

Lab 7: PGP
Due: 11/4/09 in class

Pretty Good Privacy (PGP was initially created to encrypt individual messages – but now it is so much more, including protecting or shredding stored data. There are commercial and freeware versions of PGP, with the latter having less functionality.

The commercial version of PGP supports both symmetric encryption and PKI; it also creates message digests using hashing algorithms.

Algorithms supported by PGP	Sample
Symmetric key	AES, IDEA, TripleDES, Twofish
PKI	RSA
Hashing	SHA-1, MD5

Objectives of the Lab: to gain a working understanding of PGP and PKI

Important: Although the instructions are quite thorough, this lab does take some time to complete properly. It may require a degree of trial and error and thought. Please be sure to start early so that you can play around with the tools. In fact, the lab requires you to familiarize yourself enough to do the last parts on your own.

1. Start up your VM
2. Click on the link below for the trial version page of PGP at <http://www.pgp.com/downloads/desktoptrial/desktoptrial2.html>
3. Read the page and then Accept the License Agreement



Note: The version you are downloading is valid for only 30 days – after that you will only be able to decrypt email messages, but not encrypt any new ones. But remember there are versions that are completely free (though with limited functionality) that are available to you as scholars.

4. You will need to provide your name/ alias and a proper email address.

Home > Products > PGP Desktop Trial License

PGP Desktop Trial License

Please complete the information below, then click on the download button matching your OS platform choice

First Name*	Last Name*
<input type="text"/>	<input type="text"/>
Title	Telephone*
<input type="text"/>	<input type="text"/>
Company	Address 1*
<input type="text"/>	<input type="text"/>
Address 2	City*
<input type="text"/>	<input type="text"/>
State	Postal/Zip Code*
Select a State <input type="button" value="v"/>	<input type="text"/>
Country*	
Select a Country <input type="button" value="v"/>	

Download information will be sent to your email address:

Email Address*	Confirm Email Address*
<input type="text"/>	<input type="text"/>

Which PGP Desktop product do you currently use?*

What feature of PGP Desktop interests you most?*

What is the size of your organization?*

Estimated users in organization using encryption?

What is your primary motivation for using PGP Desktop?*

What email client do you primarily use?*

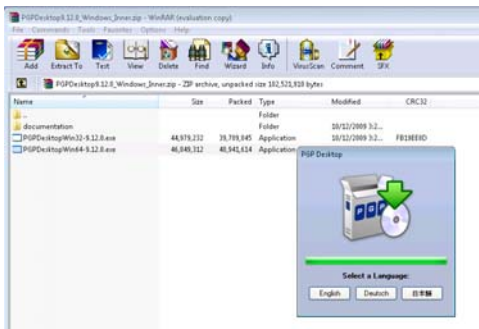
5. PGP will email you a personalized link for the actual PGP download.

The screenshot shows the PGP website interface. At the top, there is a navigation bar with links for Products, Purchase, Downloads, Support, Partners, Newsroom, Company, Careers, and Contact. The main content area is divided into three sections:

- Customer and Order Information:** Displays Order #1370210, fulfilled on October 27, 2009. It lists the purchaser as Nazli Moll (nazli.mollah@millersville.edu) and the purchase location as Millersville University, Millersville, 17551, United States.
- Product:** Shows 1 seat of PGP Desktop Corporate 9.12 for Windows - 30-Day Trial. The SKU is QEAD27XE and the license key is D4HAD-Q4WM4-VD14A-Y1QMN-OBPGE-SZA. It is noted as an Evaluation License.
- Helpful Links:** A list of links including "How to download and install PGP Desktop for Windows", "How to download and install PGP Desktop for Mac", "HOW TO: Perform the Basic Functions of PGP Desktop 9.x", "Help with licensing your product", and "Customer Service and Technical Support".

There is also a section titled "How to License Your Product" with a note: "NOTE: If you have purchased multiple seats, you will need..."

