With the recent increase in sensitive information being compromised worldwide, Murray State University is taking the initiative to help you secure your data. One way to do this via email is through the use of PGP (Pretty Good Privacy). PGP is a computer program that provides cryptographic privacy and authentication. It is used for signing, encrypting, and decrypting emails to increase the security of the email communication. For our particular setup, we are going to use a program called Gpg4win which is a windows installation package to support PGP to create and maintain the public/private keys.

---

## Installing and Creating Public/Private Keys with Gpg4win

### Step 1 – Downloading the Gpg4win

Download the latest version of Gpg4win from http://www.gpg4win.org/download.html.

### Step 2 – Installing Gpg4win

Double click on the gpg4win-x.x.x.exe file and then follow the instructions provided by the program. Please accept all of the default values when installing.

### Step 3 – Starting Gpg4win

Once the installation is complete you can click on Start → All Programs → Gpg4win → GPA to open up the program.

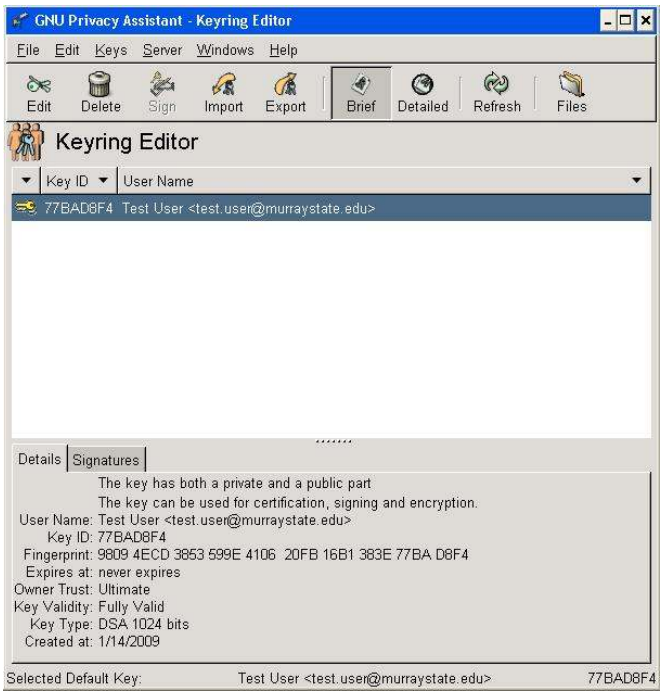
### Step 4 – Generating a key

This will open the GNU Privacy Assistance - Keyring Editor. As soon as you open it, the program will ask you if you want to "Generate a key now". Go ahead and click on that button and then follow the directions to create your public/private keys. When you get to the screen to generate a passphrase, it is recommended that you use a complex passphrase that is 12 characters or more. Gpg4win will warn you if your password is less than 12 characters, however you can still accept a weaker passphrase but for the most security, you need a complex/long passphrase.

After creating the key, you will also be asked if you would like to back up the key now. It is recommended that you do this; however you need to store this backup in a secure place such as putting the backup on a CD and placing it in a safe or using a program such as TrueCrypt and putting the backup in another encrypted file.

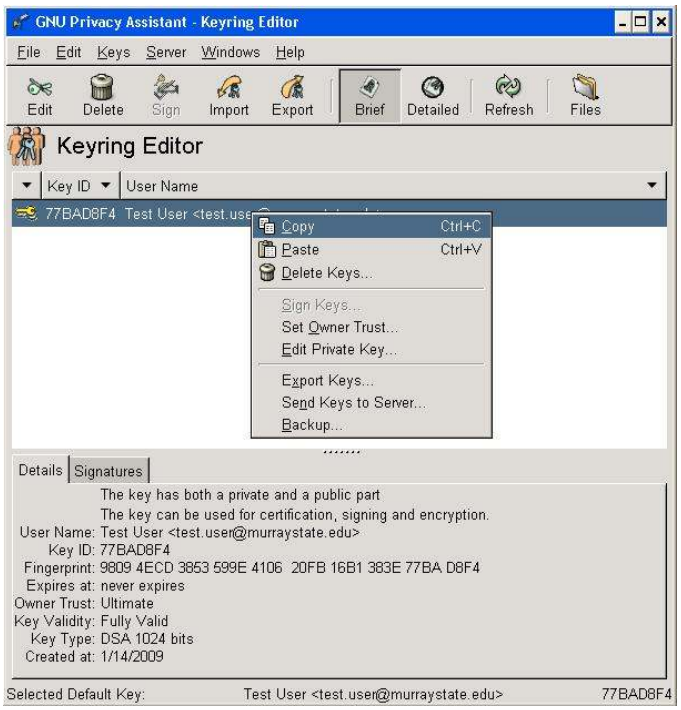
**Step 5 – Verifying your key**

Once your keys have been created it takes you back to the main page of the program. You will now see your key in the Keyring Editor.



