Laboratory Exercise – Cryptography Using PGP

Submission: Provides screen captures to backup your work and answer the questions at the end.

1. Overview

In this lab, students will:

- Gain experience in installing the PGP encryption tool and creating key-pairs
- Encrypt and securely handle sensitive files and data

Lab Theory: Cryptography is used to protect information by transforming it into an unreadable format called cipher text. Only the person or persons possessing the key can decrypt and read the data. In other words, if the message falls into the wrong hands, that person cannot make sense of the message because they do not possess the key.

PGP uses key pairs, one public and one private. The public key is distributed to everyone. That key will be used to encrypt the data and send messages to the owner of the public key. The owner then uses their closely guarded private key to decrypt the data into a readable form. Since only the owner of the public key should possess the private key, only he or she can decrypt the message.

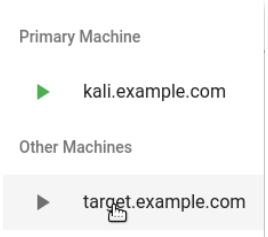
2. Resources required

A Windows virtual machine running in the Cyber Range and the **PGP Desktop Win64-10.1.1** application.

3. Initial Setup

In this lab, you will log in to your Cyber Range account and select the ***Kali Linux and Vulnerable Windows 7(64bit)*** *VMs* environment, then click "start" to start the environment. You will be using the Windows 7 VM in this exercise (target.example.com) on the Cyber Range.

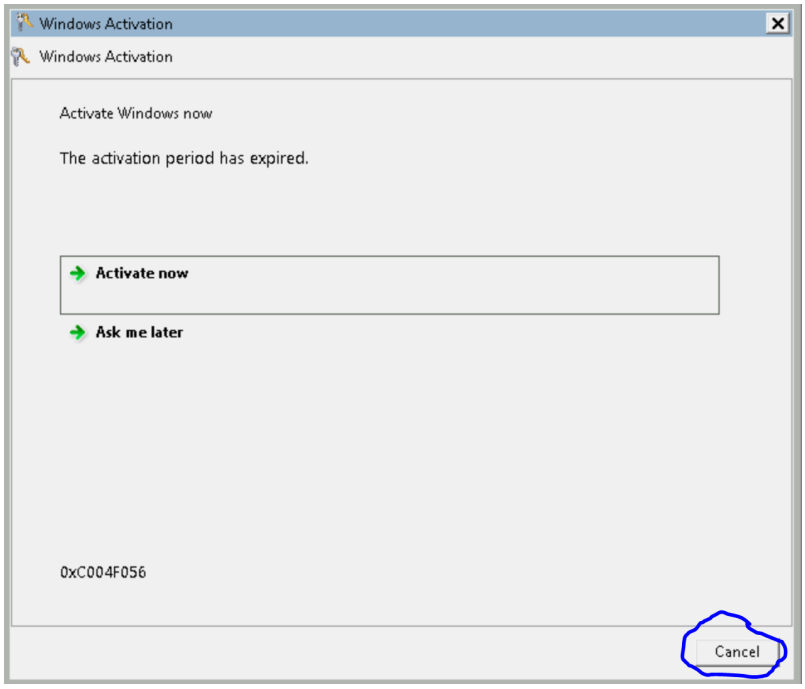
3.1. **Log into the Cyber Range (you activated your account at the beginning of the course)**



3.2. **Log into Target Windows VM:** Click on the Join (play) icon and select the login for the target.example.com machine. When the familiar Window login pops up for that VM, click on the **student** button, and then enter **password=student** (if needed).

