

6.3.1

Email Encryption / Decryption (PGP)

BEGIN PGP MESSAGE

qANQR1DBwU4D9aFrzuWBnR4QB/9GrTlu9YuQQBDmJmvZiKW
uz3XBQXBWW3e390AYyK67pmcm3F5JQ1bl8s3L/3HF1zqAGEH4
Vmf4Qdje4fPUI4FYhjGAaq4aYlge65315KegS3PevzKXSjfDV42BW
fMZA33xNTbBKxL6H/BhZkHapLomKis3LfN5ghOatCqx6agU0LIQ
hU+pkjznOXrmY0lgtf2r56LYmEdV2GELfNcL1oxjm7Gl9V342R1E/
BGfvANJ6zHcEkeXoKkfUSPsQmblqSvglktKkf9WVzxfwlvFhZGA
BG3r5VpTPl5/vyzSxjo4YiF0qnXn+OctXALr7BXQv7k/WDNxXm1a
OcueVjHMoBHCACuhDjj7NSADNqS



Laboratory Overview

Objective

At the end of this lab students will be able to encrypt and decrypt messages using PGP.

Information for Laboratory

- A. Students will create keys and passphrases to use for sending and receiving email.
- B. Students will create hotmail accounts for this lab.
- C. Students will list reasons why they would use something like this in a business environment.

Student Preparation

Students will have completed requisite reading. Students will require paper for notes and should be prepared to discuss the exercises upon completion.

Students will be sure that the freeware version of PGP 6.5.8 is available for download, that MS Outlook Express is loaded on their computers, and that they have internet access.

Estimated Completion Time

45 Minutes



Email Encryption/Decryption

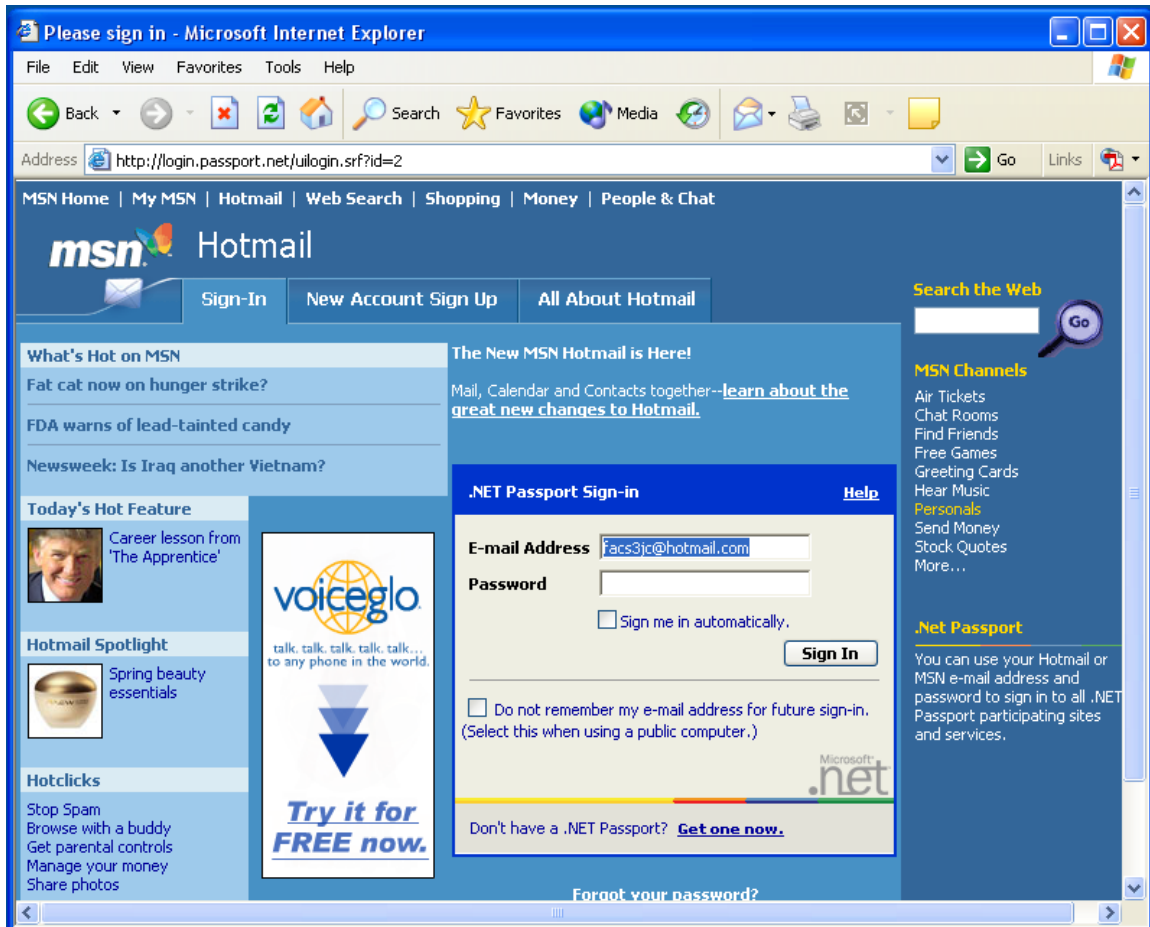
SMTP sends messages in clear text across the internet. Obviously, this is very insecure. There are two main standards for encrypting/decrypting Email – S/MIME and PGP.

PGP

PGP was developed by Phil Zimmermann in 1991 in response to U.S. Senate Bill 266 which was designed to force manufacturers of secure communications to provide a "back-door" by which the U.S. government would be able to read those communications. The Bill was ultimately defeated, but PGP was born. Version 2 became the standard version of PGP in the early 1990's. While Zimmermann was working on Version 3, the U.S. government laid criminal charges against him, accusing him of "exporting munitions". The government wanted to control the public use of encryption, and declared it a type of "munitions" in order to achieve this control. However, the law controlling encryption export in fact made the export of paper copies of the code legal, which was what Zimmermann had been doing. The charges were eventually dropped.



Step 1: Go to www.hotmail.com and create an email account for yourself. It will redirect you to a login MS passport site. See screen shot below for an example.



Click on the New Account Sign up tab. You will be brought to a screen similar to the one shown below.

Put in your profile info, the registration check info and then Click on the I Agree button at bottom of screen. You will be taken to another screen like the one shown below.



Click on Continue. You will be brought to another screen like the one shown below.



All for only \$19.95 a year!*



No Account Expiration

Sign in to your MSN Hotmail account whenever you want. You'll never have to worry about losing your account, regardless of how often you sign in.



Send/Receive Large Attachments

Generous size limits for sending or receiving photos & files - up to 3 times more per e-mail.



Virus Scanning

To keep your account and PC safe, Hotmail scans all attachments using technology from McAfee.



Hotmail 10MB Inbox

With 10MB Inbox you'll have plenty of room for e-mail, photos, etc. Plus you can send/receive attachments as large as 3MB.



Extra Groups Storage

You'll get 30MB of storage on MSN Groups- the perfect way to store and share photos, files, etc.*

Buy Now

Or, sign up for [FREE E-mail](#) (with a 2MB storage limit and without the other features).

*Annual fee plus applicable taxes. To take advantage of the MSN Groups Extra Storage offer you need an e-mail address ending with '@hotmail.com' or '@msn.com'. MSN Extra Storage is only available via a yearly subscription.

© 2004 Microsoft Corporation. All rights reserved. [TERMS OF USE](#) [Advertise](#) [TRUSTe Approved Privacy Statement](#) [GetNetWise](#) [Anti-Spam Policy](#)