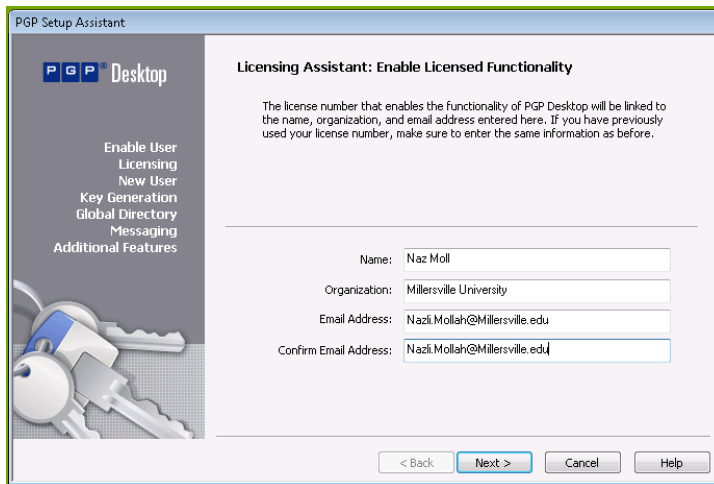
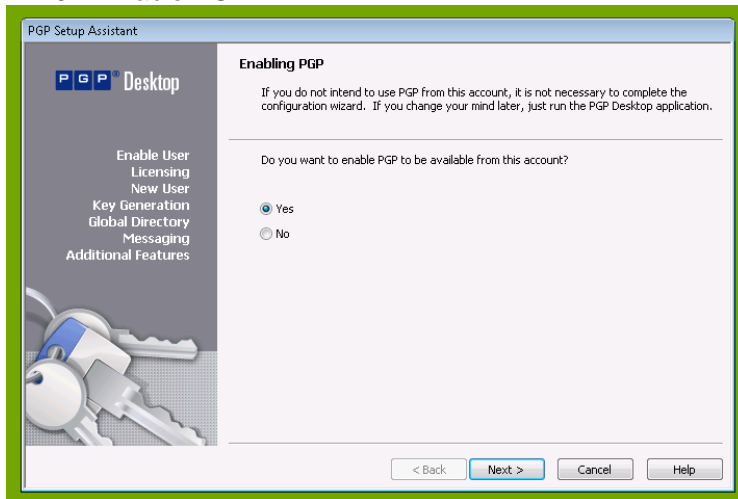
6. Your email will contain a .pdf file that contains your License Number, amongst other things. Make note of this number since you will need it soon.



7. Carry out the installation process

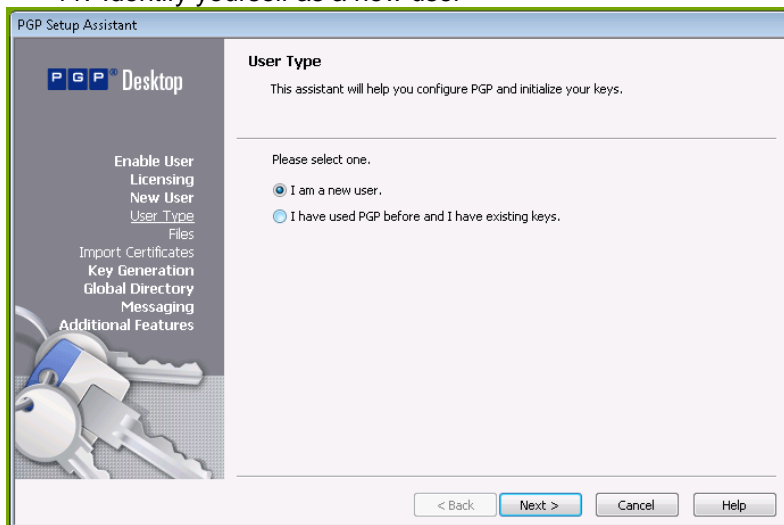
8. You will need to restart your machine (VM)

