Pretty Good Privacy (PGP) Laboratory – Module 6 Cryptography

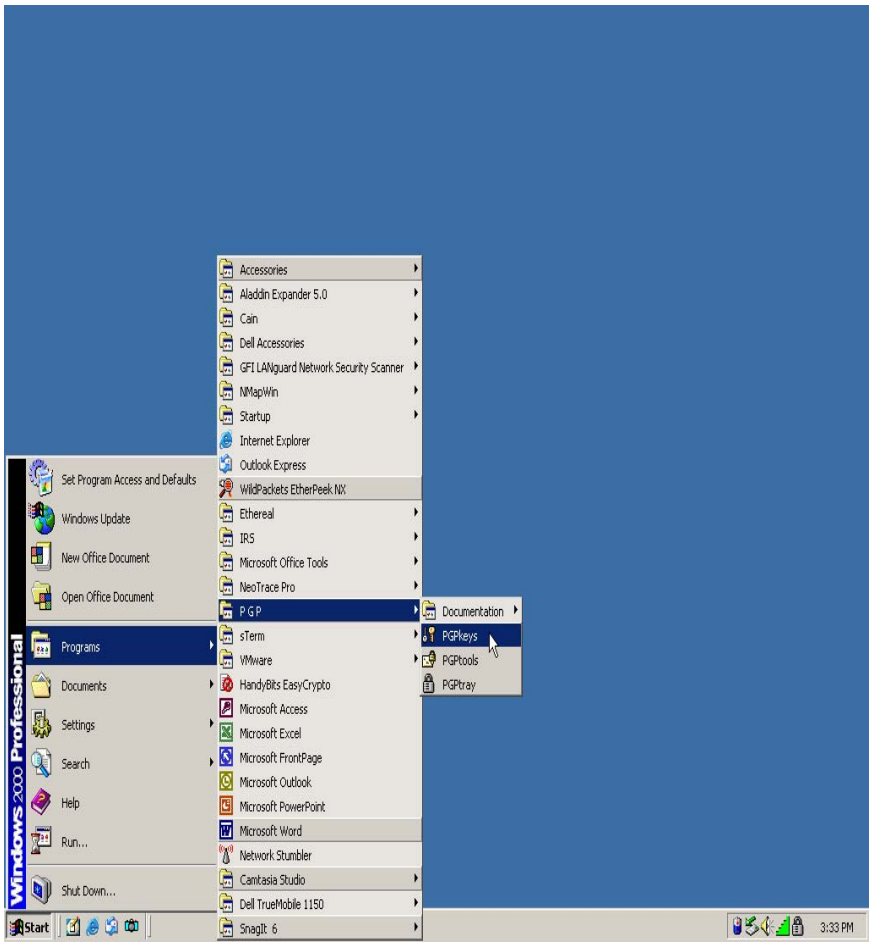
Background: This Lab reinforces the concepts of public key cryptography and encryption as detailed in the lecture. PGP is a tool originally authored by Phil Zimmerman that allows data to be encrypted, distributed, and decrypted securely.

Requirements/assumptions:

- **Windows NT 4.0/2000**
- **Local Administrative privileges**
- **PGP version 6.58 (available at http://web.mit.edu/network/pgp.html). This is the last open source version available and is therefore preferred.**
- **Students must be split into pairs (partners) for portions of this Lab**