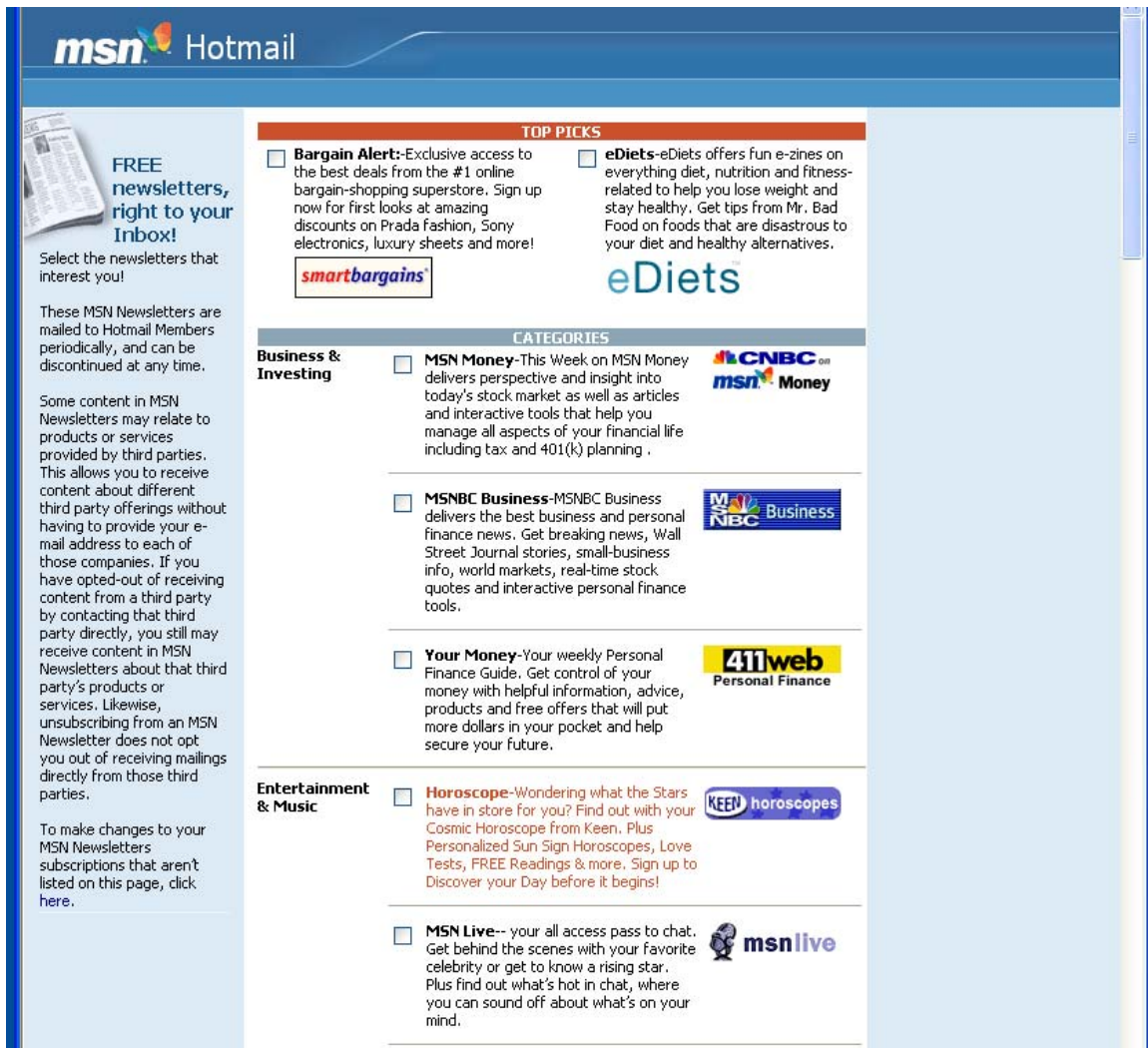
Click on the [Free E-mail](#) link.



CSSIA



You will be brought to a screen like the one shown below. (This is only a partial screen shot).



At the very bottom of the screen, click on the Continue button.

You will be brought to another screen like the one shown below.

msn Hotmail

Featured Offers, right to your Inbox!

MSN Hotmail continuously searches for special discounts with select merchants, then notifies Hotmail members who have indicated an interest in related topics.

These MSN Featured Offers are mailed to Hotmail Members periodically, and can be discontinued at any time.

Some content in MSN Featured Offers may relate to products or services provided by third parties. This allows you to receive content about different third party offerings without having to provide your e-mail address to each of those companies. If you have opted-out of receiving content from a third party by contacting that third party directly, you still may receive content in MSN Featured Offers about that third party's products or services. Likewise, unsubscribing from an MSN Featured Offer does not opt you out of receiving mailings directly from those third parties.

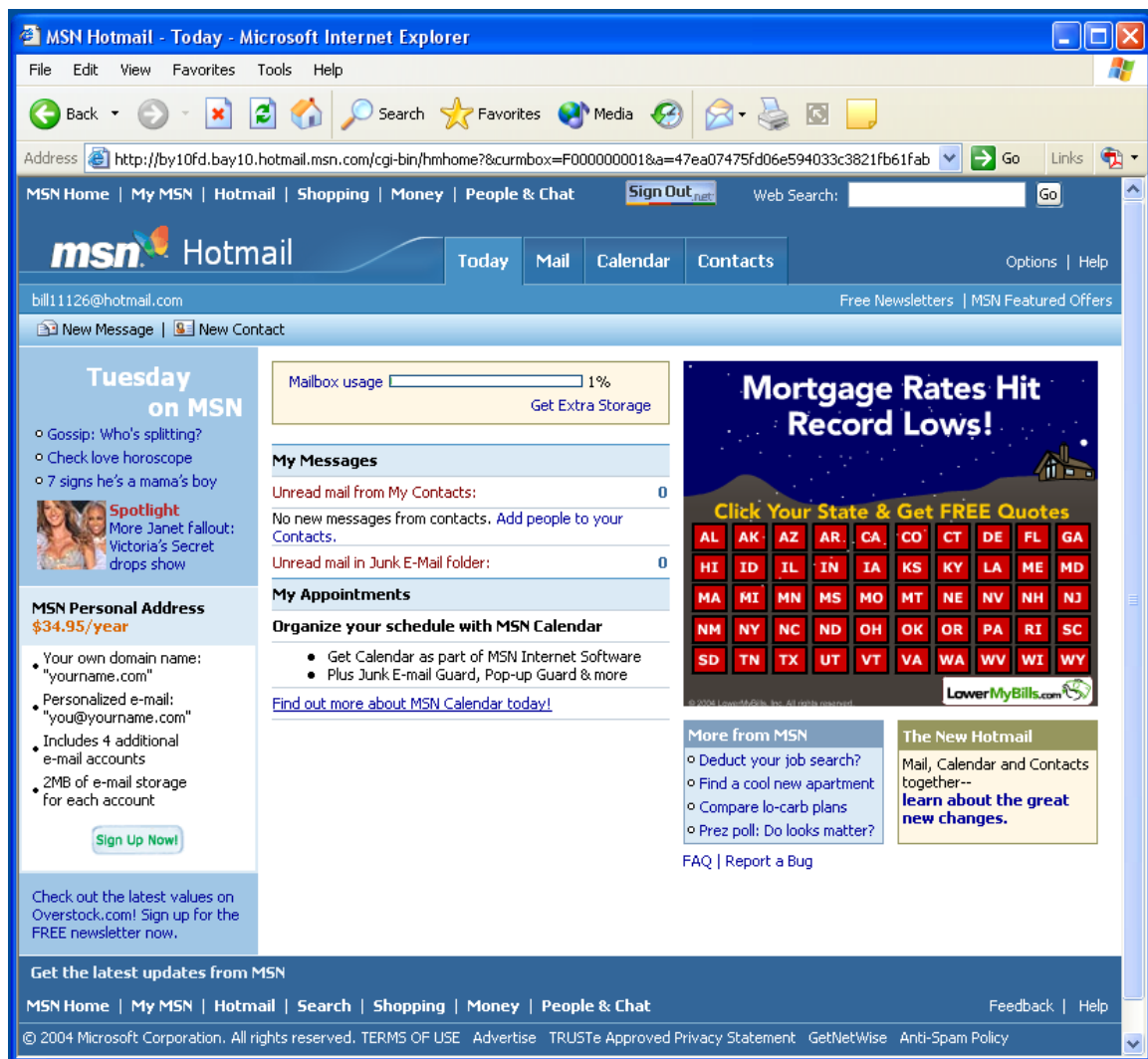
Select the topics that interest you!

<input type="checkbox"/> Apparel & Accessories	<input type="checkbox"/> Teen Apparel <input type="checkbox"/> Men's Apparel <input type="checkbox"/> Children's Apparel <input type="checkbox"/> Jewelry & Watches	<input type="checkbox"/> Women's Apparel <input type="checkbox"/> Fitness Apparel <input type="checkbox"/> Lingerie <input type="checkbox"/> Luxury & Designer
<input type="checkbox"/> Entertainment	<input type="checkbox"/> New Music & Video Releases <input type="checkbox"/> Video Games <input type="checkbox"/> CDs <input type="checkbox"/> Home Theater & Stereo	<input type="checkbox"/> Books & Magazines <input type="checkbox"/> Travel <input type="checkbox"/> DVDs <input type="checkbox"/> Romance & Relationships
<input type="checkbox"/> Home & Family	<input type="checkbox"/> Home Improvement & Gardening <input type="checkbox"/> Pets <input type="checkbox"/> Health & Wellness <input type="checkbox"/> Automotive <input type="checkbox"/> Baby & Maternity	<input type="checkbox"/> Furniture & Furnishings <input type="checkbox"/> Bath & Beauty <input type="checkbox"/> Prescription Savings <input type="checkbox"/> Kitchen
<input type="checkbox"/> Money & Business	<input type="checkbox"/> Banking & Bill Pay <input type="checkbox"/> Investing & Brokerage <input type="checkbox"/> Insurance <input type="checkbox"/> Careers	<input type="checkbox"/> Credit Cards <input type="checkbox"/> Mortgages & Loans <input type="checkbox"/> Small Business
<input type="checkbox"/> Shopping	<input type="checkbox"/> Bargains & Clearance <input type="checkbox"/> Coupons <input type="checkbox"/> Flowers <input type="checkbox"/> Gifts & Gourmet <input type="checkbox"/> Local Shopping	<input type="checkbox"/> Sweepstakes & Free Stuff <input type="checkbox"/> Sports & Recreation <input type="checkbox"/> Games & Toys <input type="checkbox"/> Hobbies & Collectibles
<input type="checkbox"/> Tech & Gadgets	<input type="checkbox"/> Computer Software <input type="checkbox"/> Internet & Broadband <input type="checkbox"/> Telecommunications	<input type="checkbox"/> Hardware & Devices <input type="checkbox"/> Photography (Digital & more) <input type="checkbox"/> Wireless Devices

[Continue](#)

Click on the Continue button.

