Using PGP E-mail

Setting up Enigmail + GnuPG for on Thunderbird

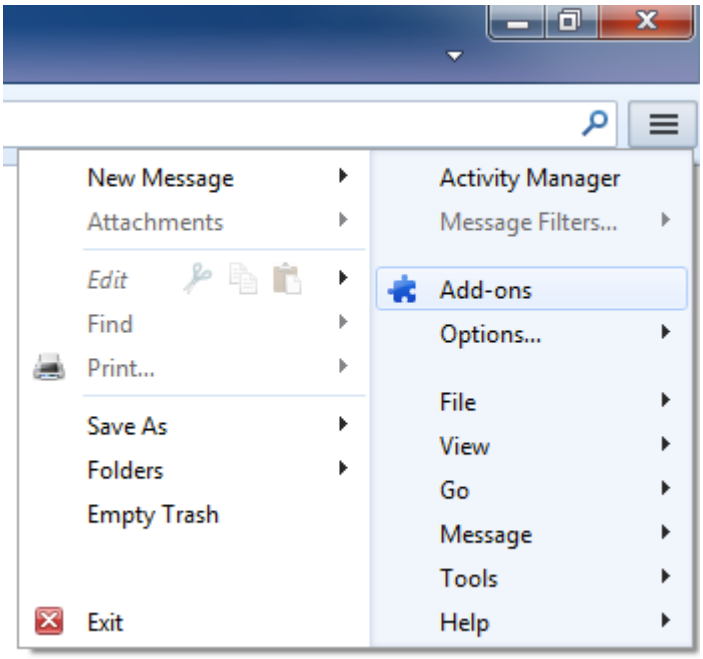
In this document, we are going to try to setup the e-mail environment that you can use sign or sign+encrypt. PGP is one of the widely used for CSIRTs in the world, and mainly we use GnuPG for that. There still Unix command line version of GPG, but using Thunderbird with Enigmail plugin makes easier to use PGP e-mail.

1. Make sure you have downloaded files as follows
GnuPG : http://www.gnupg.org / http://gpg4win.org/download.html
Thunderbird : http://www.mozilla.com/thunderbird/

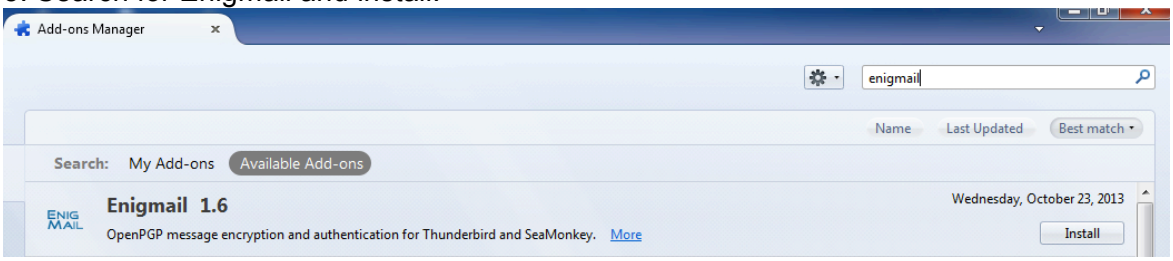
2. Install GnuPG for Windows. Double click the binary and continue to clicking “Next” until the end. Finally you’ll click “Finish”.

3. Install Mozilla Thunderbird for Windows. Double click the binary and continue to clicking “Next” until the end. Finally you’ll click “Finish”. Configure Thunderbird to your email account. Suggested protocol is IMAP so that you will have a copy of email in your server.