9. Enable PGP

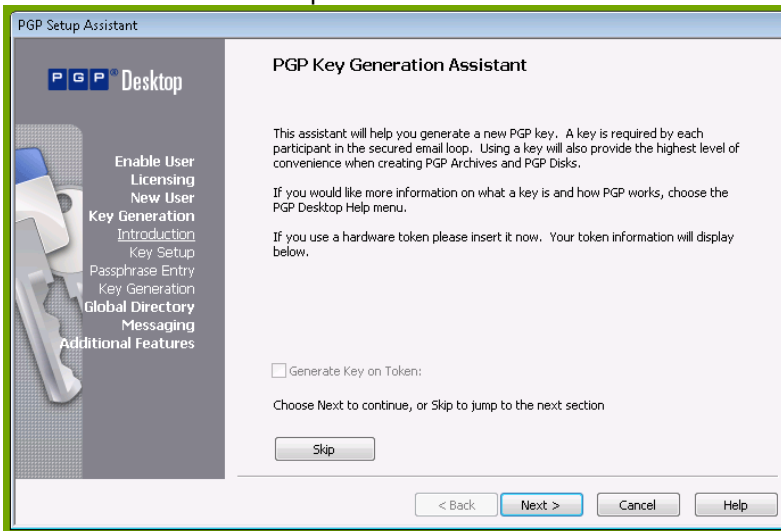


10. At this point you will be asked to enter your license number – go ahead.

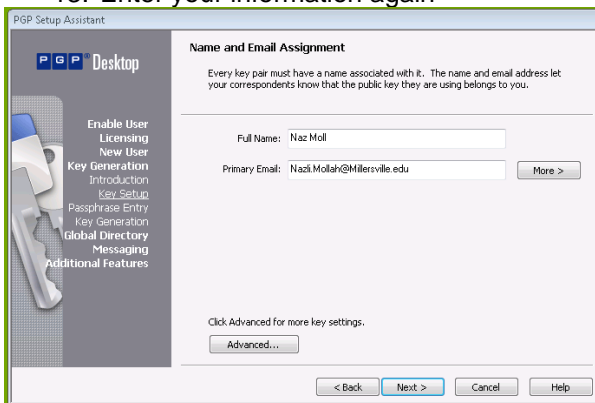
11. Identify yourself as a new user



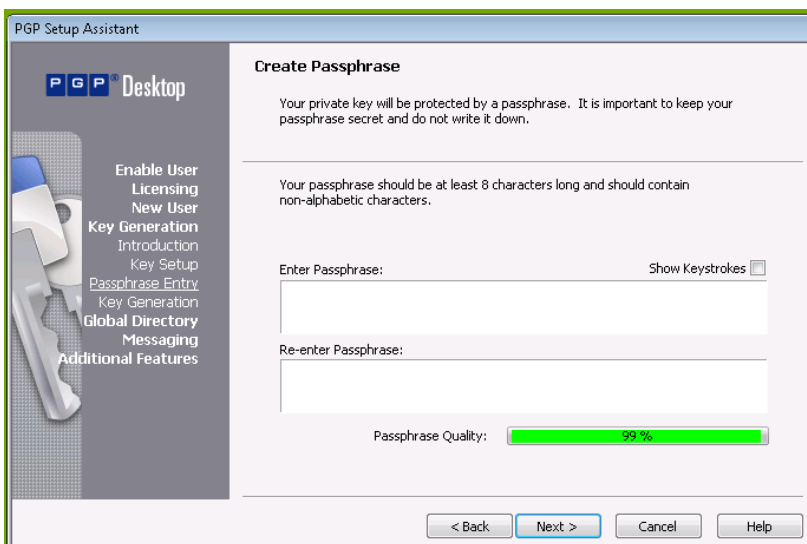
12. Click on “Next” or “Skip”