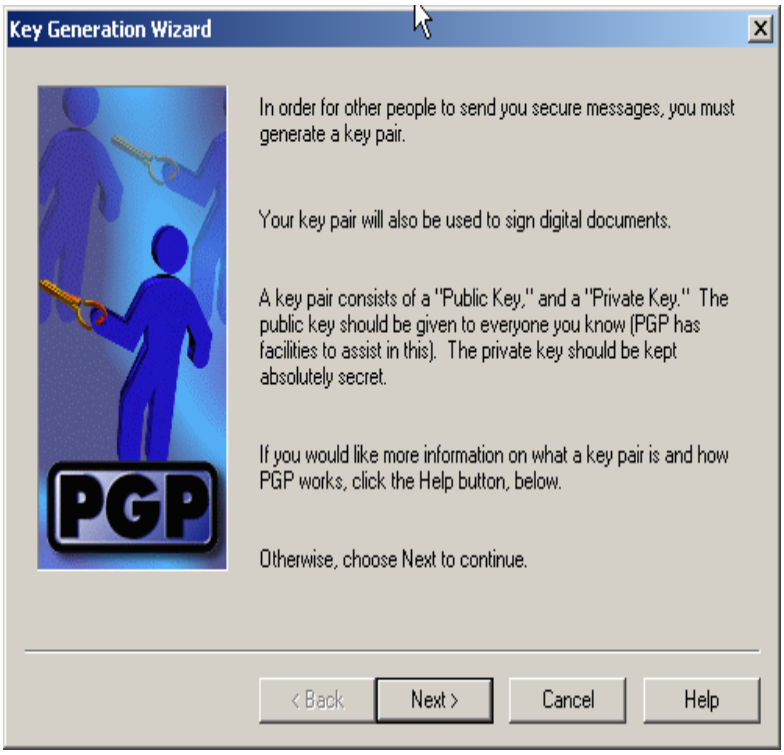
Exercise 1 – Create a public/private key pair in PGP

1. Using an ISFTS Student Laptop Computer, power on the computer. During start-up you will be presented with a window to choose an Operating System, select "Windows 2000". The loading process for Windows 2000 may take several minutes. Once Windows 2000 has completely loaded a desktop login window interface will appear requesting a Username: "Administrator" and Password: "tartans".



2. Once log-on is complete, a Windows 2000 Desktop interface will appear. In order to begin utilizing PGP, you must first launch the program. You will need to click on the "Start" button once; then click once on the "Program Folder"; and click on the "PGP Folder". At this point you should double click on the "PGP Key" Icon.

3. At this point you should see the Key Generation Wizard. If you do not see this window but rather a “PGP Keys” window, you must click on the “Keys” drop-down menu and select “New Keys” to arrive at the Key Generation Wizard. Start the Key Generation Wizard by clicking the “Next” button.



4. The next window in the Key Generation Wizard will require a “Full Name” [use your computer’s hostname, this should be something close to isftsstudent1---see label on display lid of your computer] and an “Email Address” [use your computer’s hostname@192.168.30.19 (i.e. isftsstudent@192.168.30.19). After providing this information proceed to the next window.

   NOTE: Be careful not to make a typo when completing Step 4, as this may cause the PGP email exercise to fail.

5. The Key Generation Wizard will now ask for you to select a “Key Pair Type”. You will need to select “Diffie-Hellman”. After selecting the correct “Key Pair Type” proceed to the next window.

6. Now the Key Generation Wizard will ask you to select the “Key Pair Size”. The default setting is 2048 bits. This default setting is fine. All that you need to do is click “Next” and proceed on to the “Key Expiration” window.

7. At this point the Key Generation Wizard will require you to select a “Key Expiration”. The default setting should be “Key pair never expires”. Ensure this setting is correct and then proceed to the next window.

8. Next the Key Generation Wizard requires you to enter a passphrase to protect your private key. Enter a passphrase that you can easily remember in both the “Passphrase” and “Confirmation” boxes. [The passphrase must be at least eight character in length] Once you have provided the passphrase click “Next”. PGP will now create your key pair.