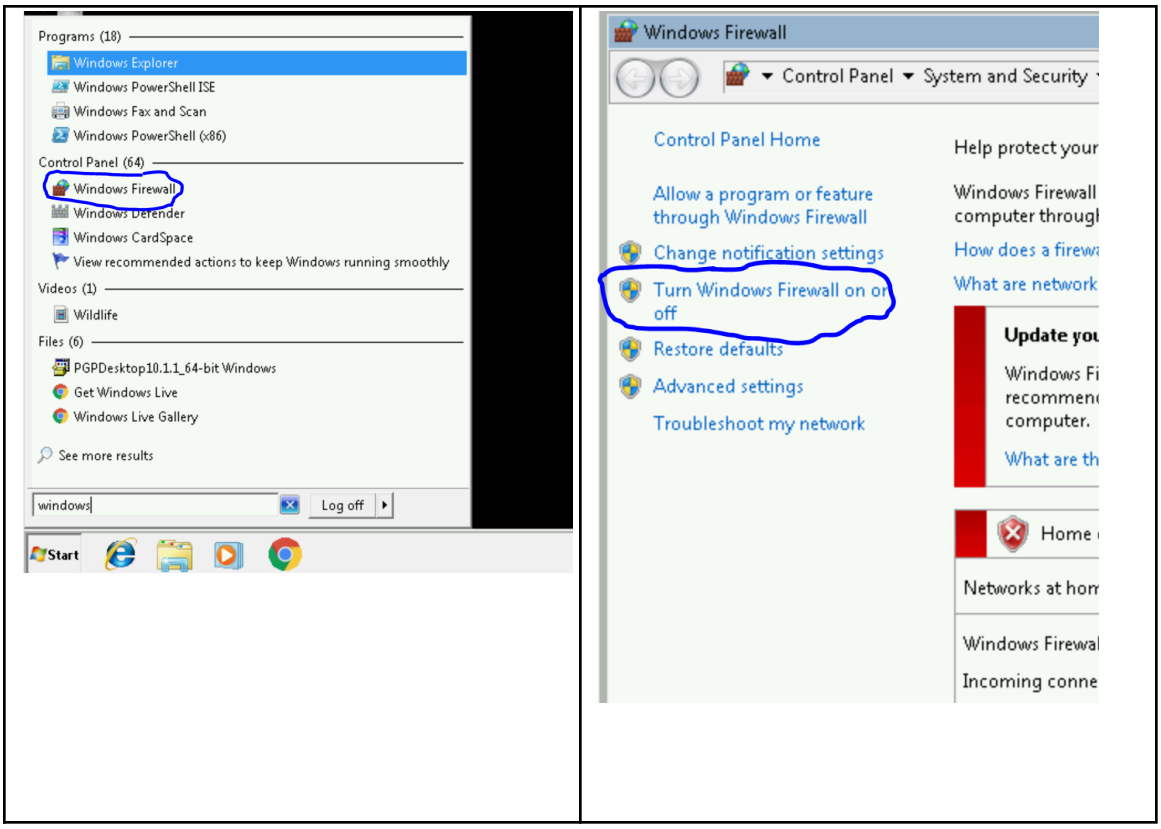
3.3. Once logged into the Windows desktop, a one-time "Windows Activation" window may pop up. If it does, just bypass this by clicking on the "**Cancel**" button. [NOTE: We are not registering this OS since this is for temporary, educational use.]

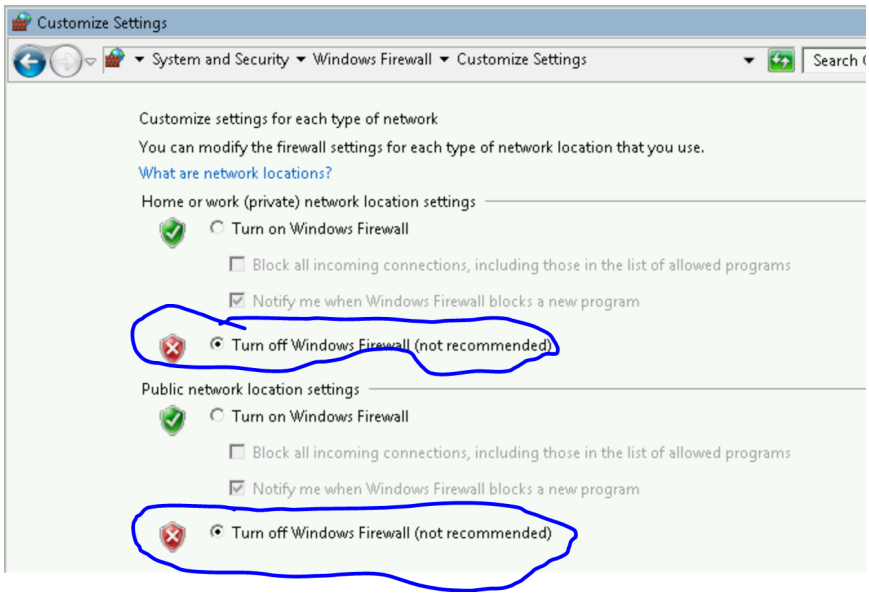
NOTE*: DO NOT select "Activate Now" or this will cause problems for you and you'll have to ask me to reset your VM environment.*



3.4. **Set Windows Network Location:** If you have never booted this VM before, you may also get this one-time network security check the first time this windows system comes on line and sees a new network. If you get this "Set Network Location" requester, you will get three options, "Home Network" (trusted), "Work Network" (trusted), or "Public Network" (untrusted). Select either Home or Work so that the Windows firewall will be disabled and you will be able to attack this target system from the Kali VM if required.