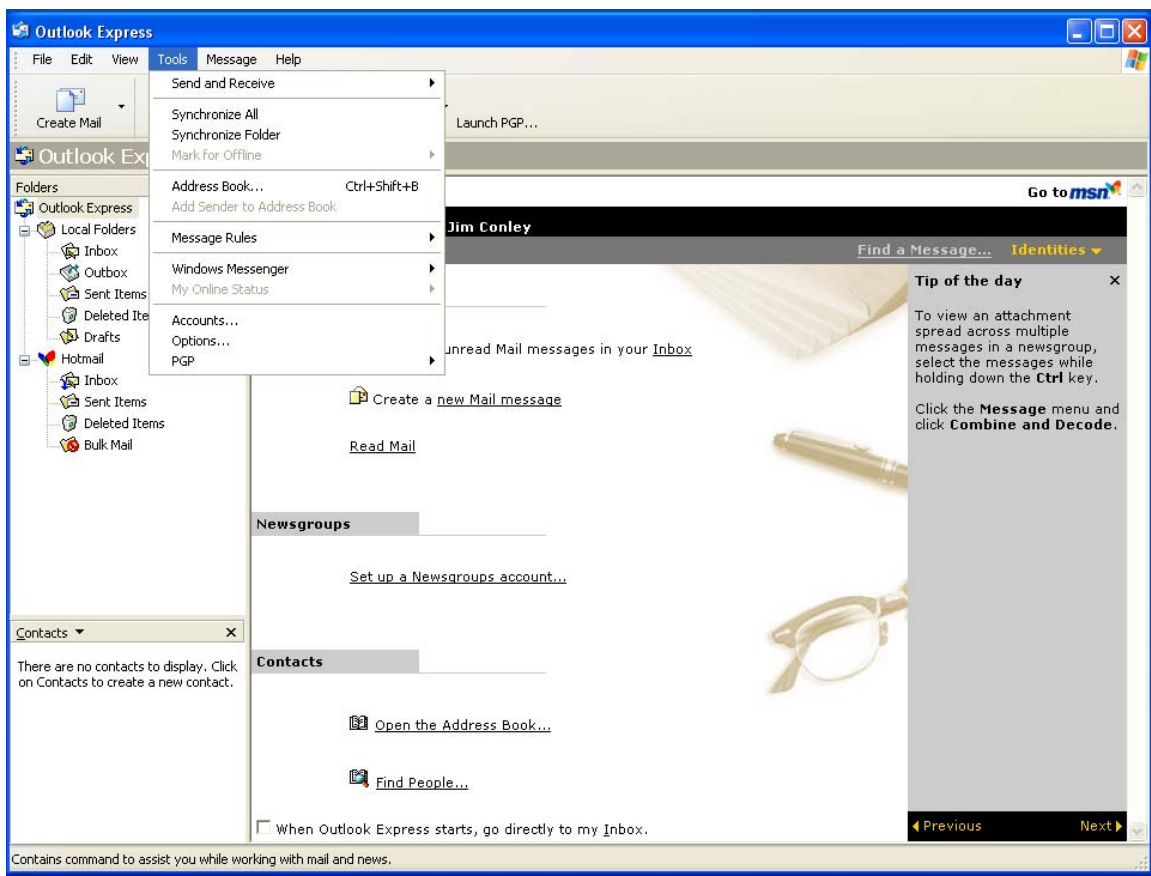
You will be brought to a screen like the one shown below.

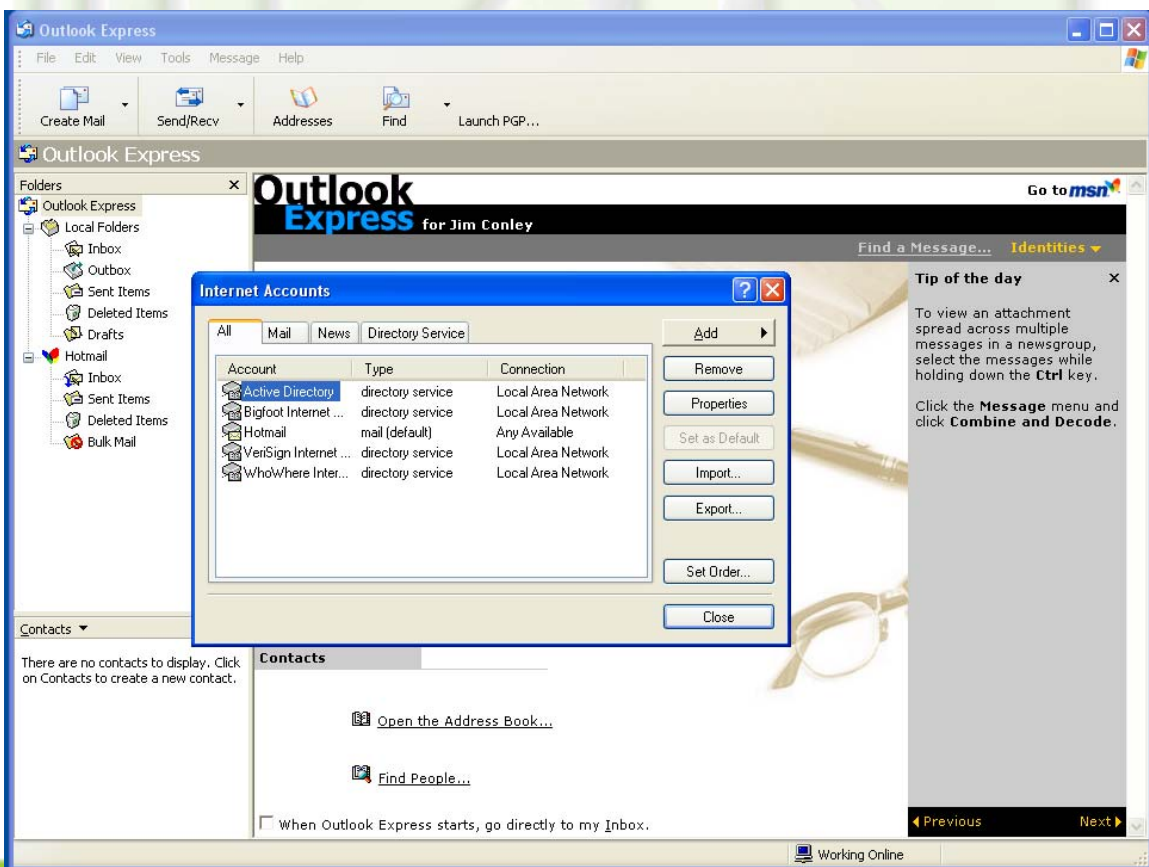


To check your mail, click on the Mail tab. This is where we will be doing our work. Congratulations, you now have a Hotmail account! You can close this window now.

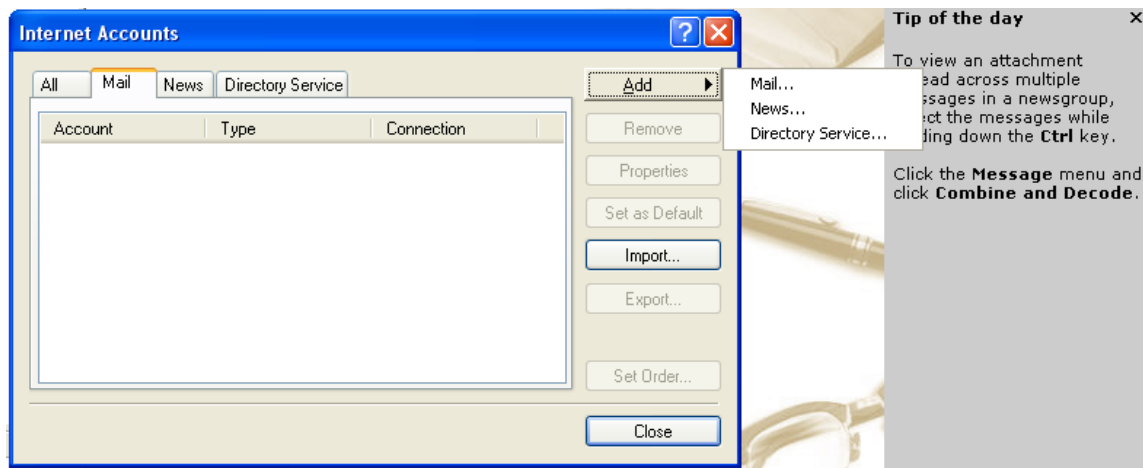
Step 2:

You now need to add this Hotmail account to Outlook Express. Launch Outlook Express from your computer. Click on **Tools** from the menu bar and select **Accounts**. See below for some screen shots of this.