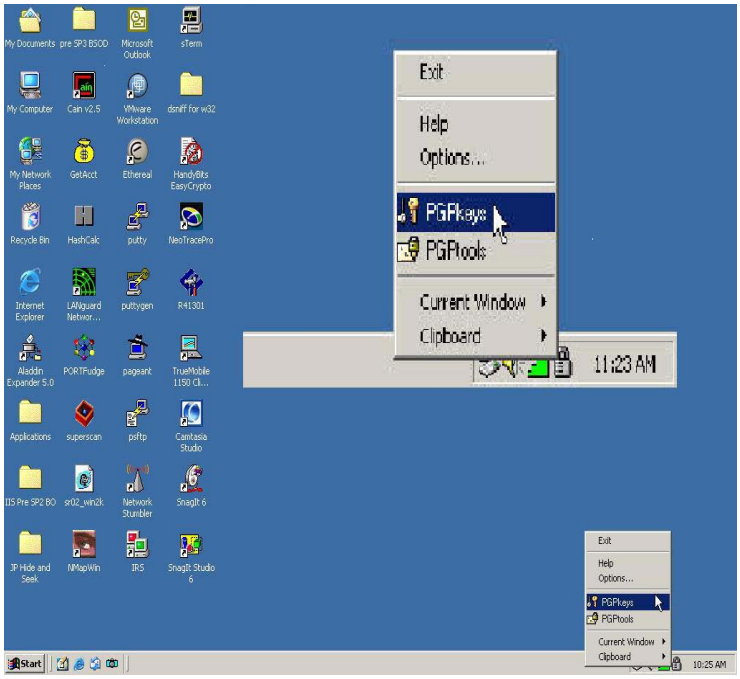
9. Once the key pair is created, the next Key Generation Wizard window will prompt you send your newly created key pair to a root server. **Do NOT** send the key to the root server. Make sure the box is unchecked then click next.

10. This is the last window in the Key Generation Wizard. Click Finish to complete the Key Generation Wizard.

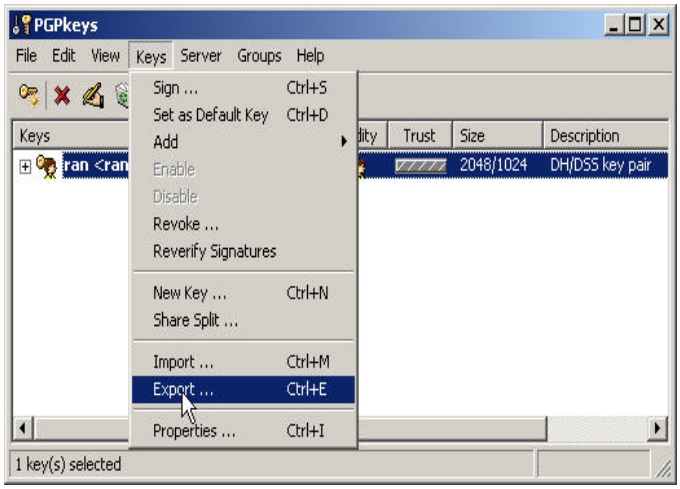
Exercise 2 – Create revocation key

A revocation key is used for revoking keys (typically stored on public Internet key servers) when a passphrase has been forgotten or the key pair has been lost. It is recommended that this revoking key (and any backup of your actual key pair) be stored on a floppy disk and kept in an alternate/safe location.