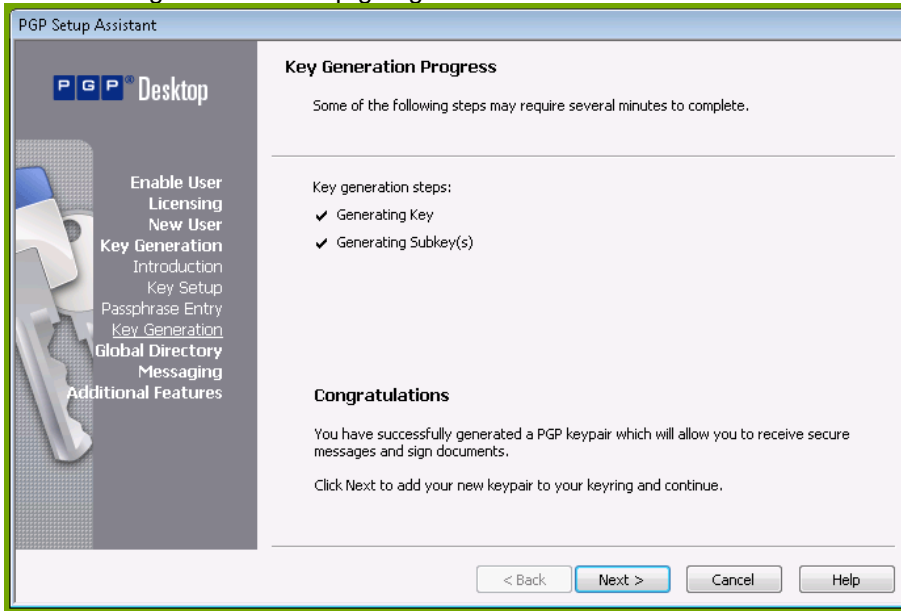
13. Enter your information again



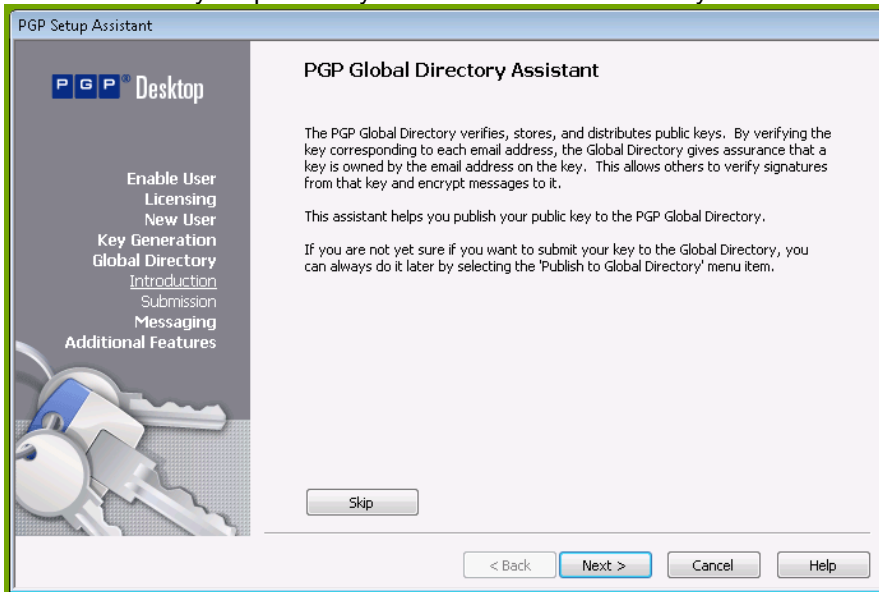
14. Enter your passphrase – you can choose to either show your keystroke or hide your typing. Remember it! (Yours truly forgot hers and had to start all over again!)

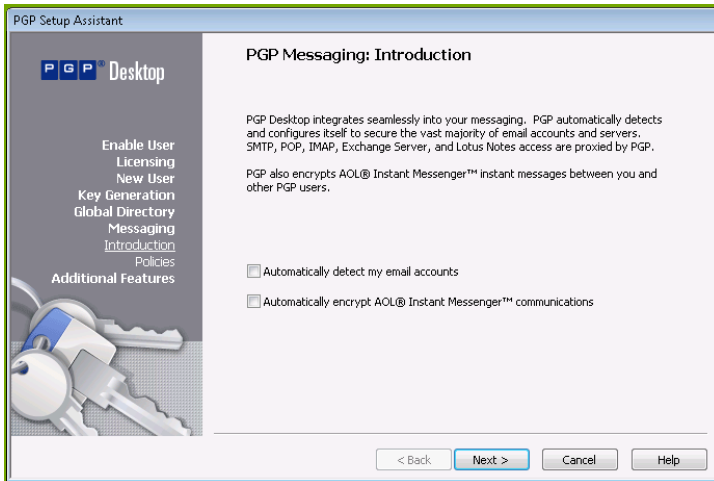
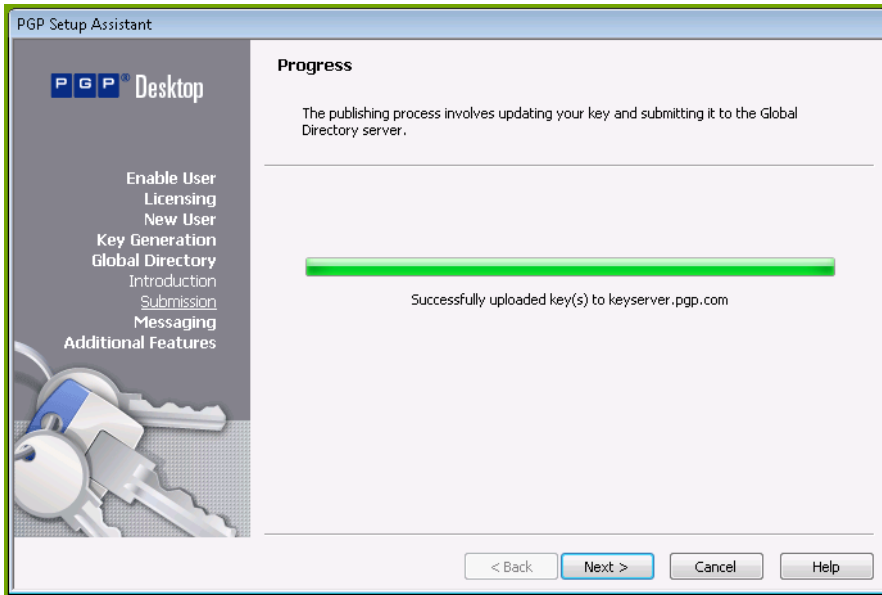


