified file and add it to your keyring. 
4. You can view the imported key by using the command: 

```
1 gpg --list-keys
```

This will show you the names, email addresses, and fingerprints of all the keys in your keyring, including the imported key.


**Note:**


- It's important to ensure that you are importing the correct public key, otherwise you will not be able to encrypt messages or files for the intended recipient.
- If you are importing a key that you did not generate, it is recommended to verify the key's fingerprint with the key owner before importing to ensure that you are importing the correct key.

File Name	Hash (SHA 256)
wcox_pubkey.asc	dd972e5cc9e11dbf58e80fb858cb5a9c232dd9c5d54253bb5


## Encrypt a File

### Windows


1. Create a text document and name it encrypted-text.txt
2. Put the following message in the file “Professor Cox should give me a good grade!” 
3. Save the file
4. If you haven't done so, download my public key [https://drive.google.com/drive/folders/1FEePJLk6KZX\\_UT7UKNVX6pO31jbB0YBW?usp=sharing](https://drive.google.com/drive/folders/1FEePJLk6KZX_UT7UKNVX6pO31jbB0YBW?usp=sharing)
5. To encrypt a file using Gpg4win, you can use the drag-and-drop feature of the Kleopatra tool.
  1. Drag the file you want to encrypt onto the Kleopatra window.

2. In the “Encrypt files” dialog box that appears, select the public key of your Instructor.
3. Click on the “Encrypt” button.
4. Kleopatra will create a new encrypted file with the extension .gpg in the same location as the original file. The original file remains unencrypted. 
6. Email the file to your Professor

### Linux/Mac

1. Create a text document and name it encrypted-text.txt
2. Put the following message in the file “Professor Cox should give me a good grade” 
3. Save the file
4. If you haven’t done so, download my public key [https://drive.google.com/drive/folders/1FEePJLk6KZX\\_UT7UKNVX6pO31jbB0YBW?usp=sharing](https://drive.google.com/drive/folders/1FEePJLk6KZX_UT7UKNVX6pO31jbB0YBW?usp=sharing)
5. Encrypt the file using the following command:

```
1 gpg --encrypt --recipient "William Cox" encrypted-text.txt
```

6. This command encrypts the file “encrypted-text.txt” for the recipient “William Cox”
7. This will create a new file called “encrypted-text.txt.gpg” that is the encrypted version of the original file. The original file remains unencrypted. 
8. Email the file to your Professor.

### Decrypt a File

#### Windows

1. Email your professor asking for the encrypted file.
  1. Make sure your Professor has your public key.
  2. Your professor will create an encrypted file and email it back to you.
2. To decrypt the file using Gpg4win, you can use the drag-and-drop feature of the Kleopatra tool.
3. Drag the encrypted file (with .gpg extension) onto the Kleopatra window.
4. You will be prompted to enter your passphrase.
5. Kleopatra will create a new decrypted file with the same name as the original file(before encryption) in the same location as the encrypted file.
6. The encrypted file remains unchanged.
7. Open the unencrypted file and Answer the question.
8. Place the answer in your Lab report file.

#### Note:

- In order to decrypt the file, you must have the private key that matches the public key that was used to encrypt the file.
- If the private key and passphrase do not match the encrypted file, decryption will fail.

### Linux/Mac


1. Email your professor asking for the encrypted file.
  1. Make sure your Professor has your public key.
  2. Your professor will create an encrypted file and email it back to you.
2. To decrypt the file use the following command:

```
1 gpg --decrypt file.txt.gpg
```

3. This will prompt you for your passphrase.
4. The encrypted file remains unchanged but a new unencrypted file will be created.
5. Open the unencrypted file and Answer the question.
6. Place the answer in your Lab report file.

### List your keys

#### Windows

1. To list the keys in your keyring using Gpg4win, you can use the Kleopatra tool.
2. Open Kleopatra, click on the “My Certificates” tab.
3. You will see a list of all the keys in your keyring, including your own key pair and any imported public keys. 
4. You can see the name, email address and key ID of each key in the list.

You can also use the command line tool gpg.exe to list keys


```
1 gpg.exe --list-keys
```

This will list all the keys in your keyring, including your own key pair and any imported public keys.

### Linux/Mac



1. To list all the keys in your keyring, you can use the command:

```
1 gpg --list-keys
```

This will show you the names, email addresses, and fingerprints of all the keys in your keyring. 

## Revoke a key

### Windows


1. Create a new key with the following parameters:
  1. Name: bad key
  2. Email: bad\_key@badkey.com
2. Export the public key and name it bad\_pubkey.asc
3. Test the bad\_pubkey.asc
  1. Create a new file named bad-file.txt
  2. Encrypt the file with bad\_pubkey.asc
  3. Decrypt the file
4. To revoke a key using Gpg4win, you can use the Kleopatra tool.
  1. Open Kleopatra, click on the “My Certificates” tab.
  2. Select the key that you want to revoke.
  3. Click on the “Certificate” menu, and select “Revoke Certificates”. 
  4. A dialog box will appear, asking you to confirm the revocation and providing you with the option to create a revocation certificate.
  5. Select the option to create a revocation certificate, and select a location to save the certificate.
  6. Click on the “Revoke” button to complete the revocation process. 

#### Note:


Revoking a key is a permanent action and it cannot be undone. It's important to revoke a key if it has been lost or stolen, or if the private key has been compromised in any way. It's also important to share the revocation certificate with anyone who has your public key so that they can update their keyring and stop using the revoked key.

### Linux/Mac

1. Create a new key with the following parameters:
  1. Name: bad key
  2. Email: bad\_key@badkey.com
2. Export the public key and name it bad\_pubkey.asc
3. Test the bad\_pubkey.asc
  1. Create a new file named bad-file.txt

2. Encrypt the file with bad\_pubkey.asc
3. Decrypt the file
4. To revoke a key you can use the command: 

```
1  gpg --gen-revoke "bad key"
```

5. This will create a revocation certificate for your key, which you can then distribute to others to inform them that your key is no longer valid. 

## Reflection

Explain GPG and why it is important?

### Requirements:

1. Follow Lab File Formatting (beginning of this document)
2. Words - limit to 1 page
3. APA or IEEE
4. 3 sources minimum
5. If using markdown, 5 extra points will be added to your score. If you get a 100 then you will receive 5 points extra credit.