3.5. Disable the windows firewall. Please make sure the Windows Firewall is disabled. You will not be able to download the files below if the Windows Firewall is **ON**





3.6. **Download Lab Artifacts (files):** This lab requires **the PGP-10.1.1 encryption software package**. If this lab's artifacts (the PGP install package and Guo.txt file) are not on your desktop or in your Downloads folder already, download these exercise artifacts onto ***your Windows VM*** before continuing:

- Windows PGP Desktop Package - https://vacr.io/art_guo_3C_winpgp
- Sample Text File - https://vacr.io/art_guo_3C_txtfile

*Special Note: This lab contains two steps to complete the lab. In the first step below (i.e. **4.1 Install PGP Desktop Win64-10.1.1 and Create Your Own Keys**). You need to read the prompts in each step before clicking on Next. Doing so helps you to better understand the concepts.*

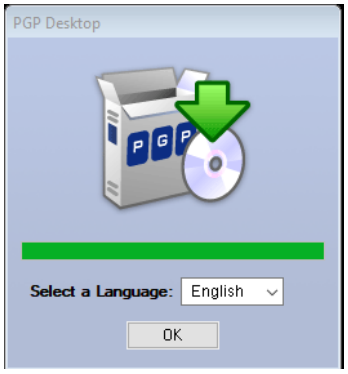
4. Tasks

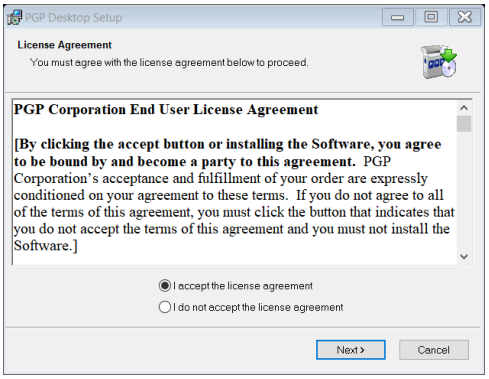
The required tasks for this lab are split into two steps: install PGP and then use PGP to encrypt files.

4.1: Install PGP Desktop Win64-10.1.1 and Create Your Own Keys

4.1.1. Navigate to your Windows Download folder, right click on the executable and select "Run as Administrator" and click "Yes" if prompted.

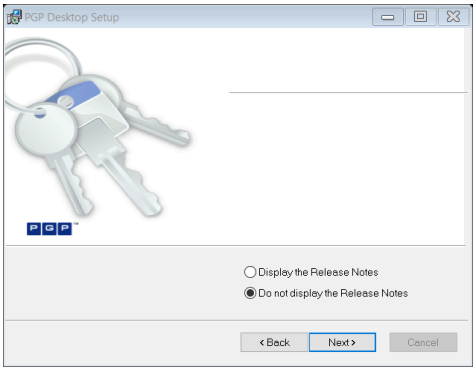
4.1.2. Leave the language setting default as English, click Ok, and on the 'Licensing Agreement', choose 'Accept agreement' and then click Next.



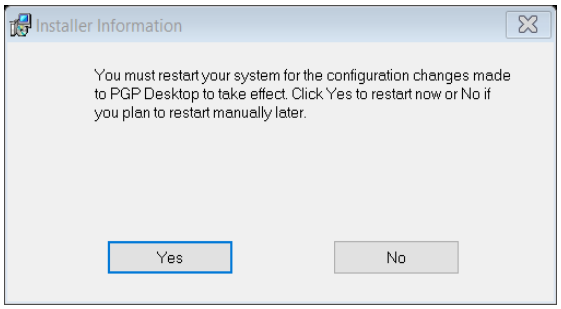


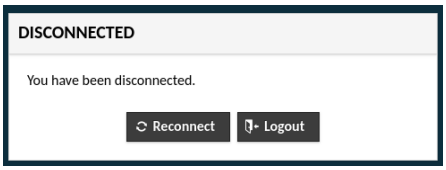
4.1.3. Choose 'Do not display the Release Notes', then click Next.

If a window notification shows up and asks for permission, then select "Yes" and wait 30-60 seconds for the installation to complete.