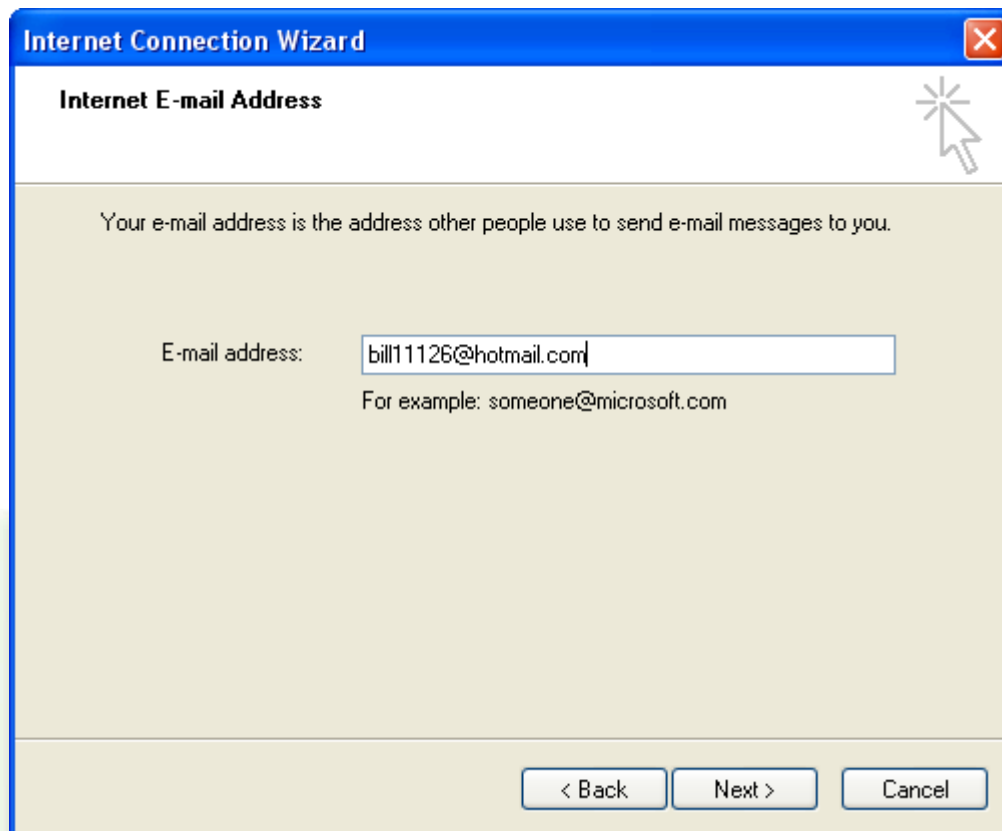
Click the **Mail** tab, then click **Add** button and select **Mail**. See a sample screen shot of this below.



After clicking on **Mail**, you will see a screen like the one below.

The screenshot shows the 'Internet Connection Wizard' window. The title bar says 'Internet Connection Wizard'. The main heading is 'Your Name'. Below it, there is a text box for 'Display name:' with a cursor inside. Below the text box, it says 'For example: John Smith'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

Enter your name and click **Next**. You will be brought to a screen like the one shown below.



The image shows a Windows XP-style dialog box titled "Internet Connection Wizard". The subtitle is "Internet E-mail Address". The main text reads: "Your e-mail address is the address other people use to send e-mail messages to you." Below this, there is a label "E-mail address:" followed by a text input field containing "bill11126@hotmail.com". Underneath the input field, it says "For example: someone@microsoft.com". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel". A mouse cursor is pointing at the "Next >" button.

Internet Connection Wizard

Internet E-mail Address


Your e-mail address is the address other people use to send e-mail messages to you.


E-mail address:


For example: someone@microsoft.com


< Back Next > Cancel

Enter your Hotmail account email address and click **Next**. You will then see a screen like the one shown below.

Internet Connection Wizard 

E-mail Server Names 

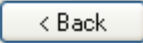


My incoming mail server is a **HTTP**  server.

My HTTP mail service provider is **Hotmail** 

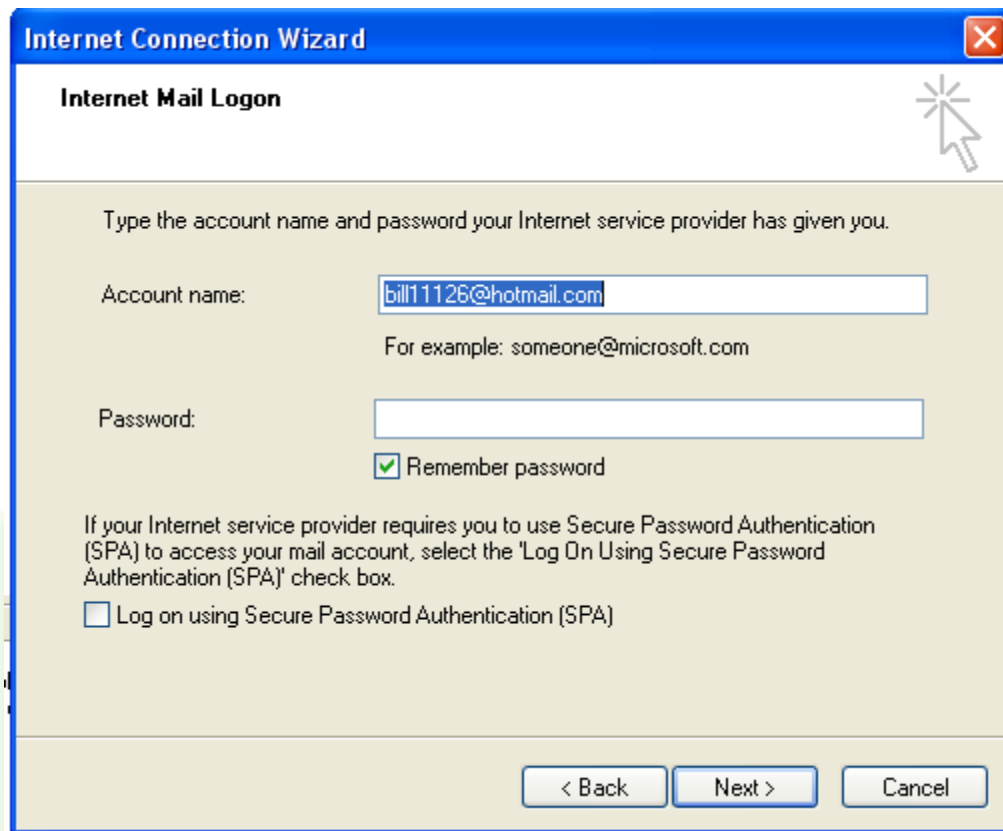
Incoming mail (POP3, IMAP or HTTP) server:

An SMTP server is the server that is used for your outgoing e-mail.

Outgoing mail (SMTP) server:

Select **HTTP Server** and select **Hotmail** as your HTTP mail service provider, then click **Next**. You will then see a screen like the one shown below.



The screenshot shows a Windows XP-style dialog box titled "Internet Connection Wizard" with a sub-header "Internet Mail Logon". The main text says "Type the account name and password your Internet service provider has given you." There are two input fields: "Account name:" with the text "bill11126@hotmail.com" and a hint "For example: someone@microsoft.com", and "Password:" which is empty. Below the password field is a checked checkbox labeled "Remember password". Further down, there is explanatory text about Secure Password Authentication (SPA) and an unchecked checkbox labeled "Log on using Secure Password Authentication (SPA)". At the bottom right are three buttons: "< Back", "Next >", and "Cancel". A mouse cursor is pointing at the top right corner of the dialog box.

Verify that your Hotmail account name is correct, then enter your password that you created when setting up your Hotmail account. Make sure the **Log on using Secure Password Authentication (SPA)** is checked.

Click on **Finish**.

Click Yes when Outlook Express asks you if you wish to download Folders from the Mail server.

Congratulations! You have successfully added your Hotmail account to Outlook Express. Close Outlook Express.