15. Congrats! – But keep going

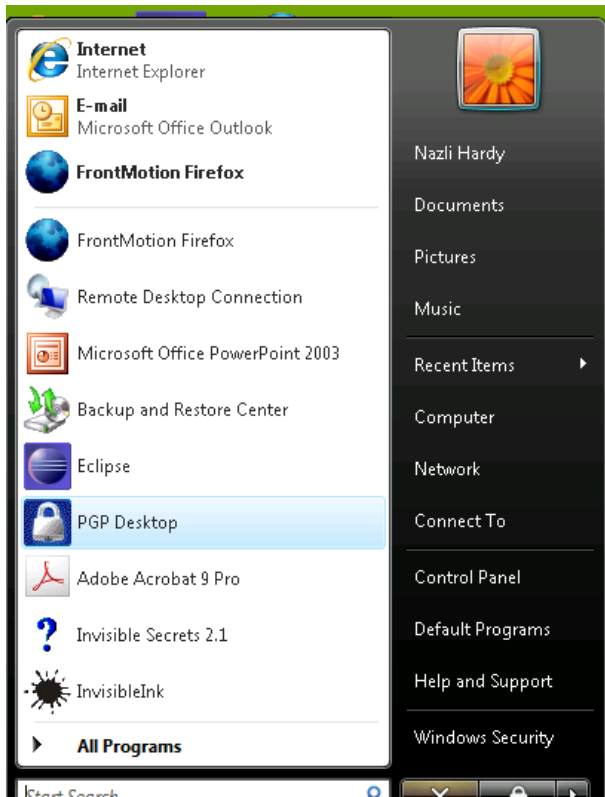


16. Publish your public key to the PGP Global Directory



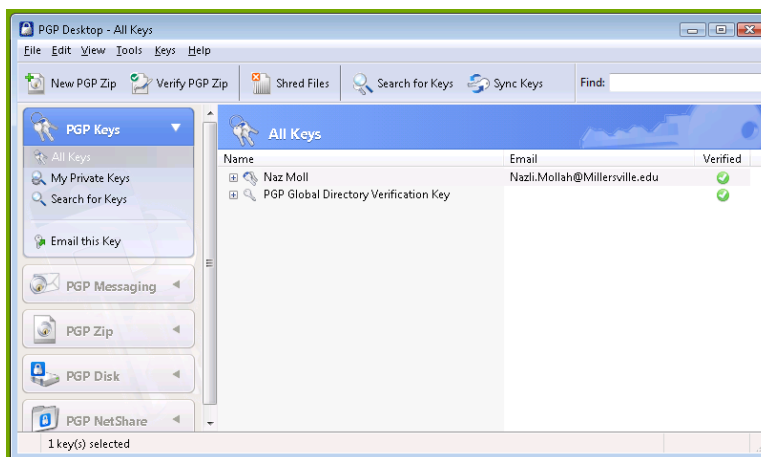


Note: you will need to restart your vm soon to be able to use PGP.