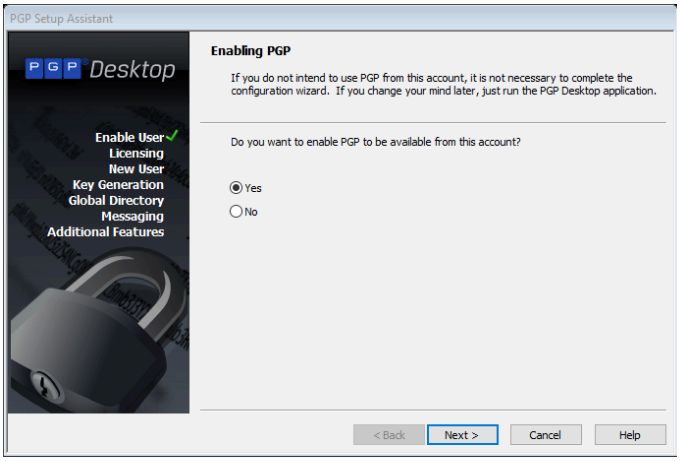
4.1.4. When prompted to reboot the computer, click ‘Yes’. Give the VM around a minute, and then click on the ‘Reconnect’ button (below).



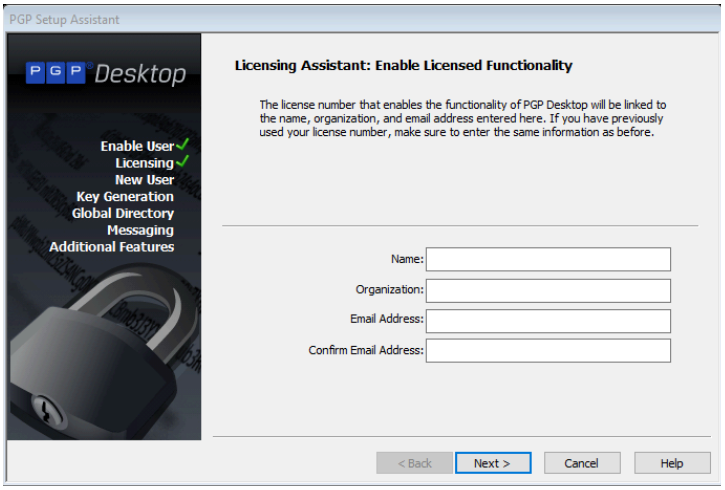


4.1.5. Once logged back in as the student user, a guide should appear asking: 'Do you want to enable PGP to be available from this account?'

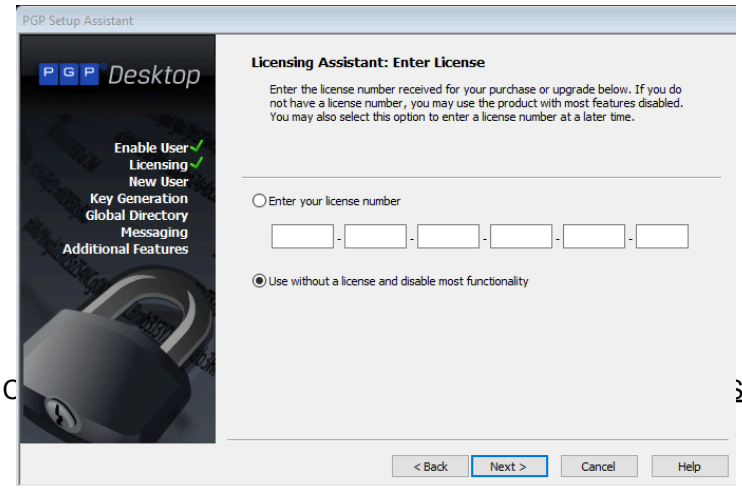
Select Yes and then click Next.