4. Install Enigmail for Thunderbird. Select “Tools” then “Add-ons”



5. Search for Enigmail and install.

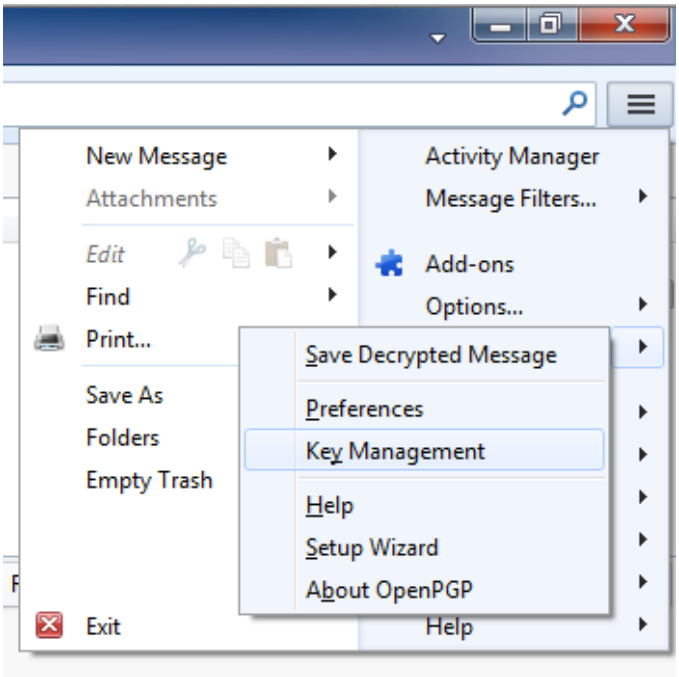


6. After clicking “Install” restart your thunderbird. Install was completed !

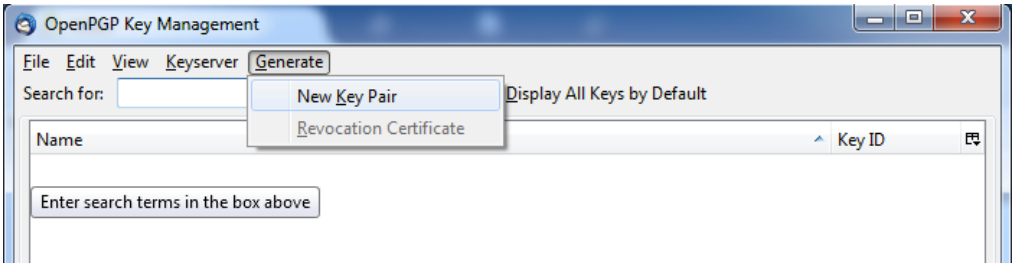
Using the Enigmail Key Wizard

By this time, you should have Thunderbird, Enigmail and GnuPG as installed.

1. Start Thunderbird
2. Go to Menu > Open PGP > Key Management



3. Click on Generate > New Key Pair to generate your PGP Key

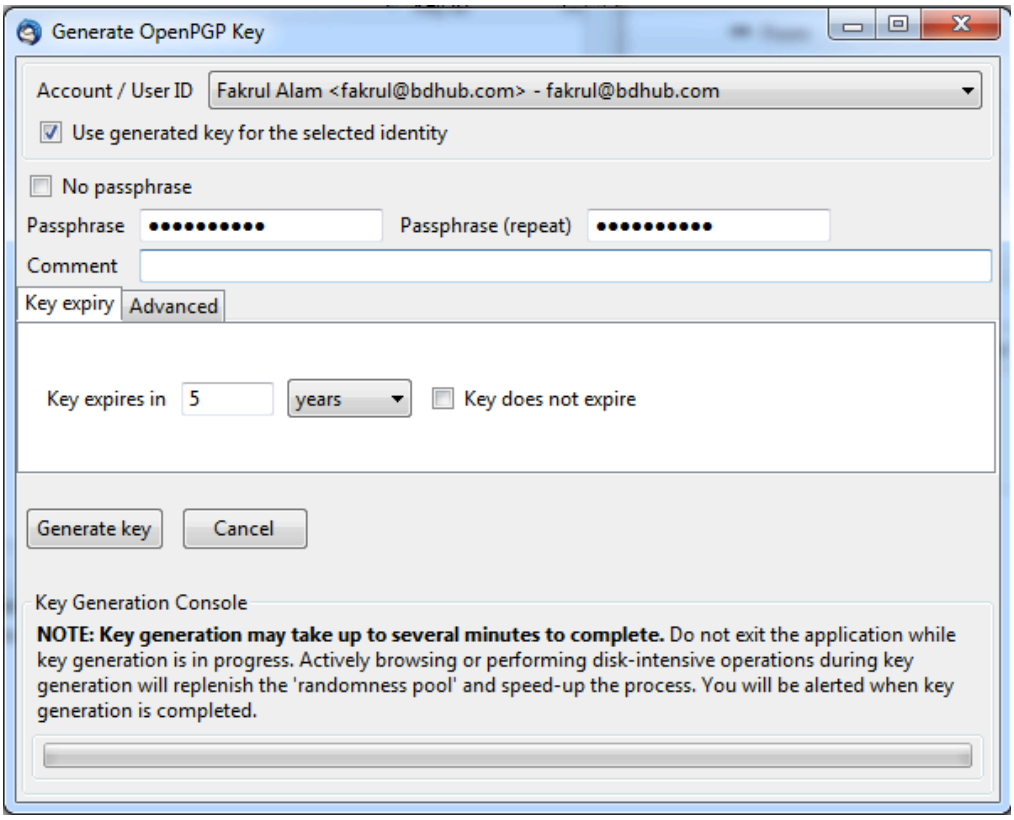


4. Now select your Account / UserID (if you have multiple email id configured).
5. Choose a passphrase. Private key are so important that GnuPG will not use them unless you know the secret phrase. You're being asked here what the secret phrase should be for your new keypair. If at all possible, choose something that is easy to remember but very hard for someone to guess.