Step 3:

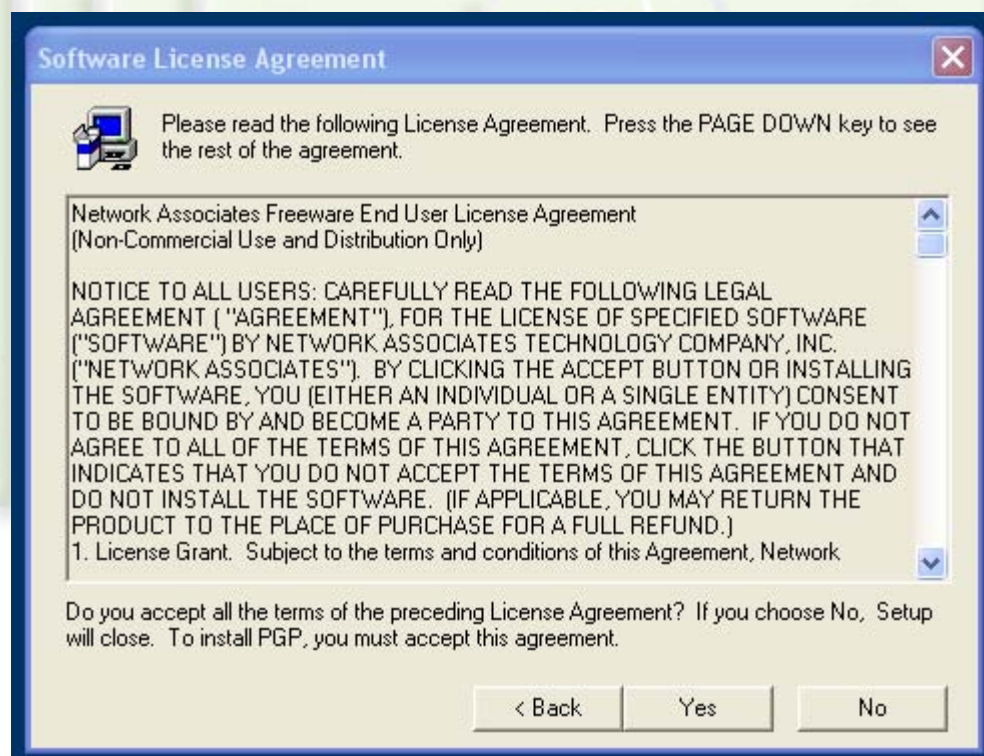
We now need to download PGP if your instructor has not already put this on your computer. Ask your instructor. For this lab, we will assume that PGP is not yet installed on the computers.

Download the PGP 6.5.8 version zip file and save to C:\PGP on your hard drive. To do this, right-click the file attachment, click Save Attachment, Create a new folder on C:\ and call it PGP.

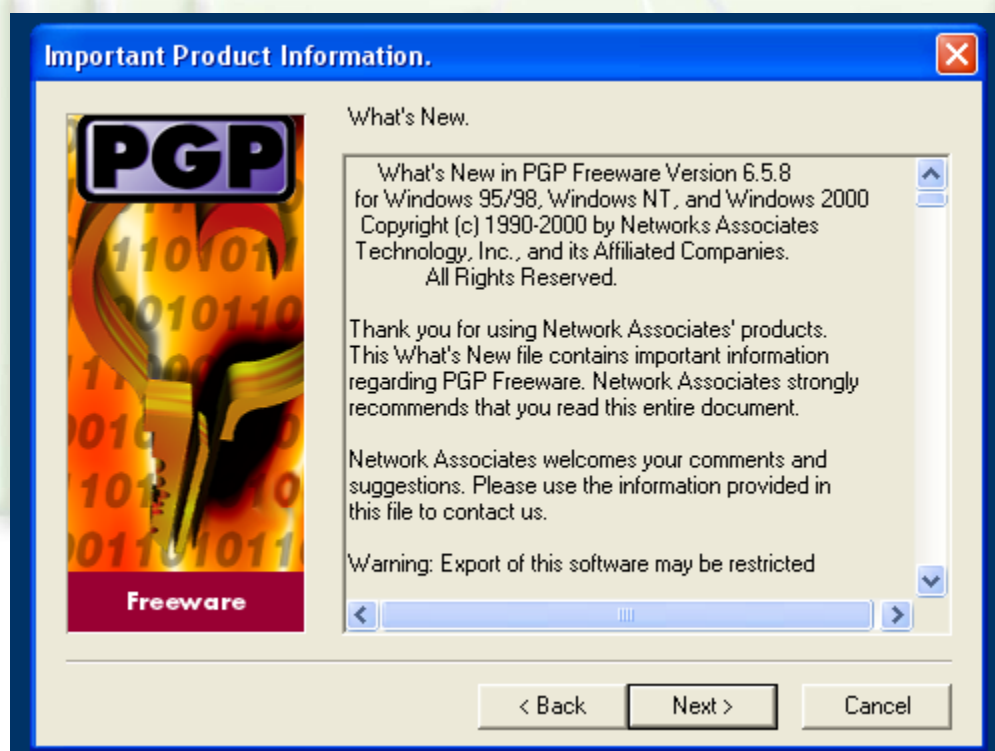
Once the zip file is on your hard drive, unzip to the same PGP directory. Double-click the setup file to install. You will see a screen like the one shown below.



Click Next. You will see a screen like the one shown below.

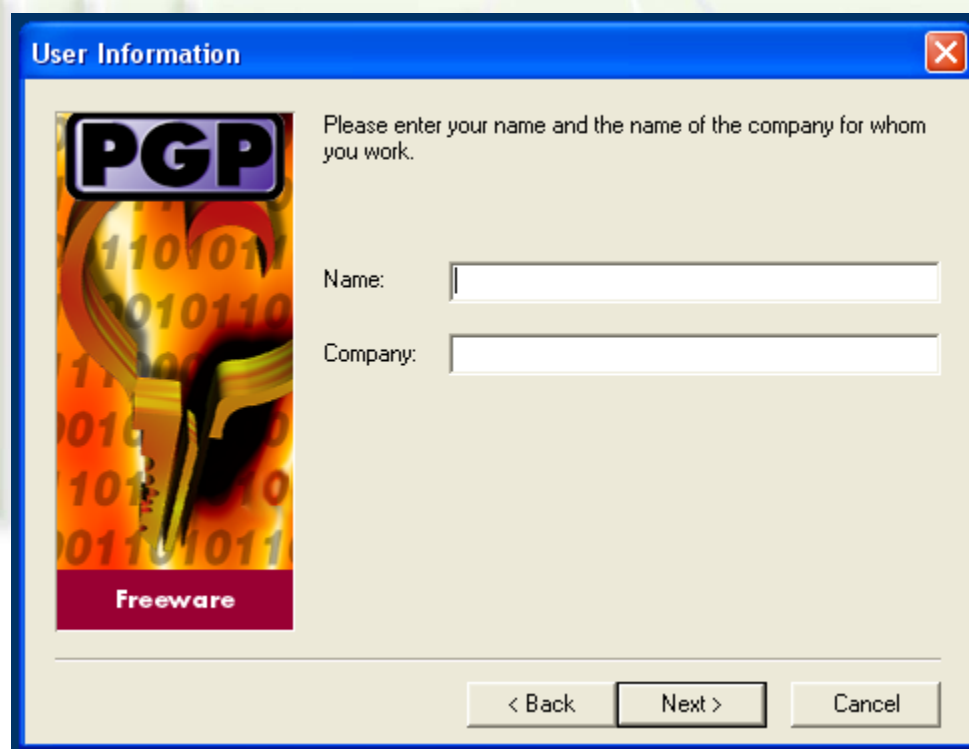


Click Yes. You will be brought to a screen like the one shown below.



Click Next. Your next screen will look like the one below.





The image shows a Windows-style dialog box titled "User Information" with a blue header bar and a red close button in the top right corner. On the left side of the dialog is a vertical banner for "PGP Freeware". The banner features the "PGP" logo in a black box at the top, followed by a graphic of a golden key against a background of binary code (0s and 1s) in orange and yellow. At the bottom of the banner is a red bar with the word "Freeware" in white. To the right of the banner, the text "Please enter your name and the name of the company for whom you work." is displayed. Below this text are two text input fields: the first is labeled "Name:" and the second is labeled "Company:". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

User Information

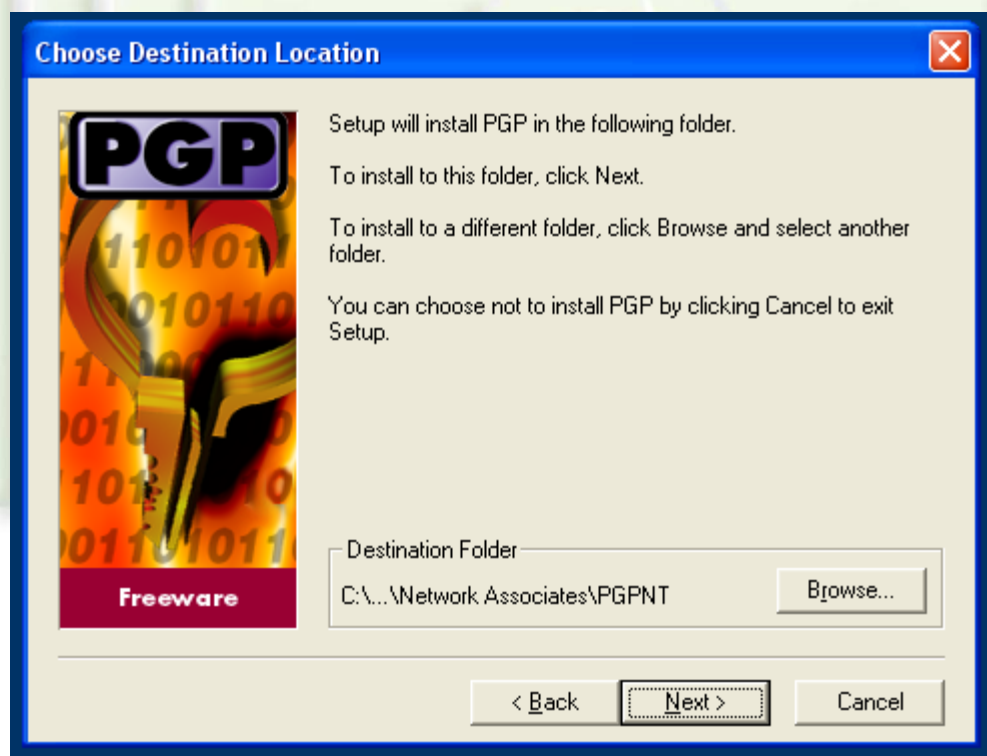
Please enter your name and the name of the company for whom you work.