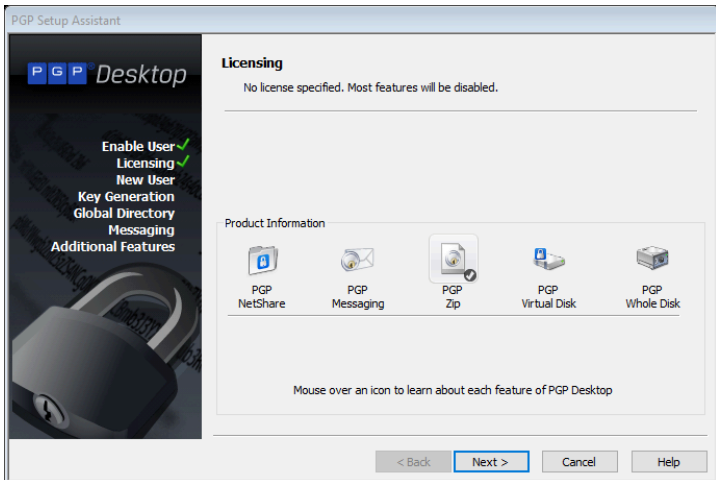
4.1.6. Enter your personal information into the fields and click Next.



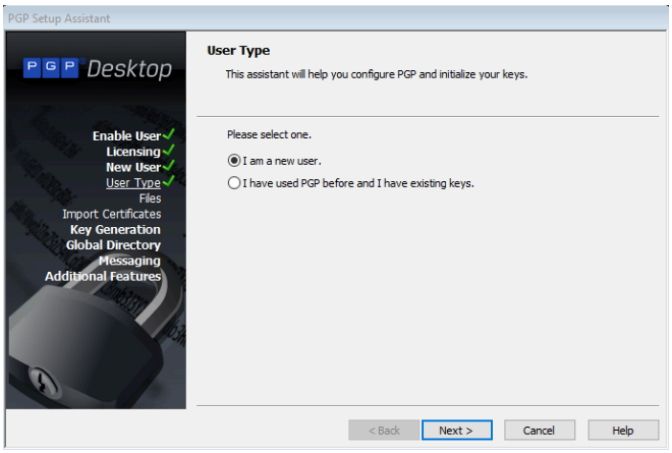
4.1.7. Select 'Use without a license' and Click Next.



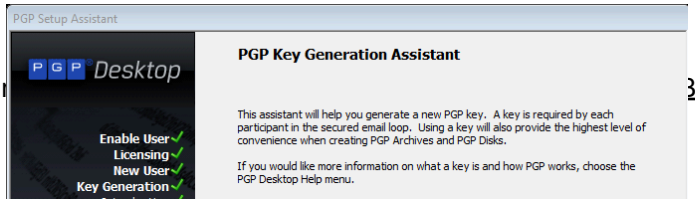
4.1.8. The Licensing page shows this. Just click Next.