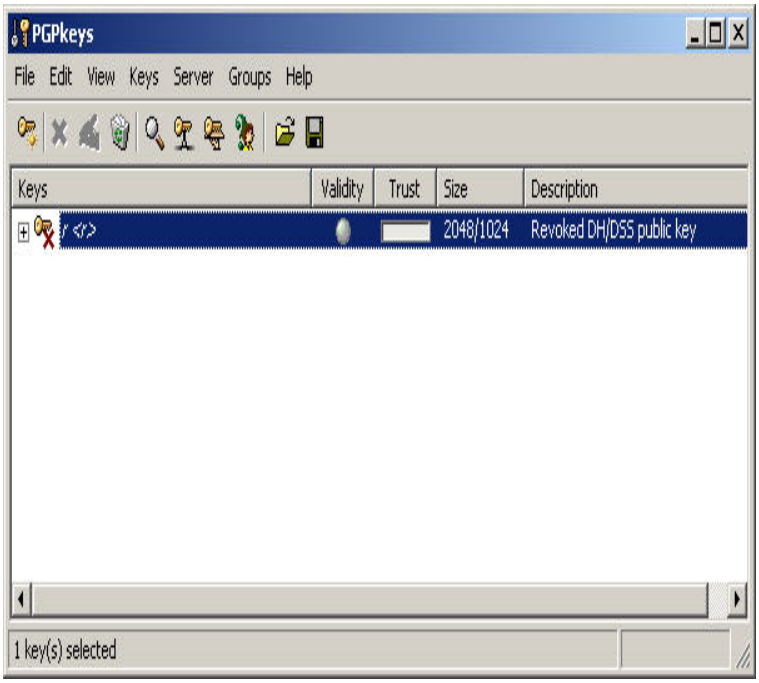
1. To begin using PGP you must right click on the "Pad Lock" icon located in the lower right side of the task bar, and then select the "PGPkeys" option. This will launch a PGPkeys window. If the "Pad Lock" icon is not located in the lower right side of the task bar, you will need to click on the "Start" button on the lower left side of the task bar and select the "Programs" folder. Now locate the "PGP" folder and click once more. At this point you will see four choices: (1) PGPkeys; (2) PGPtools; (3) PGPtray; and (4) Documentation. Select the "PGPkeys" option. This will launch the PGPkeys window.



2. At the "PGPKeys" window you should see the PGP Key Pair you just created in Exercise #1. You will need to click on your newly created PGPkey; this will highlight and select your newly created PGPkey. Once the PGPkey is highlighted, click on "Keys" option in the drop-down menu and choose the "Export" function. PGP is now going to ask for a location to export your PGPkey. In addition to providing a location **(Remember this location, because you will need to revisit this later in the exercise.)** you must be sure to include your "private key(s)". This is accomplished by checking the small box located in the lower right corner of the Export window.

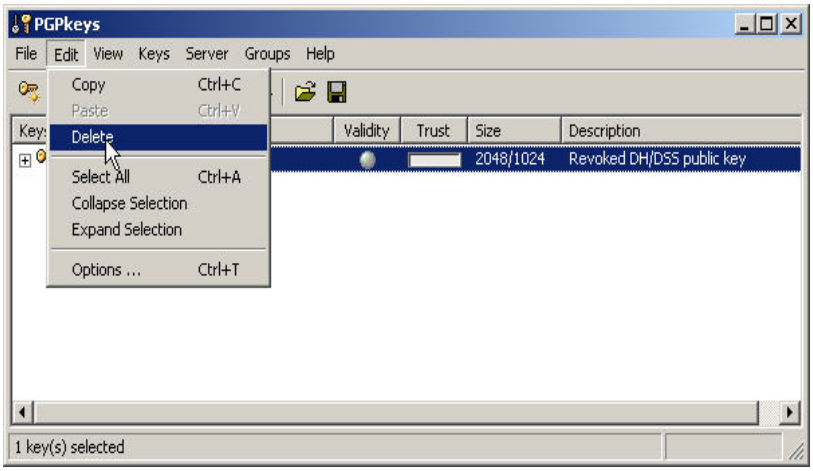


3. Once you have successfully exported you PGP Key Pair (Including your "private key(s)") you must now revoke your PGP Key Pair. To do this you will reselect your PGP Key Pair by clicking on your Key Pair, then click on the "Keys" option in the drop-down menu and choose the "Revoke" function. PGP is now going prompt a warning (read the warning and click "yes" to continue) and ask for the passphrase you created in Exercise #1 while initial creating your PGP Pair Key. After inputting your PGP Passphrase click "Ok" to revoke your PGP Pair Key. You should now see your PGP Pair Key Icon with a red "x" in the PGPkeys window.