Name:

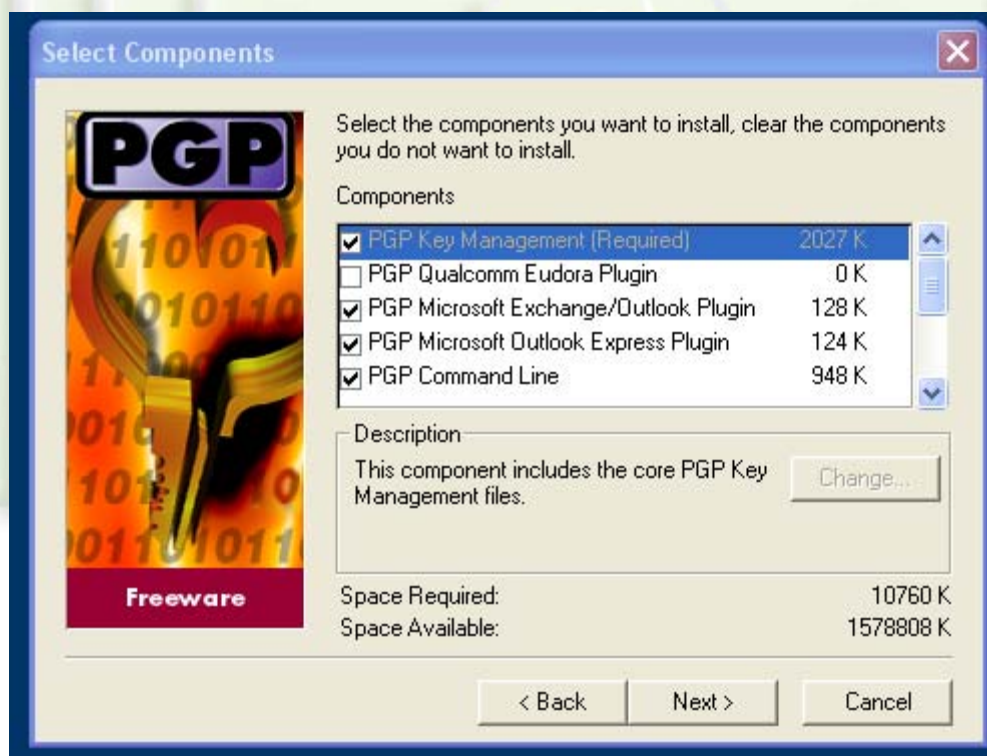
Company:

< Back Next > Cancel

Fill in your name and school name and then click Next. The next screen will look like the one below.

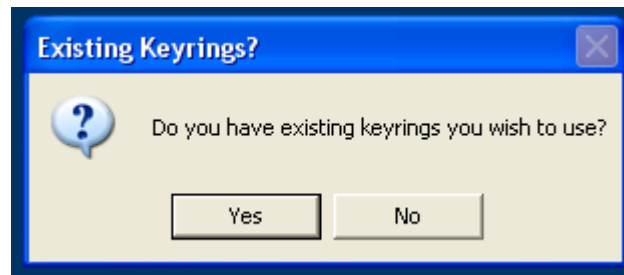


Click Next to continue. You will see a screen like the one below.

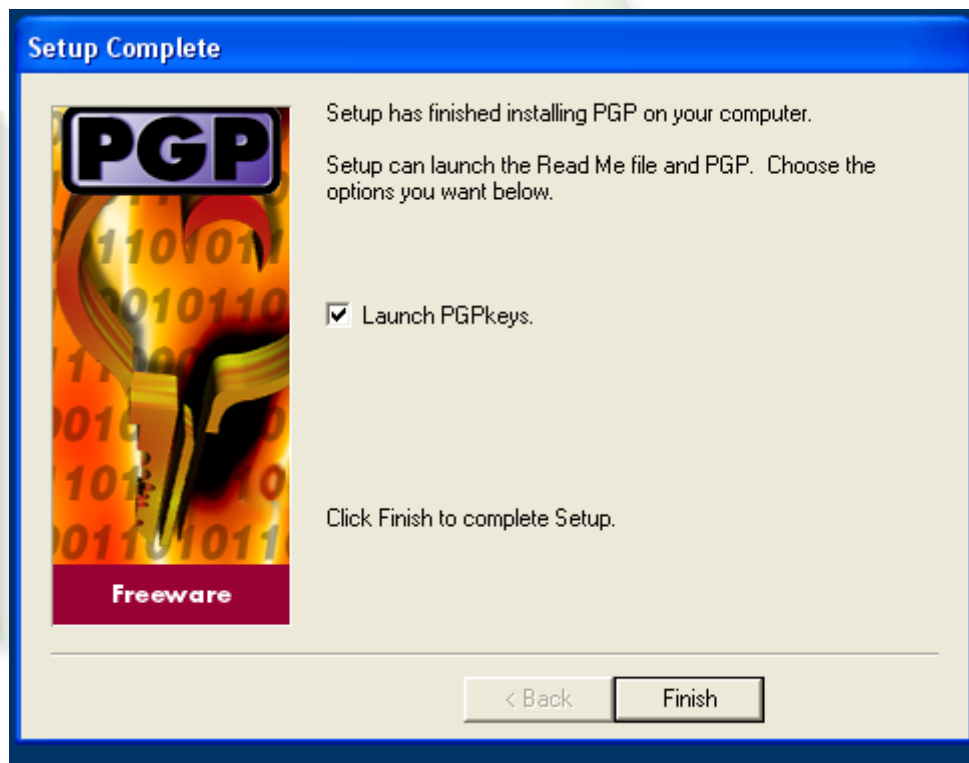


Make sure Outlook Express Plugin box is checked. Click Next to continue. It will bring you to another screen with all of your setup information. Click Next to continue.

It will then install the software. After software installation is complete, it will ask you if you have any existing keyrings. See screen below.



Say NO to existing keyrings!!! It will then bring you to a screen like the one below.

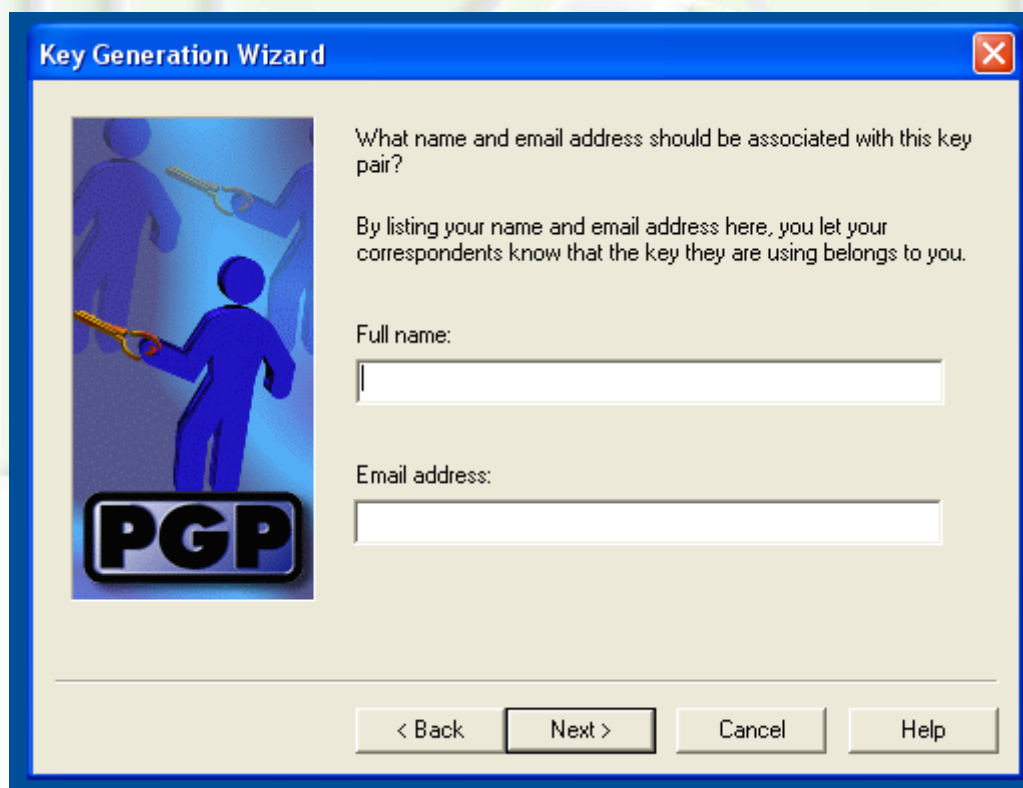


Make sure the Launch PGPkeys is checked and click Finish.

It will now go into the PGP key generation wizard. See screen shot below.



Click Next to continue. It will bring you to a screen like the one below.