4.1.9. Select I am a New User and click Next.

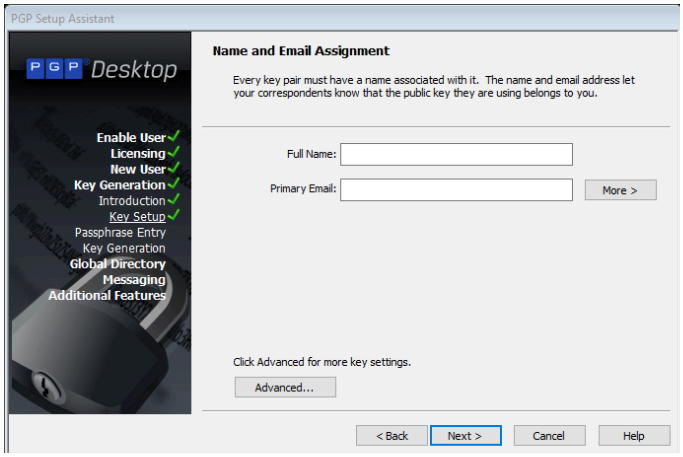


4.1.10. Now the PGP Key Generation Assistant should be asking you to create your own keys. Click Next.

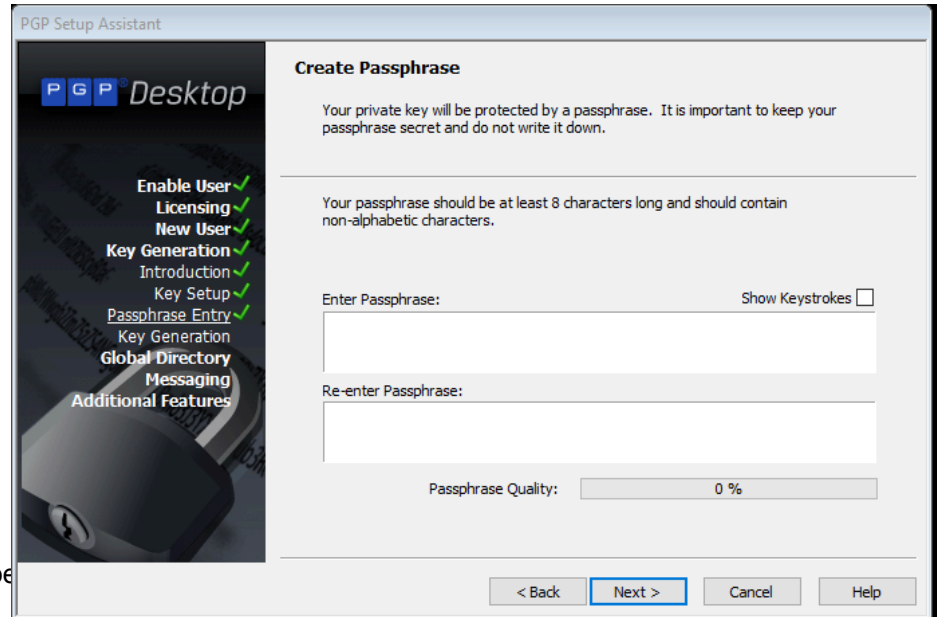


4.1.11. Enter your name and email. Click Next.

NOTE: *More than one email can be associated to the same key, but you need only one in this exercise.*



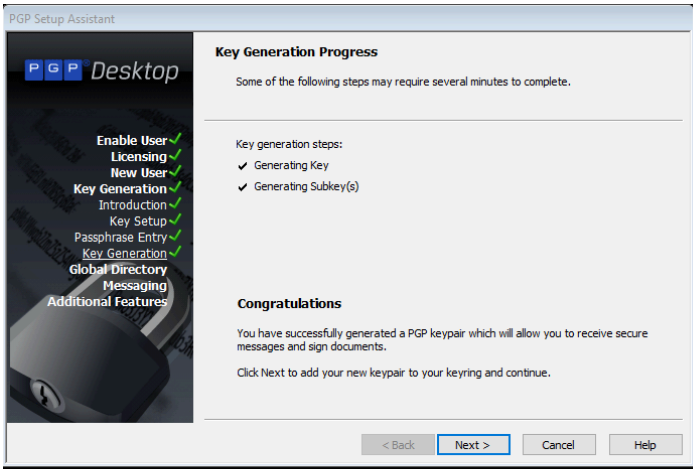
4.1.12. Provide the paraphrase (twice) that protects your private key, and click Next.



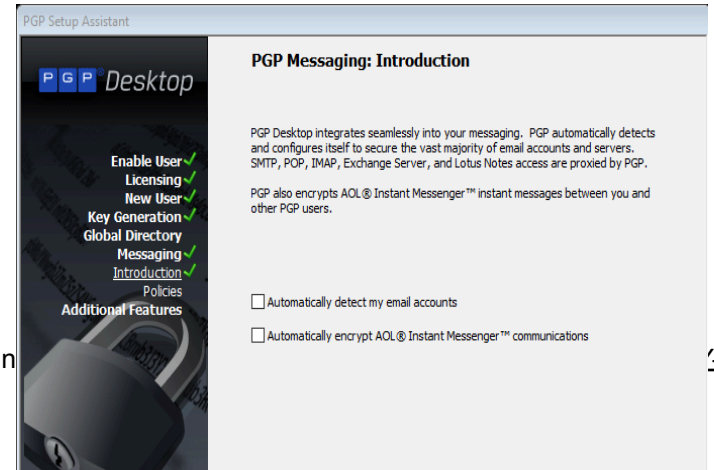
NOTE: *A passphrase is a string of multiple meaningful words that will give you an easy to remember, 20-30 upper/lower characters, numbers and special characters. Make it easy to remember, but most importantly, make it long.*

NOTE: *Remember, it is critical that the private key is always kept private. Never email it, post it, share it, or give anyone else access to the drive it is stored on. Some security minded people prefer to actually store their private key(s) on a smart-card (left) or a thumb drive (right) instead of a laptop that can be stolen.*

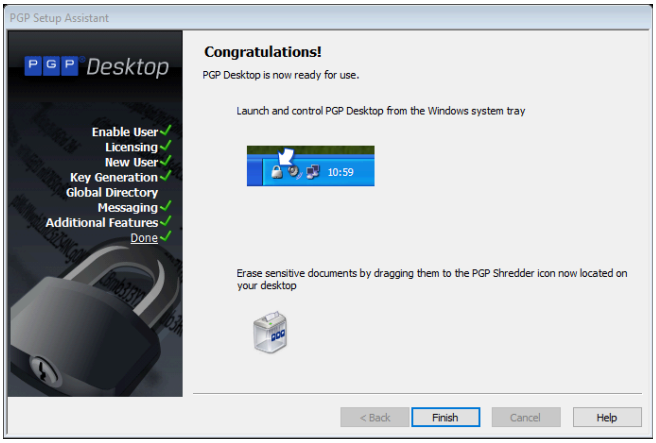
4.1.13. A “Key Generation Progress” window pops up indicating that a pair of public/private keys has been created for you. Click Next.