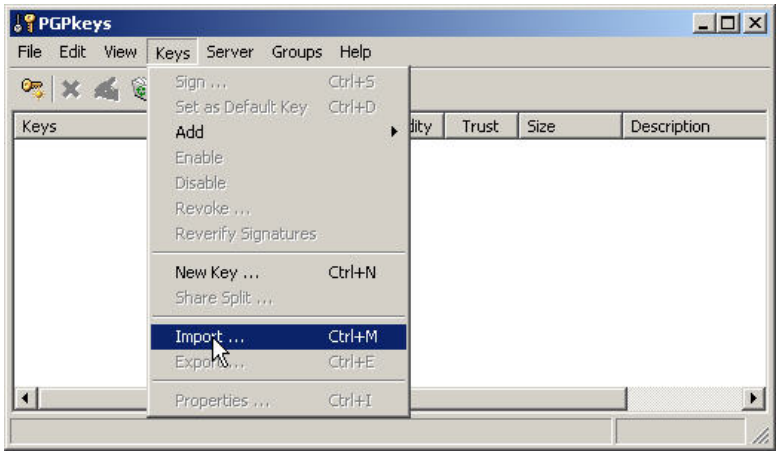


4. Now you must repeat Step #1 only this time exporting your “Revoked” PGP Key Pair. Before exporting and saving the “Revoked PGP Key Pair” make sure to rename the Revoked PGP Key Pair so to distinguish it from the Un-Revoked PGP Key.

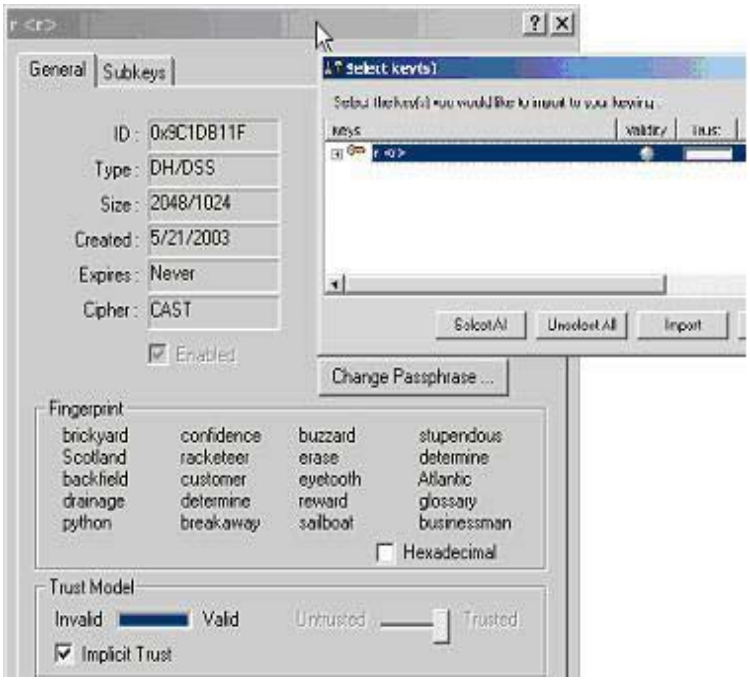
5. The next step is to delete the revoked key pair from the PGPkeys window. At the PGPKeys window you should see the PGP Key Pair you just revoked. You will need to click on your revoked PGPkey; this will highlight and select the revoked PGPkey. Once the revoked PGPkey is highlighted, click on the “Edit” option in the drop-down menu and choose the “Delete” function and click “yes” to delete your revoked PGP Key Pair.



6. Next you will need to import your original PGP Key Pair that was saved prior to revoking. From the PGPkeys window, click on the “Key” option in the drop-down menu and choose the “import” function. You will need to select the location where the original PGP Key Pair was saved; select that file, and click “open”. A second window will appear (Select key(s)) that will list the Key File you just selected. Highlight that file and right click selecting the “key properties” and ensure that the