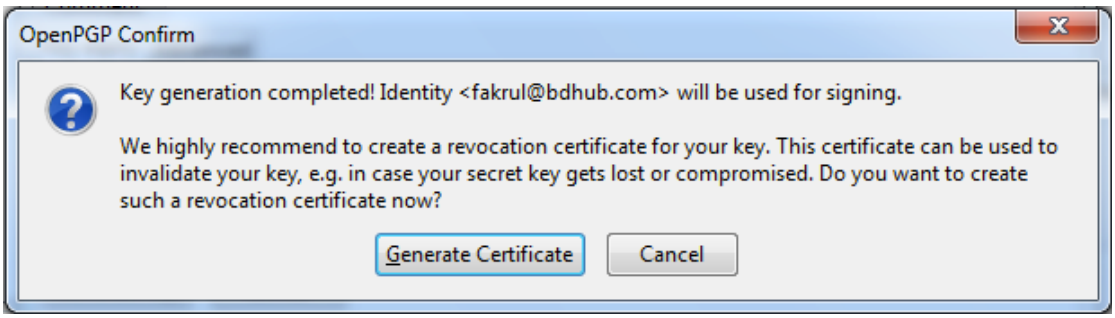
Enter your passphrase in the "Passphrase" box. Then repeat it again in the "Passphrase (repeat)" box. By entering it twice, Enigmail is protecting you from accidentally miss-entering your passphrase.

As a security feature, Enigmail will not display your passphrase as you type it.

Danger!
If you forget your passphrase, there is absolutely nothing anyone can do to help you. This is a security feature of GnuPG. There is no way around the passphrase.