4.1.14. Uncheck both Auto-detection options and click Next.



4.1.15. At the “Congratulations!” prompt, Click Finish.



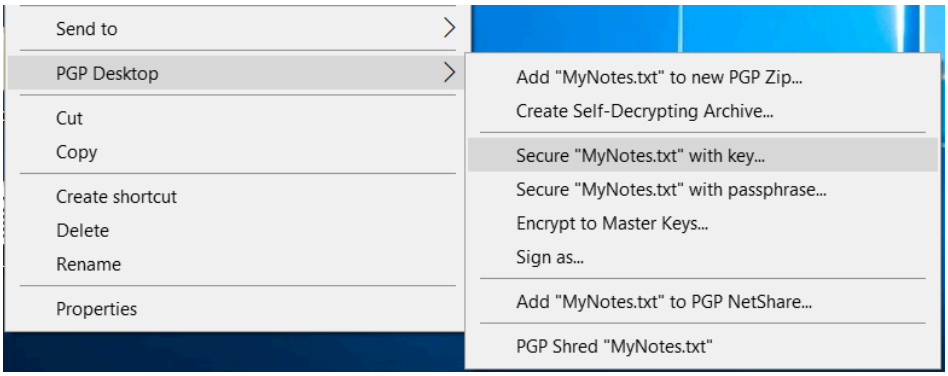
4.2: Encrypt Files Using Keys

4.2.1. **Prepare Your Sensitive Text File:** After successfully completing all steps in the previous section, now encrypt the sensitive-info document **Guo.txt** file (previously downloaded) or create your own sensitive text file, and follow the step below.

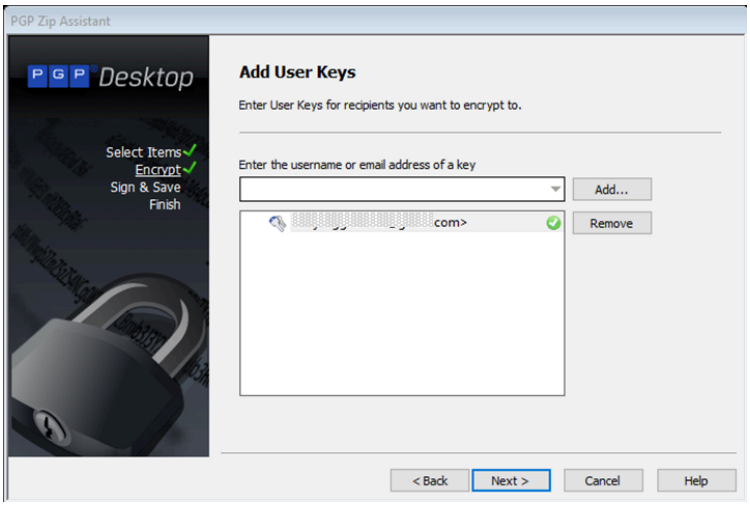
If the text file was downloaded, move it to your desktop and rename it (right click, rename) **MyNotes.txt**.

This file simulates a "sensitive info" file you might need to insecurely transfer via email. Populate it with info like bank account info (fake), SSN(fake), birthdate, or the type of data you would put on a car loan application.