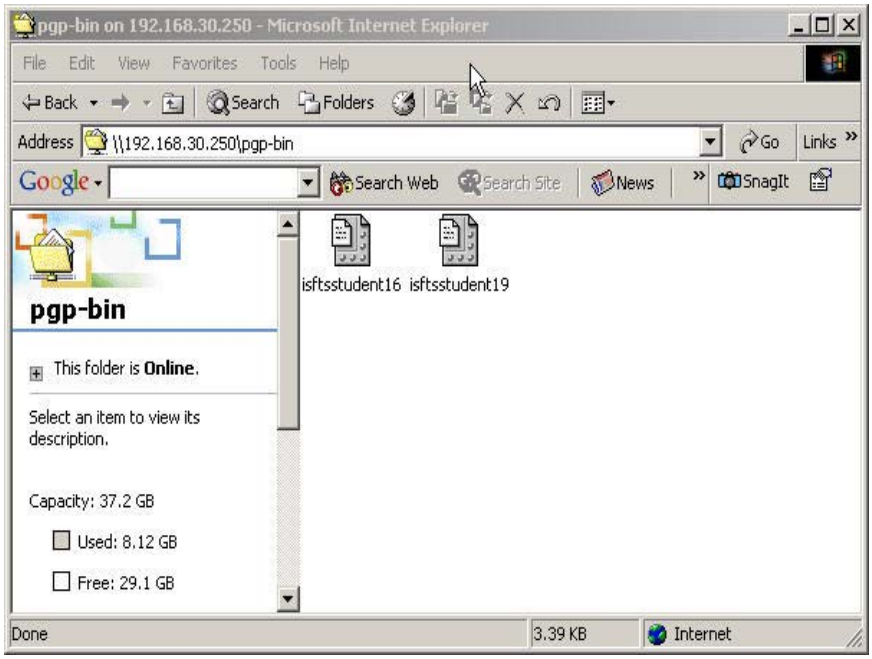
"Implicit Trust" is checked, then click the "import" button. At this point you should see the Imported Key in the PGP Keys window. You now have a current, un-revoked copy of your PGP Key Pair on your Key Ring and a revoked copy of the PGP Key in a safe place.



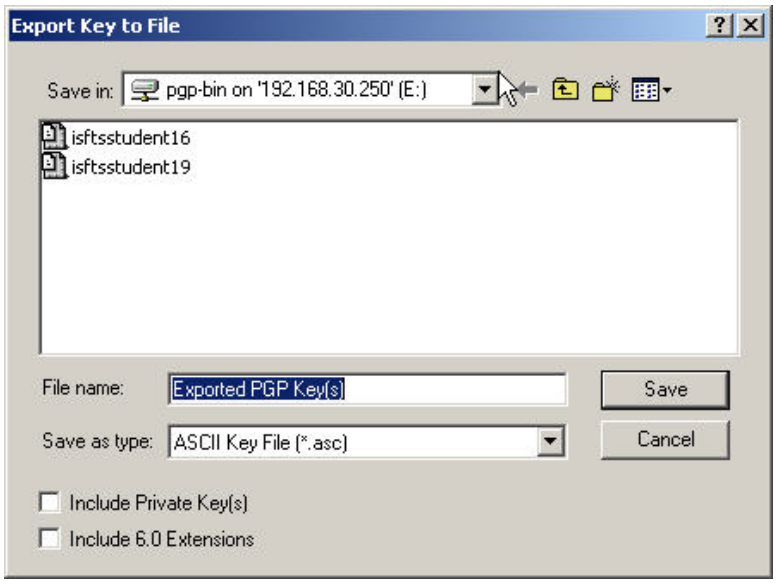
Exercise 3 – Exchanging PGP Keys with other students

This illustrates how pgp key rings can be populated with the public keys of other individuals with whom you wish to securely communicate. This exercise will simulate sending and obtaining public keys to a server like MIT's PGP Public Key Server.