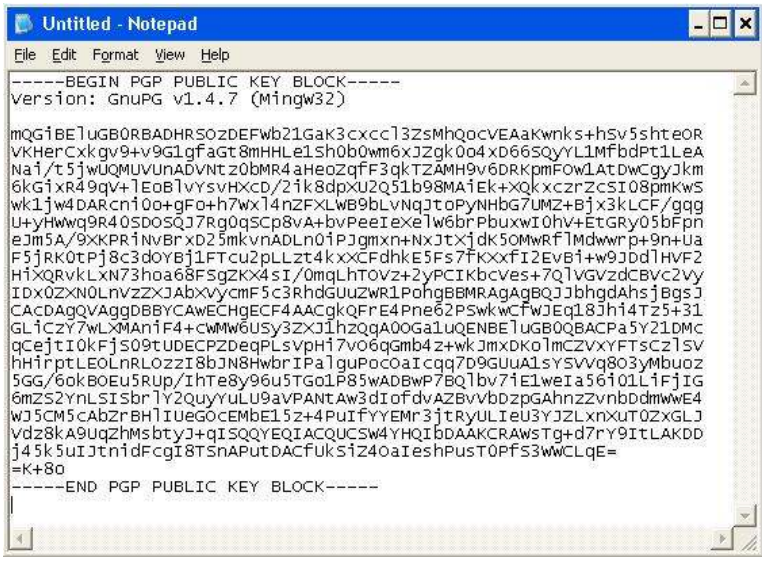
**Step 6 – Sharing your public key**

To be able to use PGP, you will need to share your public key with others. To do this you simply right click on your key and click Copy.



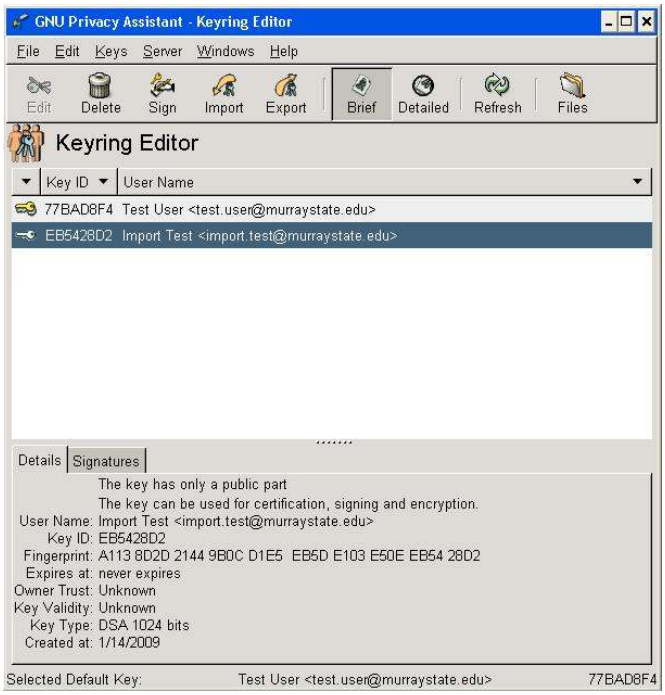

You then need to paste this into an email or document that you will give to others that want to encrypt email to you. In the screen shot below I have showed you an example of what the key will look like.