4.2.2. Right click on the text document and select "**PGP Desktop / Secure MyNotes.txt** with key"

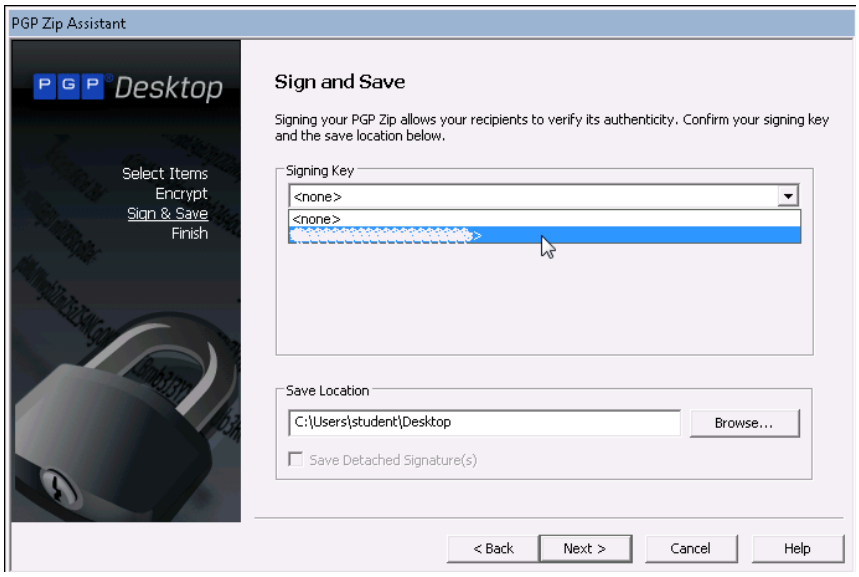


4.2.3. Select the key with your username and email (look for the green check mark) and click Next.



NOTE: *This step is optional if the username you created before is automatically added by the system (already has green check mark). If so, just click Next.*

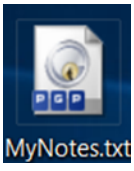
4.2.4. Select the signing key in drop-down list. Customize the save path as you like. Click Next.



USECASE NOTE: *In this example, you are essentially encrypting a file to yourself. A good use case in which you might do this is filling out a bank loan document or PDF at work, and needing to securely email it to your personal/home email for printing for the bank (for example). You should never email sensitive files like this without encryption, even if a bank or vendor naively asks for it.*

FUNCTIONALITY NOTE: *The system that you decrypt this on will need to access your private key (since it was encrypted with your public key). So obviously this would require either the same keypair on your home machine, or portably installed on a thumb drive or smart card.*

4.2.5. Once the Encryption Wizard disappears, an encrypted and signed file named **MyNotes.txt.pgp** will be created on your desktop. Try to open this file with notepad or WordPad and examine the encrypted data.



NOTE: *The .pgp file extension may be hidden, depending on your user file browser settings. The full file name can be seen by either changing this setting in the file explorer, or jumping into the CMD.exe (black text terminal) and typing* ***`dir Desktop`***.

INFO ON SECURE FILE SHREDDING: *If you look at the left side of the desktop after PGP installation, there is a newly added PGP Shredder icon. As a best practice, after creating a secure/encrypted file, you should consider destroying the original unencrypted file using the PGP Shredder (after encrypting it). Doing so is much more secure than deleting files (even with Shift+Del), which can be still recovered via raw drive forensics by hackers or anyone who has physical access to this computer.*

Complete the Following Review Questions after the above exercises:

1. **Decrypt Before a Reboot:** Without rebooting, decrypt the file back to the original file by right clicking on the file and selecting **PGP Desktop / Decrypt & Verify**.
   What did the system do? It booted up the PGP Desktop app and verified the file

2. **Decrypt After a Reboot:** Now reboot the system from **Start** and typing **`shutdown -r`** (from the Search Programs field). After waiting a minute or so, reconnecting and logging back in, now decrypt the file again.
   What did the system do differently, and why? The system asked for a password, because it is best practice

3. **Encrypting Files for Others:** What would be required to encrypt something TO a co-worker in a business environment so that only they could decrypt it? Their Public PGP Key

4. **Encryption & Security:** Why has encryption become such an important part of securing network transmissions such as e-mail? Emails have now become a standard for communication, including important information. Whether it is a Bank Loan, Personal health information, or your social security number - people are using email to send things that could be used by malicious entities for their personal gain. Whatever means possible at the time, there is a chance your emails can be intercepted or read. Encryption is another way for you to layer defense on your data, even if it is intercepted an encryption can help hide your information from prying eyes.

5. References

KSAs from NIST SP 800-181: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

- K0167 Knowledge of basic system administration, network, and operating system hardening techniques.
- K0335 Knowledge of current and emerging cyber technologies.

- S0040 Skill in implementing, maintaining, and improving established network security practices.
- S0121 Skill in system, network, and OS hardening techniques.
- S0138 Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).

NSA/DHS CAE Knowledge Units:
https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf
(you may need to accept an invalid iag.gov SSL certificate to reach this PDF)

- Basic Cryptography (BCY)