1. Open the PGPKeys window; select your PGP Key Pair from the list highlighting that Key Pair by right clicking. Next choose the "Keys" option from the drop-down menu and select the Export function. As in Exercise #2, you will now need to export your Public PGP Key. You are going to export the selected PGP Key to the *pgp-bin* shared directory on the server at 192.168.30.250. This location should be already mapped for you in "My



Computer" as pgp-bin on '192.168.30.250' (E:). If you do not see this mapped drive open Windows Explorer and browse to \\192.168.30.250\pgp-bin. This is the location where you will save your Public PGP Key. Make sure when exporting your PGP Key you **DO NOT** include your private key. In the lower left hand side of the "Export Key to File" there is a box for including private keys. Make sure that this box is unchecked; ***IF NOT, YOUR "SECRET"PRIVATE KEY WILL BE SENT DEFEATING THE PURPOSE OF PGP***.



2. Next you are going to Import your partner's PGP Public Key from the pgp-*bin* shared directory on the server at 192.168.30.250. This location should be already mapped for you in "My Computer" as pgp-bin on '192.168.30.250' (E:). If you do not see the mapped drive, open Window Explorer and browse to \\192.168.30.250\pgp-bin. Now that you a viewing the pgp-bin shared directory locate your partner's PGP Public Key. (i.e. isftsstudent16) Right click on your partner's PGP Public Key (will be an .asc file), move the mouse to PGP and select Decrypt & Verify. You will see a window with your classmate's public key information in it; make sure it is highlighted and click Import. Open your PGP Keys and verify that the new public key you have imported is in place on the key ring.

Exercise 4 – Signing the new key

PGP requires that trust be established prior to using another person's public key to communicate securely. This is accomplished by signing their public key with your private key.

1. Right click on the newly imported public key (your partner's)
2. Select Sign
3. Ensure that the 'Allow signature to be exported . . . ' box is unchecked
4. Have your partner read you the fingerprint for their public key from the display of their system. This should match exactly the fingerprint that is displayed in this window.
5. Once the fingerprint has been verified, click OK
6. Ensure your private key is selected in the drop down box
7. Enter your passphrase and click OK
8. Now the round icon to the right of the key on your key ring should be green
9. Right click on the key again
10. Select Key Properties

11. Slide the bar on the bottom from 'Untrusted' to 'Trusted'
12. Click Close

Exercise 5 – Encrypting a file using your partner's public key

PGP can be used to encrypt files so that only specified people can read them. This is accomplished by encrypting the file with the intended recipient's public key.

1. Create a text file using Notepad. Write a brief secret message (don't tell your partner what it says) and then save the file as *yourname.txt* to the My Documents folder. Use your real name for this!
2. Open Windows Explorer and browse to the file you just created
3. Right-click on the file and move the mouse over PGP
4. Click on Encrypt
5. Select your partner's public key from the list by double clicking on it
6. Click OK
7. In the same folder as the .txt file, there should be a file with a similar name which ends in .pgp (i.e. *yourname.txt.pgp*)
8. Copy this file to the *pgp-bin* share

Exercise 6 – Decrypting the file with your private key

Your intended recipient uses his/her private key to decrypt the file.

1. Open Windows Explorer and browse to the *pgp-bin* share
2. Select the .pgp file that has your partner's name as part of the filename
3. Double-click on the file
4. In the PGP window, enter your passphrase and click OK
5. In Windows Explorer, double click on the unencrypted file (yourpartner's name.txt) and read the secret message that your partner wrote

Exercise 7 – Encrypting and Signing a file

By signing the file with your private key, your intended recipient is assured that it actually came from you and that it has not been modified in transit.

1. From the My Documents folder, open the *yourname.txt* file in Notepad
2. Highlight all of the text
3. Right click on it and select Copy
4. Right click on the PGP Lock in the tray (near the clock)
5. Select Clipboard
6. Click on Encrypt & Sign
7. Double click your partner's public key and click OK
8. Enter your passphrase and click OK
9. Now the text on the clipboard is signed