**Note, It is very important that the key is in exactly the format below, or it will not work.*



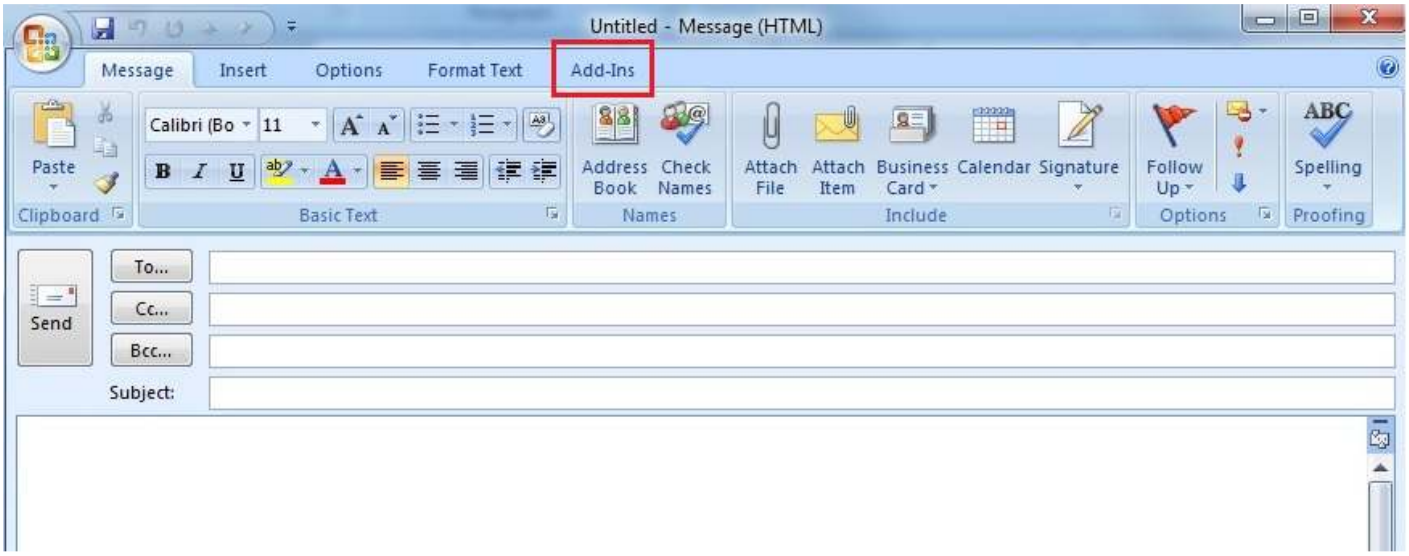
**Step 7 – Importing keys from other people**

Once someone has shared a public key with you, you need to highlight the entire key (make sure you start highlighting with the line that says BEGIN PGP and go all the way to the line with END PGP) and copy it. Then open the GNU Privacy Assistant - Keyring Editor and click on Edit and Paste. You will then see a new key pop up in your Keyring Editor like shown below.