The image shows a 'Key Generation Wizard' dialog box with a blue title bar and a close button. On the left is a graphic of two stylized figures exchanging keys, with a 'PGP' logo below. The main text asks for a name and email address for the key pair. Below this are two input fields: 'Full name:' and 'Email address:'. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

Key Generation Wizard

What name and email address should be associated with this key pair?

By listing your name and email address here, you let your correspondents know that the key they are using belongs to you.

Full name:

Email address:

< Back Next > Cancel Help

Put in your name and your hotmail email account and click Next.

Pick Diffie-Hellman/DSS for Key Pair Type and then Click Next.

Use the default of 2048 bits (2048 Diffie-Hellman/1024 DSS) and click Next.

Click on Radio button for Key pair expires. Use default date of 1 year. Click on Next. You will see a screenshot like the one below.

The image shows a 'Key Generation Wizard' dialog box. On the left is a graphic of a person holding a key with a 'PGP' logo below it. The main text area contains instructions: 'Your private key will be protected by a passphrase. It is important that you do not write this passphrase down.' and 'Your passphrase should be at least 8 characters long and should contain non-alphabetic characters.' Below this is a 'Passphrase:' label, a text input field, and a checked 'Hide Typing' checkbox. Underneath is a 'Passphrase Quality' progress bar. Then there is a 'Confirmation:' label and another text input field. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

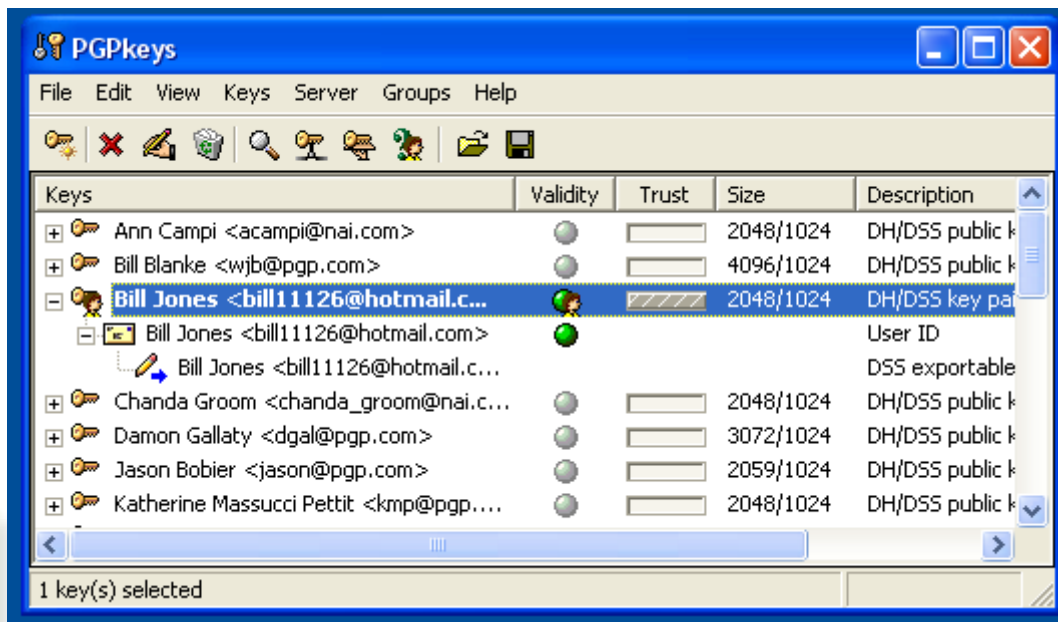
Put in a passphrase! You have to type it in again in the Confirmation: box. Remember this passphrase!!!!!! Click on Next to continue.

It will then generate your keypair. Once it is completed, click on Next to continue. You will then see a screen like the one below.



Check box so that you send the key to root server and then click Next. It will connect to root server and upload your keys. Once this is complete click on Next to continue.

Click on Finish. It should then close the key generation window and open up a new window similar to the one shown below.



Close this box by clicking on the X at top right-hand corner. It will bring up a screen like the one shown below.



Click on Don't Save.

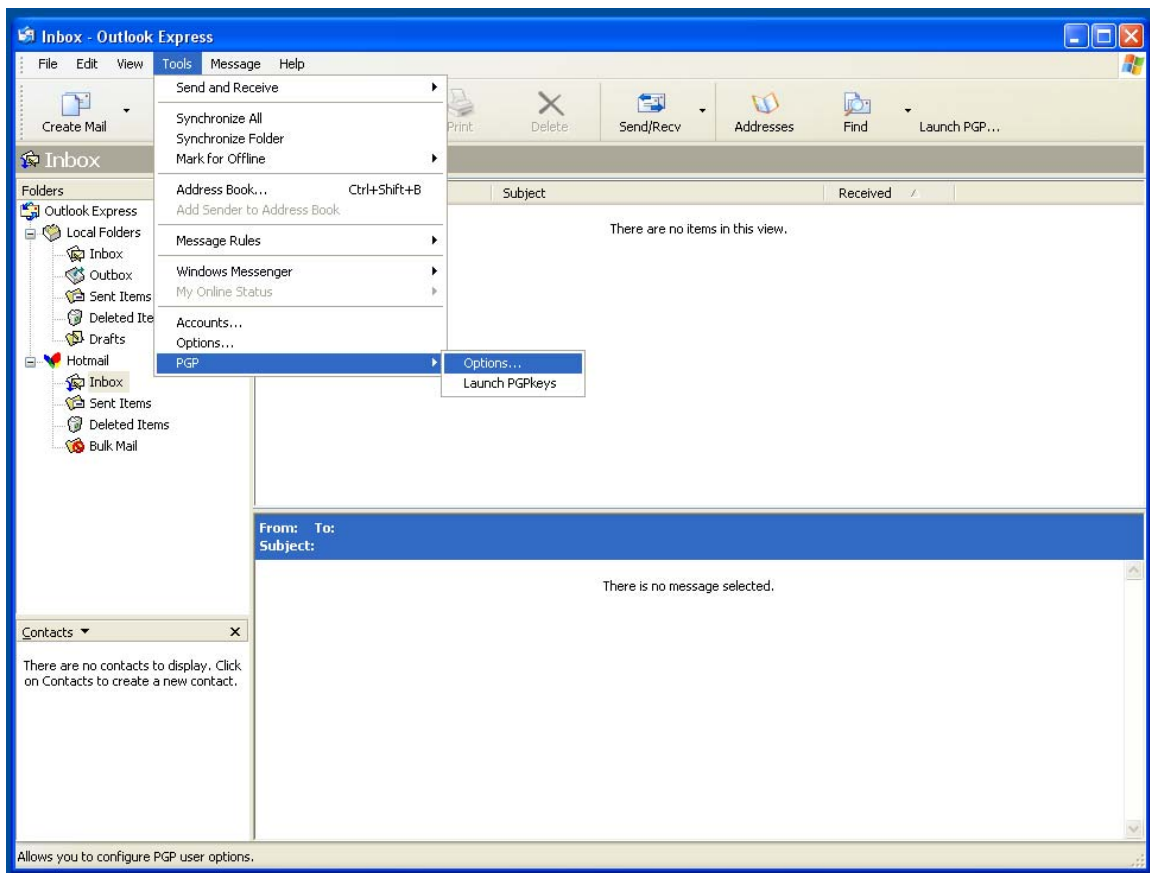
Congratulations. You have now installed PGP.

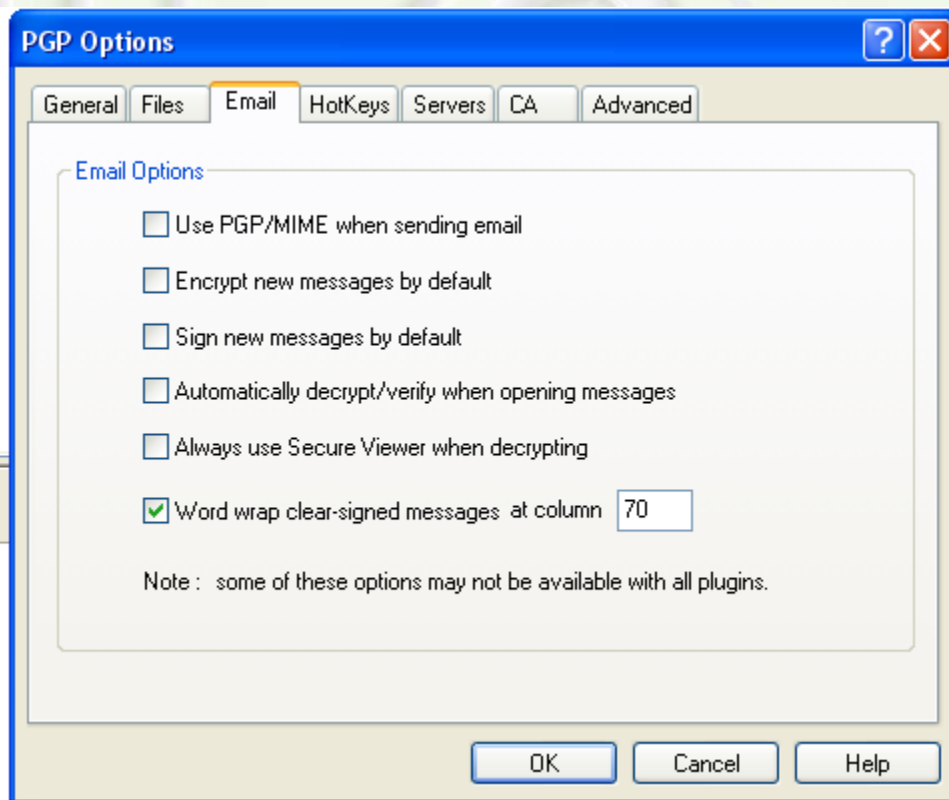
Step 4: Reboot your machine!!!!!!