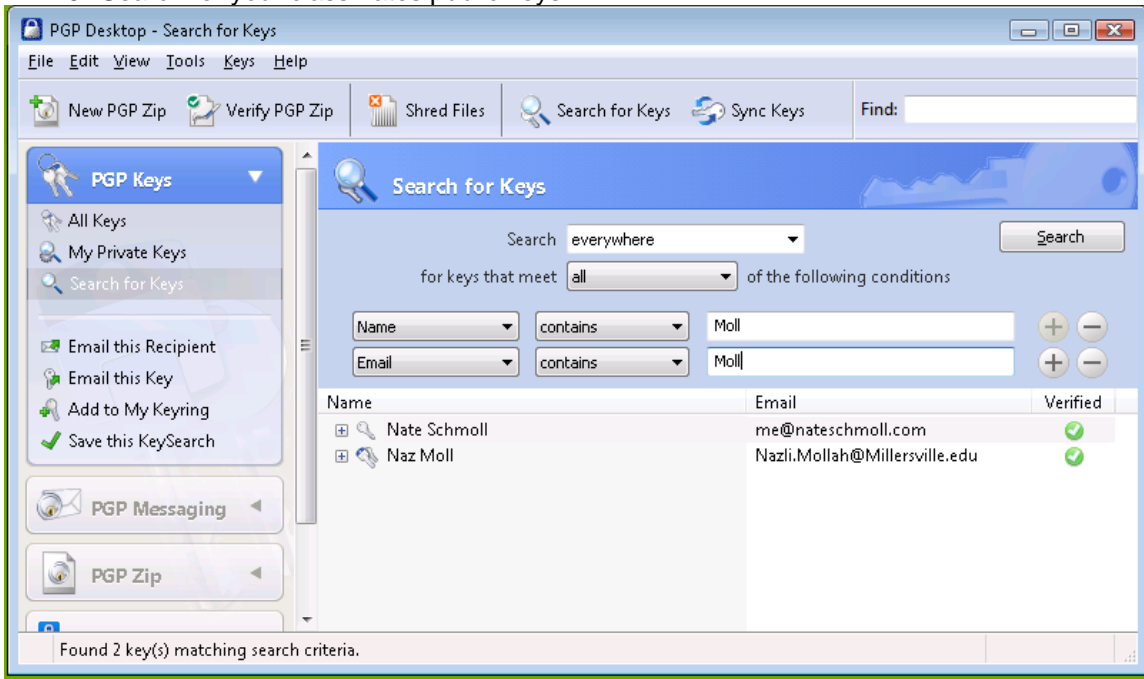


17. Click on Start and then PGP Desktop

18. Shred a file (you may have to create one that you don't want to see ever again)

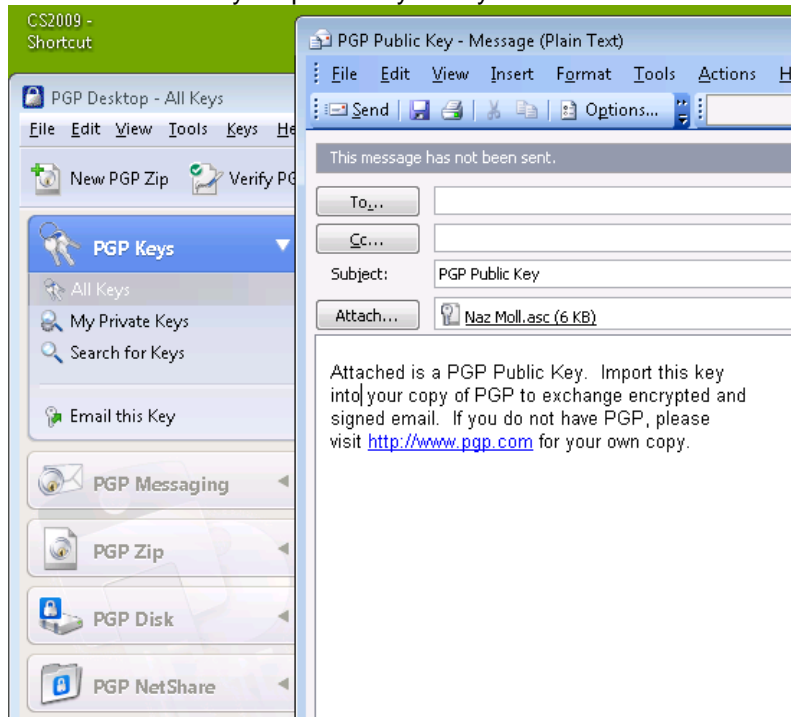


19. Search for your classmates public keys



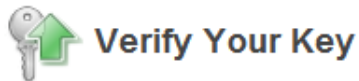
20. Play around . Click on “All Keys” and “My Private Keys” on the left bar

21. You can email your public key to anyone



Some additional steps

22. Check your email for this message and complete the verification key



A PGP public key containing the email address nazli.mollah@millersville.edu has been submitted to the PGP Global Directory.


 [Complete the Verification Process](#)

To verify this key submission, please visit the PGP Global Directory by clicking the button above. You will have the opportunity to review the details of the submitted key to ensure that it is your key, and then choose to accept or deny it.

If you did not submit this key or do not want this key in the PGP Global Directory, you may delete this message and take no further action. The key will be automatically deleted within 14 days and you will not receive any further email.


Thank you for your interest in the PGP Global Directory.

Email Address Confirmed

 Your email address has been verified, and the key you submitted is now available in the directory.

Your correspondents may find your key by searching on this website, or by adding this directory (keyserver2.pgp.com) to their list of directories.


To ensure that your PGP software trusts keys verified by this directory, you must download and trust this directory's Verification Key.

 **Download the Verification Key**

After downloading, import the Verification Key into your PGP software. Then, sign the key with your key and mark it as Trusted. Please see the documentation for your PGP software for specific instructions on trusting a key.

Done

Publish Your PGP Public Key

 Upload your key to the PGP Global Directory - Verified Key Service by either browsing to a file on your computer or pasting a key block.

Upload Key File


C:\keyserver2.pgp.comGlobalDir
 (C:\keys\mypublickey.asc)


23. In order to send/receive encrypted email to/from your friends' search for their email addresses here: <https://keyserver2.pgp.com/vkd/GetWelcomeScreen.event>

Search For Keys

Enter a name, email address, or key ID [advanced](#)

The PGP Global Directory is a free service designed to make it easier to find and trust the universe of PGP keys. Publish your key today and allow others to start sending you secure email.