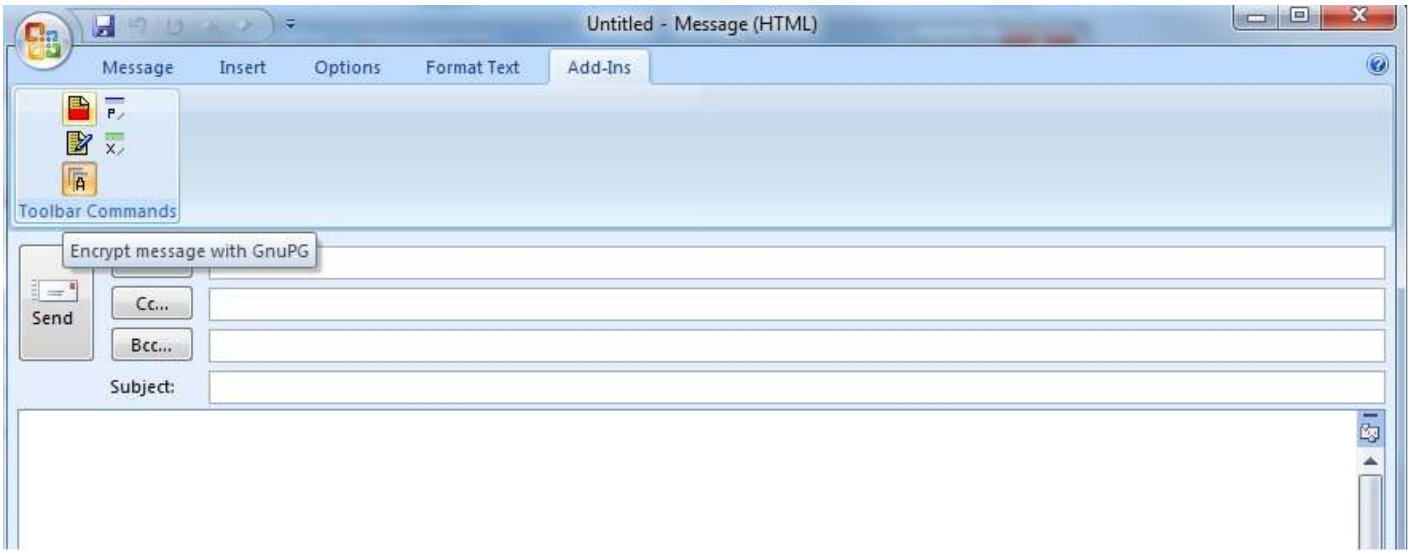


## Implementing PGP with Microsoft Outlook

To be able to send PGP encrypted emails through outlook is very easy. All of the software is already installed when Gpg4win was installed. All you have to do now is open up Outlook like normal, and click on "New" to create a new email. Once you do this a new window will open up that looks like the following screenshot.

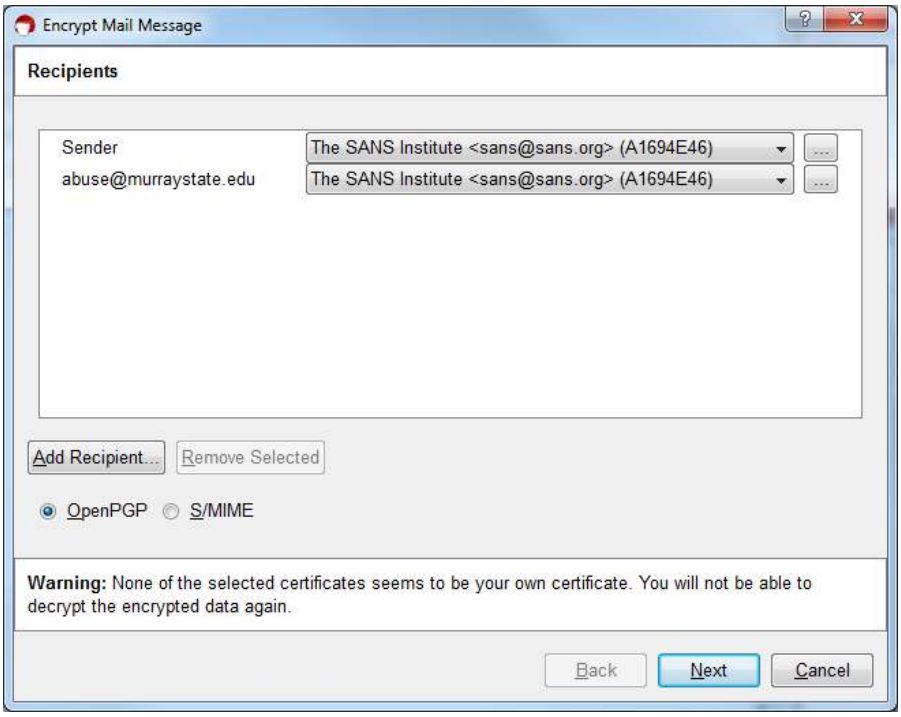



As you can tell, I have highlighted the "Add-Ins" section above. This is the section you will need to click on to access Gpg4win. Once you click on that, the following screen will appear.