Step 5:

We will now let MS Outlook Express know about PGP and that you wish to encrypt your messages by default. Launch Outlook Express.

Click on **Tools, PGP, Options**. You will see screens similar to the ones shown below.





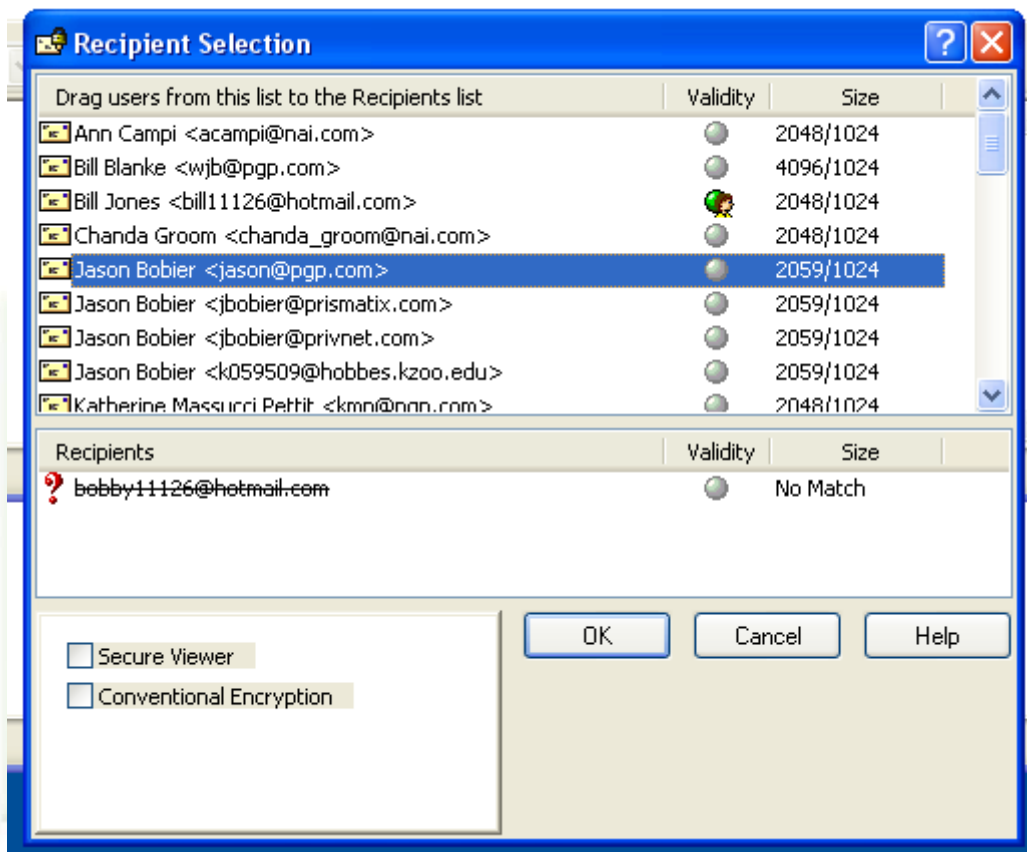
Make sure the Email tab is selected. Check the *Encrypt new*

messages by default and the *Sign new messages by default*.

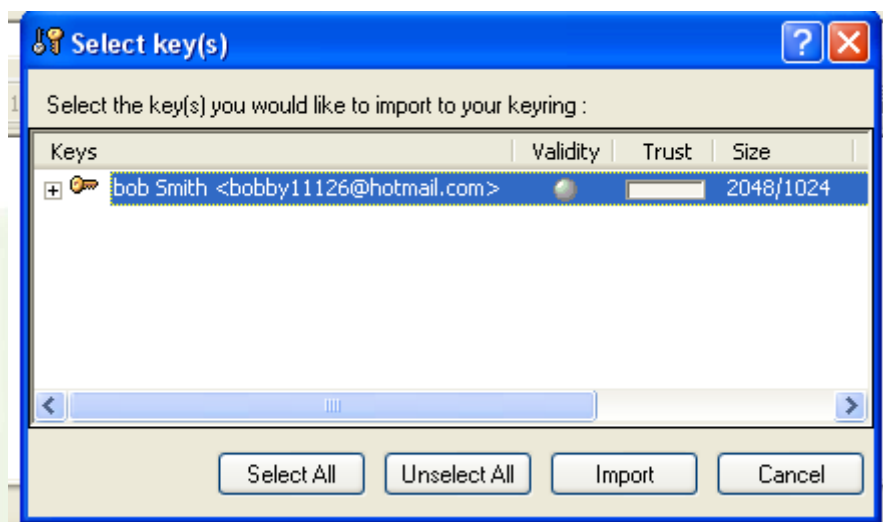
Click OK.

You are now ready to send an email message to your instructor.

Create a new message to your instructor. Click on send. You should get a screen similar to the one shown below.

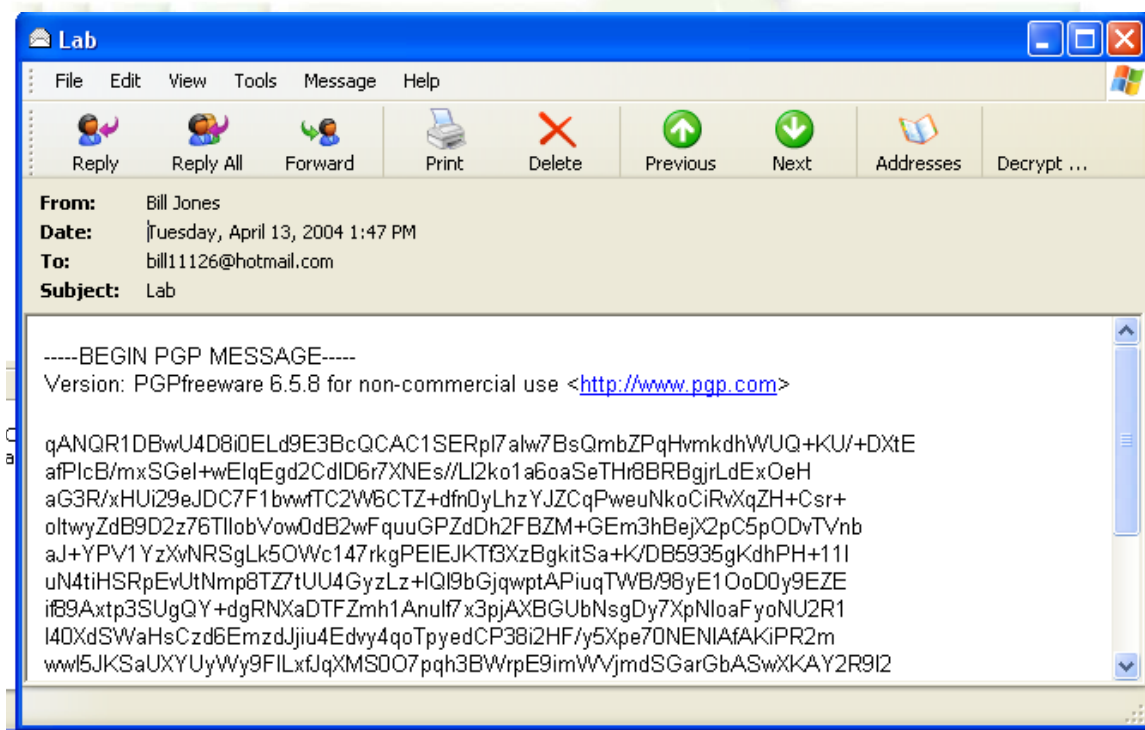


You need to get keys from this user (Jason Bobier is just an example. Use your instructor's name). Right click on the recipient with the question mark and choose Update from Server. Click OK. You will get a screen like the one shown below.



Click on import. You will be prompted for your passphrase. Type it in the box. It will then encrypt your message.

Your instructor will reply to your message. It will be encrypted. See screen below for sample.



Click on the decrypt button. You will be prompted for *your* passphrase. Type it in and message will decrypt.

Step 6: Analysis

- 1) What kinds of business applications would you use this tool for?
- 2) After working with PGP, what do you feel you should study further? Why?
- 3) Why should you use something like PGP with your email?



Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

Research software with similar functionality

Research S/MIME

Research History of PGP and Phil Zimmerman

Appendix:

This lab was developed using PGP version 6.5.8. PGP may be obtained from,

www.pgpi.org

Version 8 of PGP is now available.

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).