 **Publish Your Key**
Upload your PGP public key to make it searchable by the PGP community.


 **Remove Your Key**
Remove your key from the searchable directory.

0% of DownloadKey.event from keyserver2.pgp.com Com...

File Download

Do you want to open or save this file?

 Name: key0x8D24933227FCF1B4.asc
Type: PGP Armored File
From: **keyserver2.pgp.com**

 While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. [What's the risk?](#)

Search Results

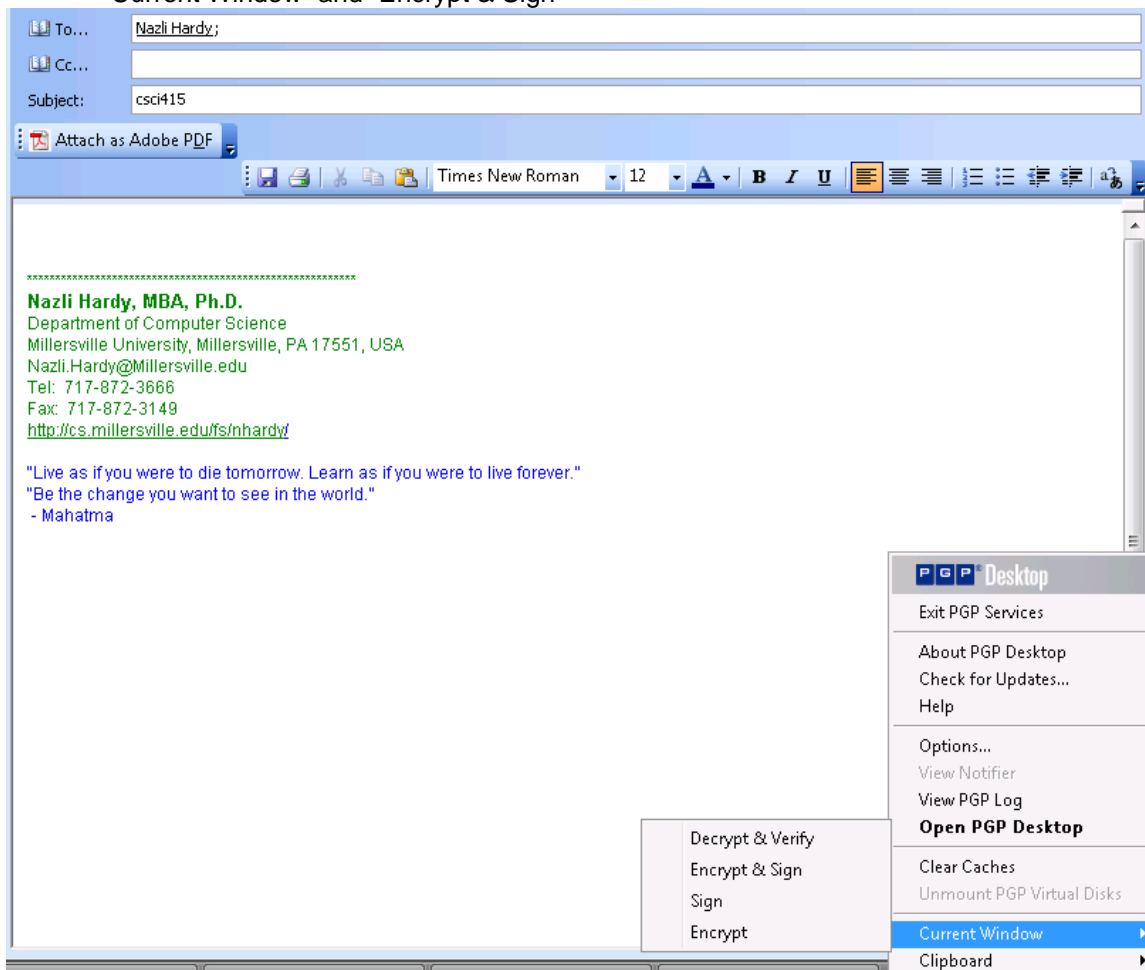
Select key(s)

Select the key(s) you would like to import to your keyring:

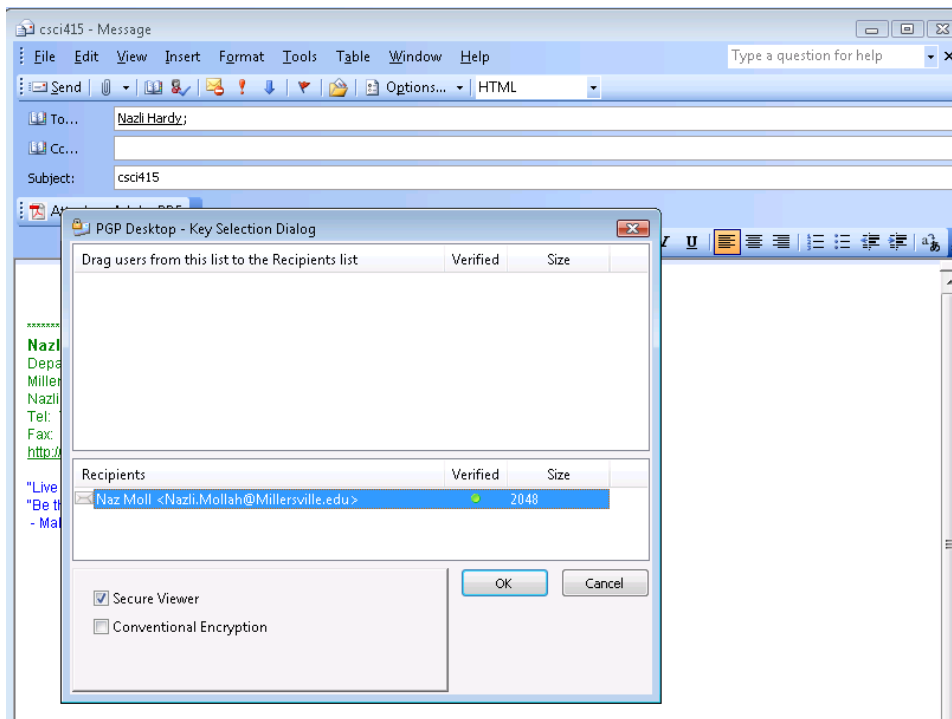
Name	Email	Verified
<input type="checkbox"/> Naz Moll	Nazli.Mollah@Millersville.edu	<input checked="" type="checkbox"/>

Select All Unselect All Import Cancel

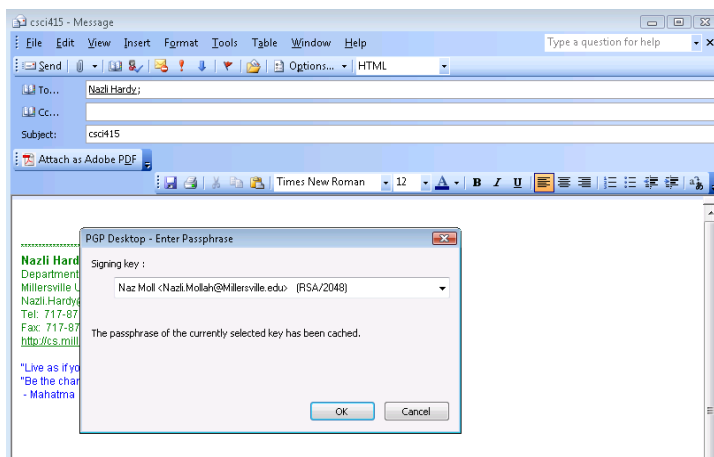
23. Send an email to your designated friend
24. Click on the PGP icon on the bottom right hand corner
25. There are a few ways to carry out the next step – but most of you will be able to use the “Current Window” and “Encrypt & Sign”

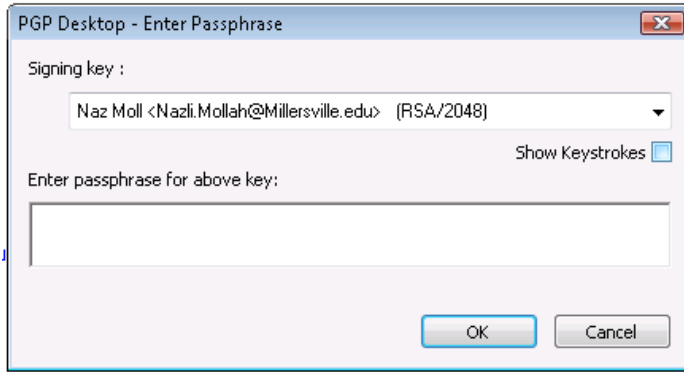


26. Add your recipients (try to figure this out ...)



27. At this point you will see this pop-up window or you may need to re-enter your passphrase depending on much time has elapsed





At this point you should be able to figure out how to do the following:

- send an encrypted message to your designated friend in class – his/her email address and public key should be in the PGP global directory
- have someone in class send you an encrypted message using your email address/public key from the PGP global directory
- decrypt this email sent to you

Please spend a few hours over the week to find your way through PGP.

What to hand in

Print a screen shots of the

- a. encrypted email you have received (please include the address of the sender and the time it was sent). Paste onto a Word document (with you name, class, professor, date)
- b. decrypted version of the email message (for which you used your private key)