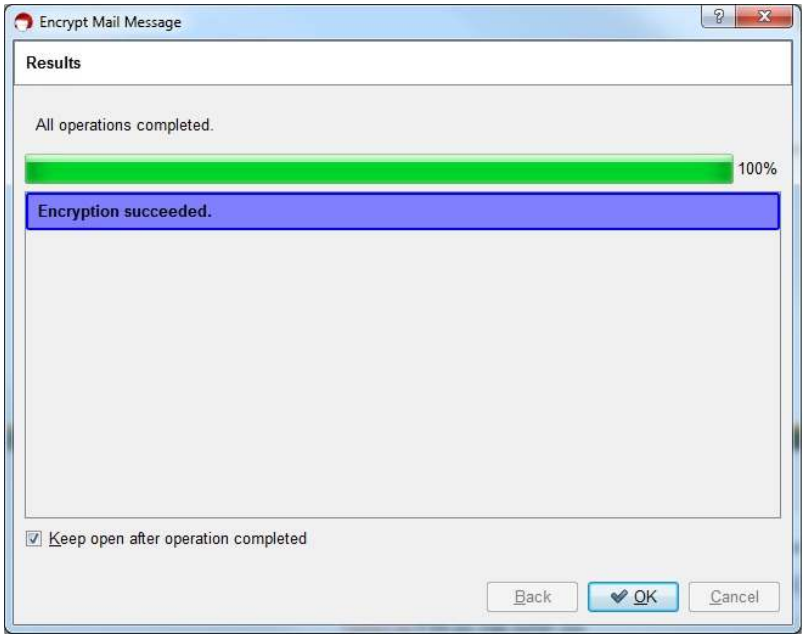



From here, you need to click on the red document on the left hand side of the screen. If you hover over it with your mouse, it will say "Encrypt message with GnuPG". Once you click on this icon, all you have left to do is type the message and press send.

After you press send, the following screen will appear asking you who the "Sender" and "recipients" are. For "Sender" you need to select yourself, and then click on "Add Recipient…" at the bottom and choose whoever you are going to send the email to. For this example I am using the same key on both the sender and receiver, this will only be the case if you are sending yourself an encrypted email.




Once you have selected all the parties involved, click the "Next" button and then the following screen will pop up saying that your email has been successfully encrypted.



## Implementing PGP with Firefox

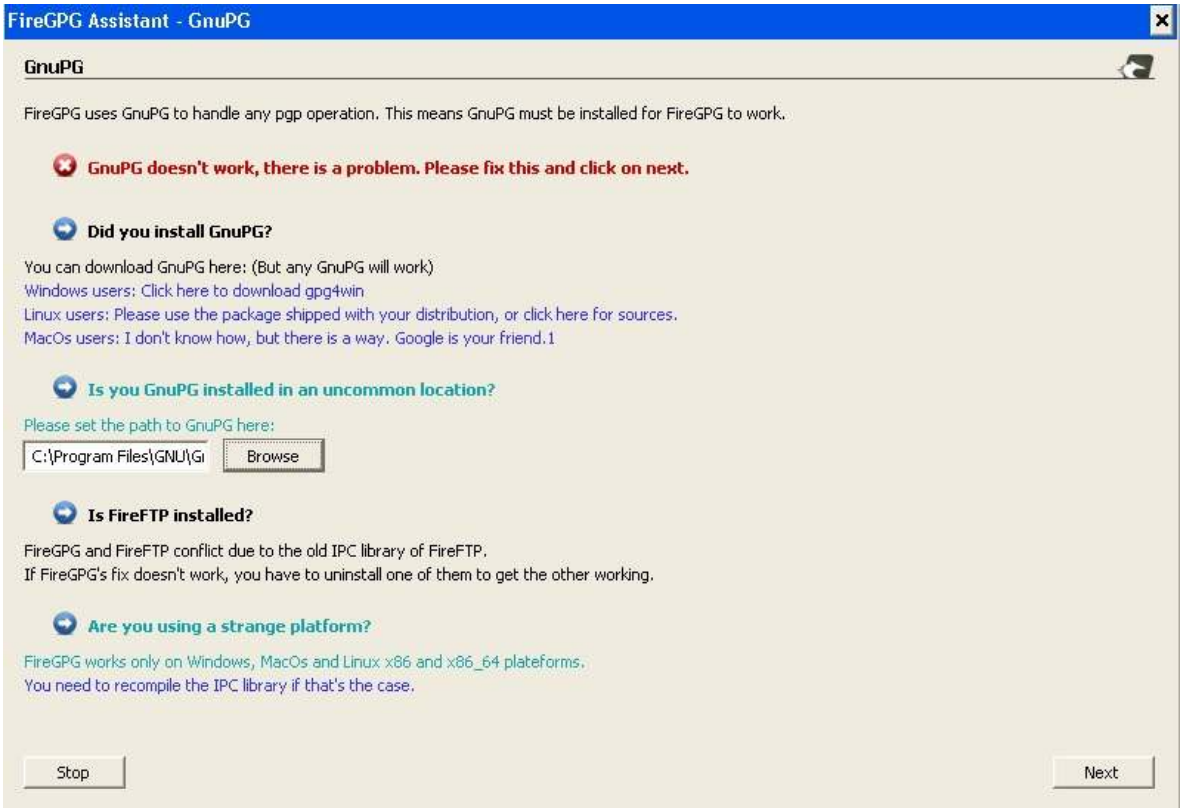
### Step 1 – Downloading FireGPG

Download the FireGPG add-on which can be found at http://getfiregpg.org/install.html. This page also has very good instructions over a lot of the functionality of FireGPG.

