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

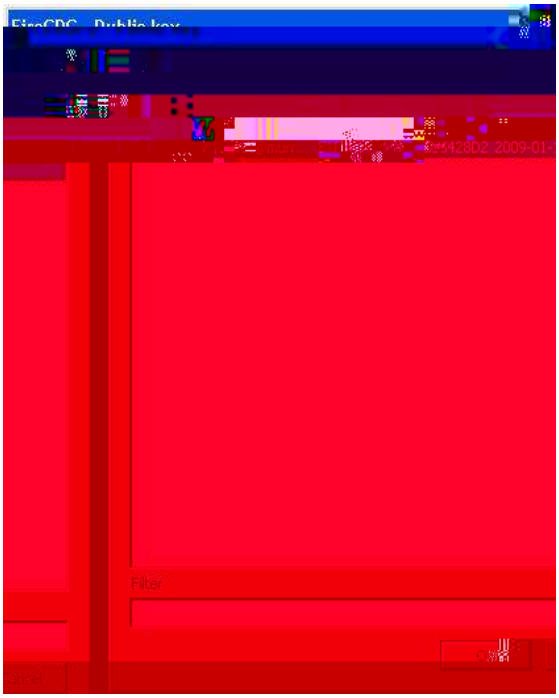
Once the installation is complete you can click on Start All Programs Gpg4win GPA to open up the program.

Step 4 – Generating a key

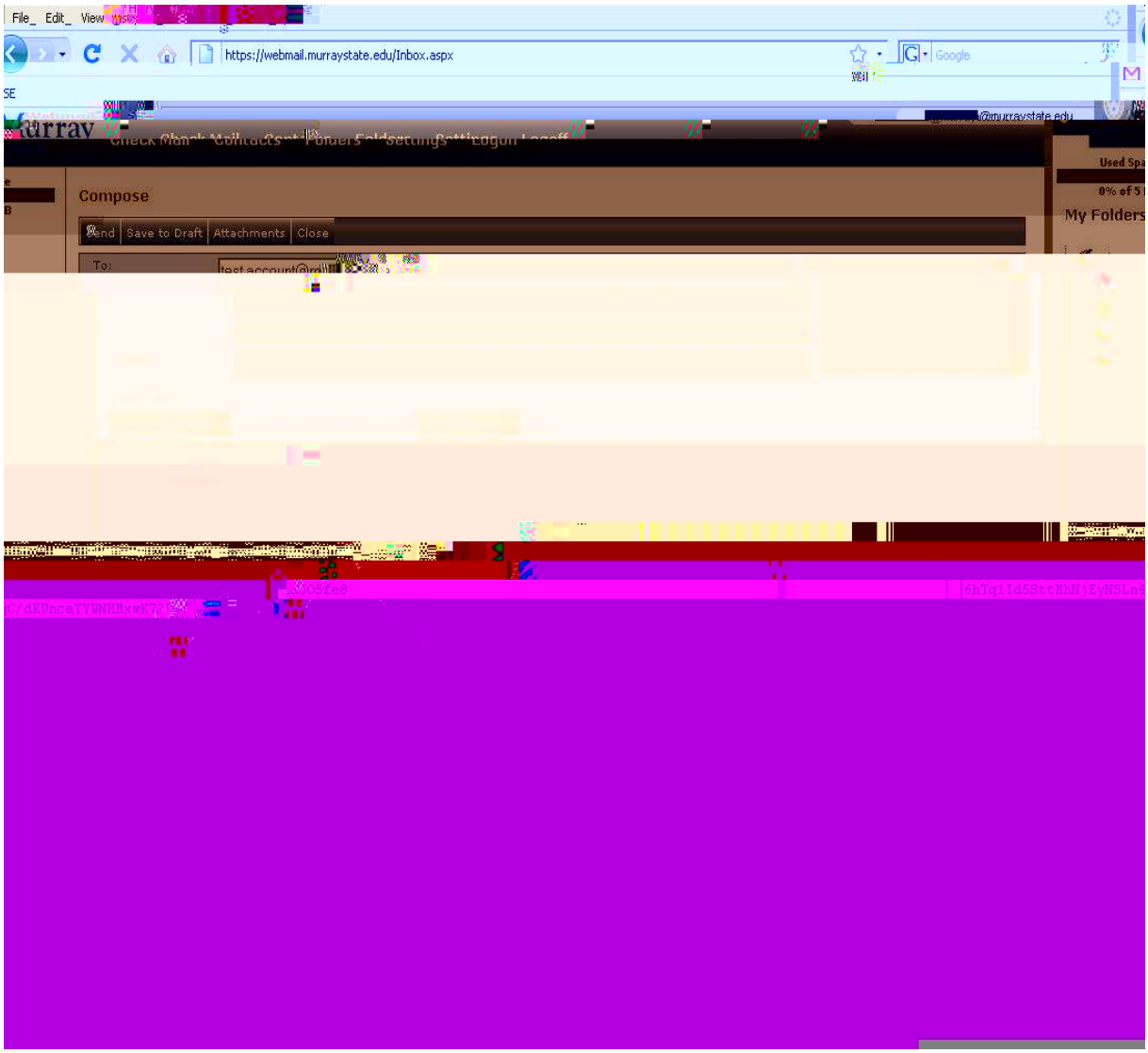
This will open the GNU Privacy Assistance - Keyring Editor. As soon as you open it, the program will ask you if you want to "Generate a key now". Go ahead and click on that button and then follow the directions to create your public/private keys. When you get to the screen to generate a passphrase, it 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.

Once you hit encrypt, it will then bring up a FireGPG – Public Key box, likes
select the public key of the person you want to send the email to. In our examp
email is import.test@murray.sl. If you wanted to send this message to multiple re
can hold "Ctrl" on your keyboard and select as many names as you need to.
to been encrypted to multiple recipients at the same time. You may also want to
each message you send as well so you are always able to unencrypt the mess



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


File_ Edit_ View
https://webmail.murraystate.edu/Inbox.aspx
Google
Compose
Send
Save to Draft
Attachments
Close
To:
My Folders