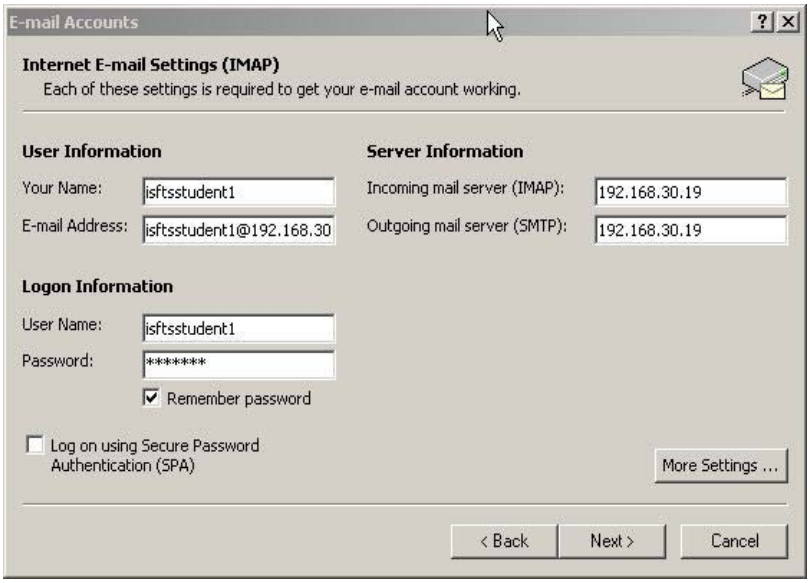
10. Go back to Notepad and delete the old text
11. Paste the encrypted/signed text into Notepad
12. Save the file as *yourname-signed.txt* in the *pgp-bin* share

Exercise 8 – Verifying the signature

1. Open the *yourpartner's-signed.txt* file from the *pgp-bin* in Notepad
2. Highlight all of the text in the file
3. Right Click and select Copy
4. Right click on the PGP lock in the system tray
5. Select Clipboard
6. Click on Decrypt & Verify
7. Notice the status of the signed message (should be 'good')

Exercise 9 – Sending Secure Email with PGP

1. Open Microsoft Outlook by clicking the icon located on the desktop
2. Click on the Tools menu and select E-mail Accounts
3. Click Add a new e-mail account and then click Next
4. Under Server Type, click IMAP and then click Next
5. In the Your Name box, type your computer's hostname (i.e., isftsstudent1)
6. In the E-mail address box, type your computer's hostname and then @192.168.30.19 (i.e., isftsstudent1@192.168.30.19)
7. In the User Name box, type your computer's hostname (i.e., isftsstudent1)
8. In the Password box, type tartans (for the purposes of this exercise, check the Remember password box)
9. In the Server Information boxes (Incoming & Outgoing) you will need to enter the following IP Address "192.168.30.19" in both fields. Once this has been completed click "Next" continue.



10. After your email account is created in Outlook (may take a few moments to synchronize), Click the PGP Menu (in Outlook at top of screen) and select Options

11. Under Email Options, check all of the boxes and then click OK

12. Now click the Tools menu and select Options
13. Click the Mail Format tab, Uncheck the *Use Microsoft Word…*boxes and then click OK
14. Click File|New|Mail Message
15. In the To: box, type your partner's email address (i.e., isftsstudent2@192.168.30.19)
16. Type anything as a subject and then type a short message to your partner in the body of the message, then click Send
17. Type your passphrase and then click OK (Click the Send/Receive button several times until your message arrives)
18. When you read the message from your partner, notice that your message is verified, decrypted, and displayed in the PGP Secure Viewer.

Exercise 10 - Adding a Public Key and sending Secure Email

1. In this exercise you will need to encrypt an email to the Instructor using PGP. Therefore, the first step is to obtain the instructor's Public PGP Key. The Instructor's PGP Key (isftsinstructor@192.168.30.19) is located in the shared pgp-bin directory at 192.168.30.250.
2. Before you can send a secure email you'll need to import the Instructor's Public Key to your Key Ring. To review the process make reference to Exercise #3.
3. Go into Outlook and send a PGP Secure email message to isftsinstructor@192.168.30.19; the instructor will verify that a message is received from each student