### Step 2 – Configuring FireGPG

Once this gets done installing, you will need to restart Firefox. Once Firefox has restarted, a box will probably pop up asking you to help configure GPG.

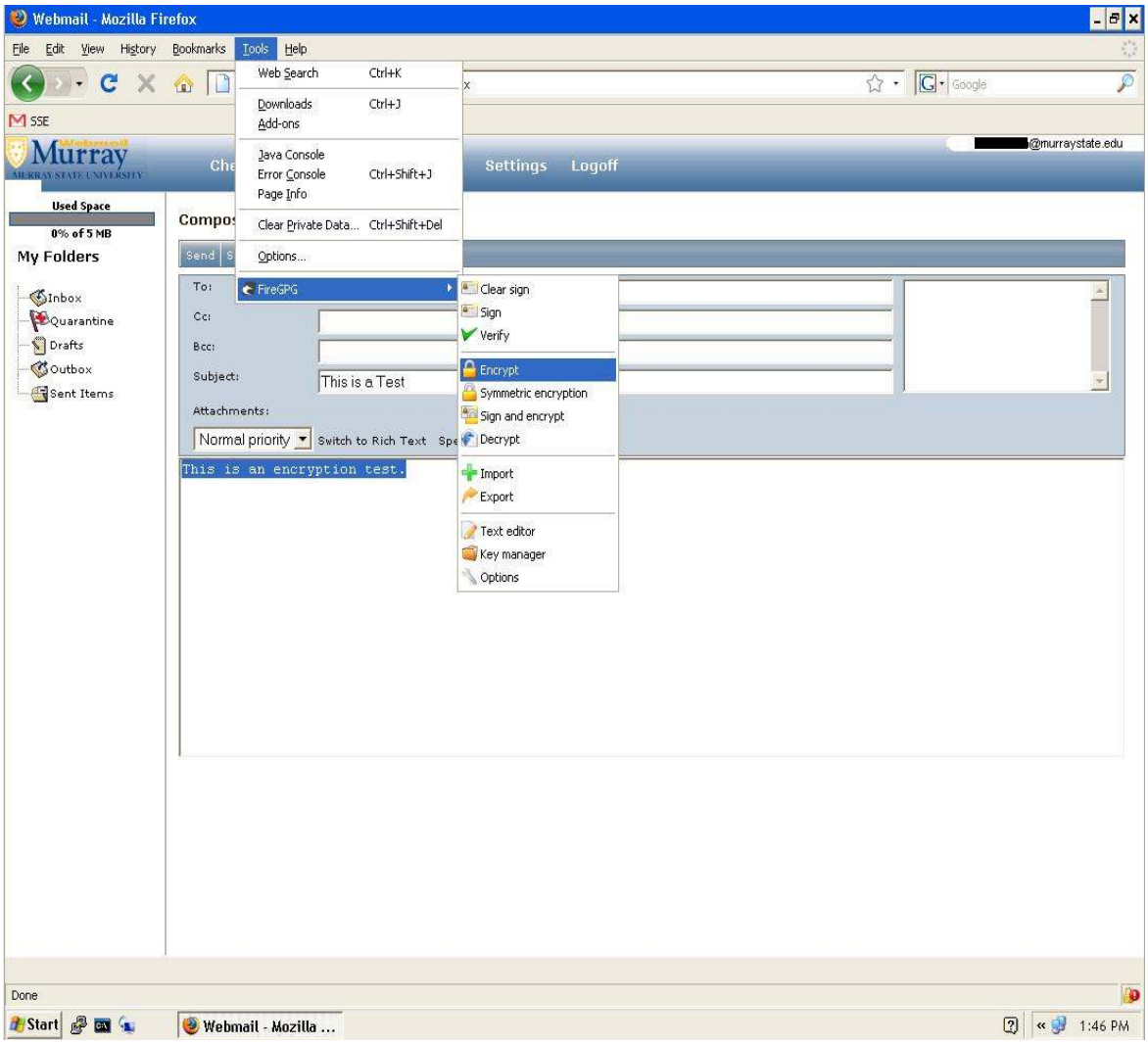
If the box does not come up then everything installed correctly. If the box does come up, then you will probably need to tell Firefox the location of your GPG program. To do this, click on the "Browse" button and go to "C:\Program Files\GNU\GnuPG\gpg2.exe" if you are using a 32 bit operating system or "C:\Program Files (x86)\GNU\GnuPG\gpg2.exe" if you are using a 64 bit operating system. A screenshot of this can be found below.



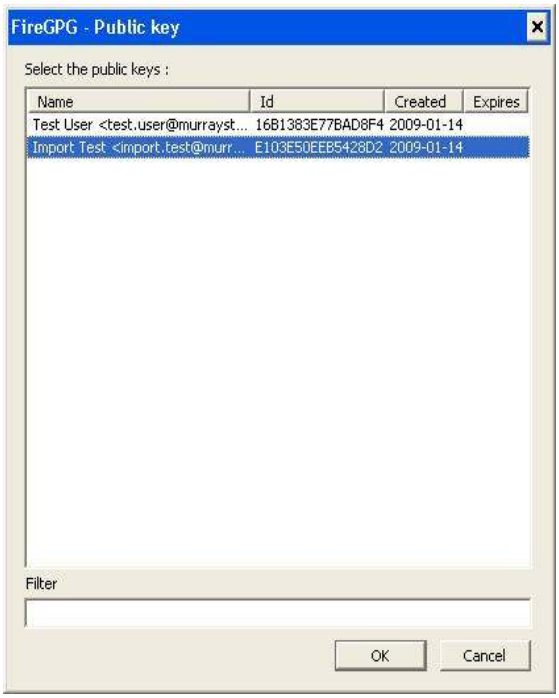

During the FireGPG Assistant program, it may also ask you other questions about what options you would like set. Unless you are familiar with these options and would like to change them for personal reasons, accept all of the default values.

## Step 3 – Encrypting email using FireGPG

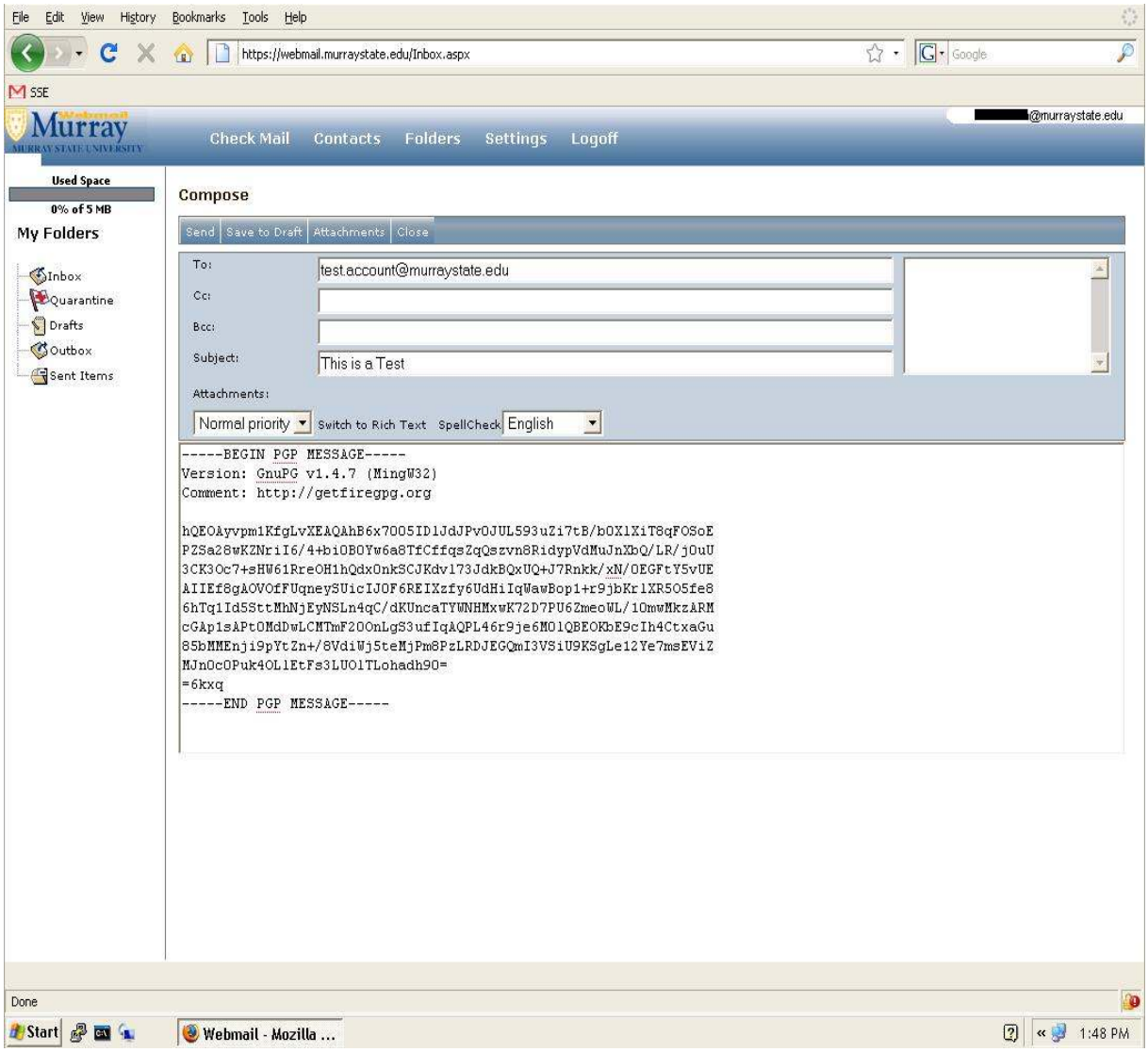
To encrypt an email using the FireGPG add-on, you simply open your Webmail program. In the example below we are using Murray State University Webmail. Once you compose your email, you highlight the text that needs to be encrypted, and then click on Tools → FireGPG → Encrypt.



Once you hit encrypt, it will then bring up a FireGPG – Public Key box, like shown below. You then select the public key of the person you want to send the email to. In our example, we are sending an email to import.test@murraystate.edu. If you wanted to send this message to multiple recipients, you can hold "Ctrl" on your keyboard and select as many names as you need to. This will allow the message to be encrypted to multiple recipients at the same time. You may also want to select your own key on each message you send as well so you are always able to unencrypt the message and read it.




After you select the public key, and click ok, you will then see your original message has become encrypted and is now ready to be sent.


File Edit View History Bookmarks Tools Help
https://webmail.murraystate.edu/Inbox.aspx
Google
SSE
Murray
MURRAY STATE UNIVERSITY
[redacted]@murraystate.edu
Check Mail Contacts Folders Settings Logoff
Used Space
0% of 5 MB
My Folders
Inbox
Quarantine
Drafts
Outbox
Sent Items
Compose
Send Save to Draft Attachments Close
To: test.account@murraystate.edu
Cc:
Bcc:
Subject: This is a Test
Attachments:
Normal priority Switch to Rich Text SpellCheck English
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.7 (MingW32)
Comment: http://getfiregpg.org
hQEOAyvpm1KfgLvXEAQAhB6x7OO5ID1JdJPvOJUL593uZi7tB/bOX1XiT8qFOSoE
PZSa28wKZNriI6/4+biOBOYw6a8TfCffqsZqQszvn8RidypVdMuJnXbQ/LR/jOuU
3CK3Oc7+sHW61RreOH1hQdxOnkSCJKdvl73JdkBQxUQ+J7Rnkk/xN/OEGFtY5vUE
AIIEf8gAOVOfFUqneySUicIJOF6REIXzfy6UdHiIqWawBop1+r9jbKr1XR5O5fe8
6hTq1Id5SttMhNjEyNSLn4qC/dKUncaTYWNHMxwK72D7PU6ZmeoWL/1OmwMkzARM
cGAp1sAPtOMdDwLCMTmF2OOnLgS3ufIqAQPL46r9je6MOlQBEOKbE9cIh4CtxaGu
85bMMEnji9pYtZn+/8VdiWj5teMjPm8PzLRDJEGQmI3VSiU9KSgLe12Ye7msEViZ
MJnOcOPuk4OL1EtFs3LUOlTLohadh90=
=6kxq
-----END PGP MESSAGE-----
Done
Start
Webmail - Mozilla ...
1:48 PM

Some email systems such as Gmail has built in support for FireGPG. The screenshot below shows an example of how this will look. To encrypt email using these shortcut keys, all you have to do is type the message, click encrypt, then press send. Once Gmail starts to send the email, it will bring up a box asking which key you want to encrypt the message with. Once you choose the key, the message will be encrypted and sent.