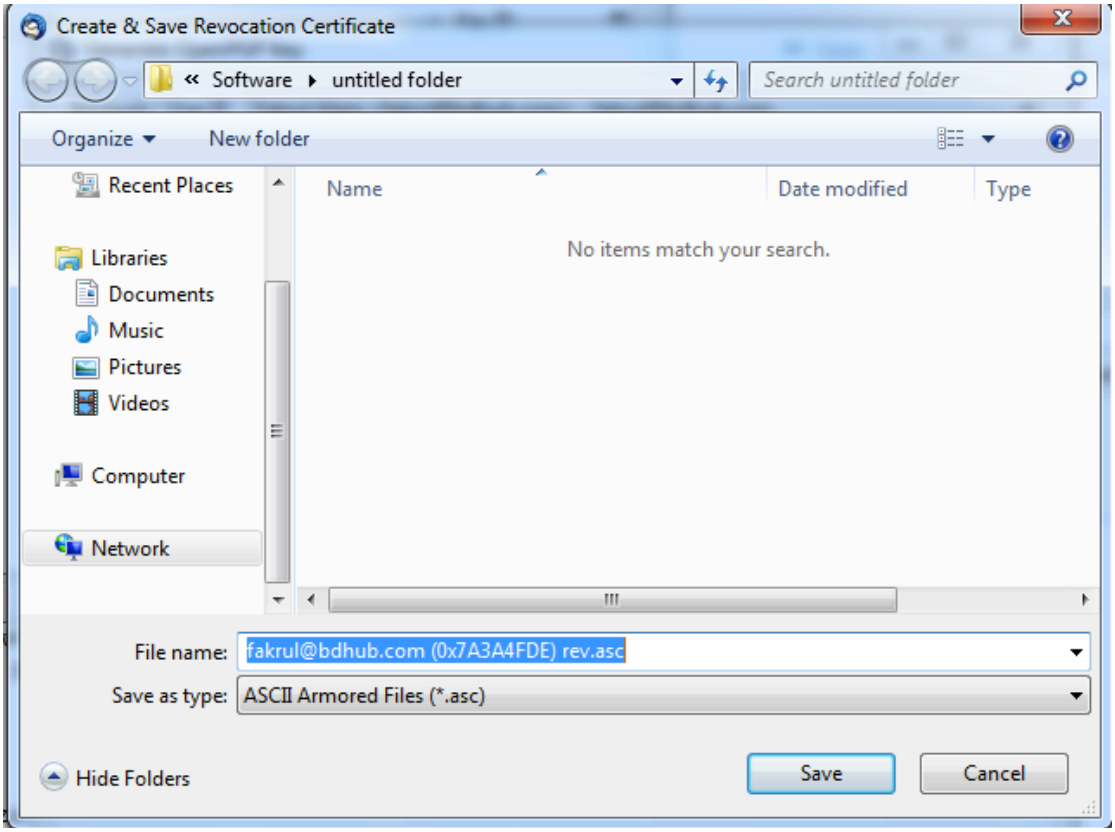


6. Click Generate Key. That's it! That's all you have to do.
7. Generate a revocation certificate. Hard drive failures happen to us all. So do house fires and theft and other things that might separate us from our keys. When this happens, it's a good idea to send out a revocation notice. You can think of this as a message from your key saying "please don't use me any more."



When you finish creating your new key. Enigmail will give you the chance to create a revocation certificate. If you want one. Click "Generate Certificate". You will asked to enter your passphrase.

8. Save the file in safe location.


Create & Save Revocation Certificate
« Software ▸ untitled folder
Search untitled folder
Organize
New folder
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
No items match your search.
File name:
fakrul@bdhub.com (0x7A3A4FDE) rev.asc
Save as type:
ASCII Armored Files (*.asc)
Hide Folders
Save
Cancel

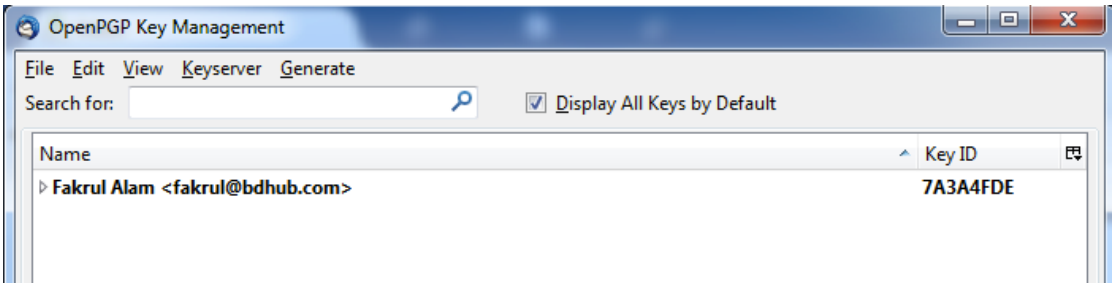
Next Steps

Your Key ID

Now that you have your key, you should find your key ID. This is a sequence of letters and numbers eight long which is used to unambiguously identify your key.

Go back to the Enigmail Key Manager and enter your email address in the search box. The key you just created should appear, and over at the right you'll see your key ID.

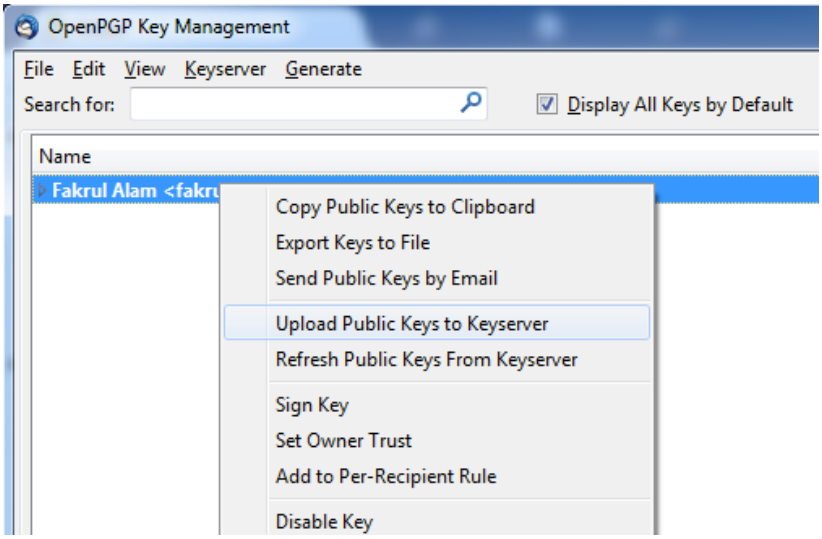
Write this down, you'll need it.



Make sure your key ID and above example tells 7A3A4FDE is a key ID.

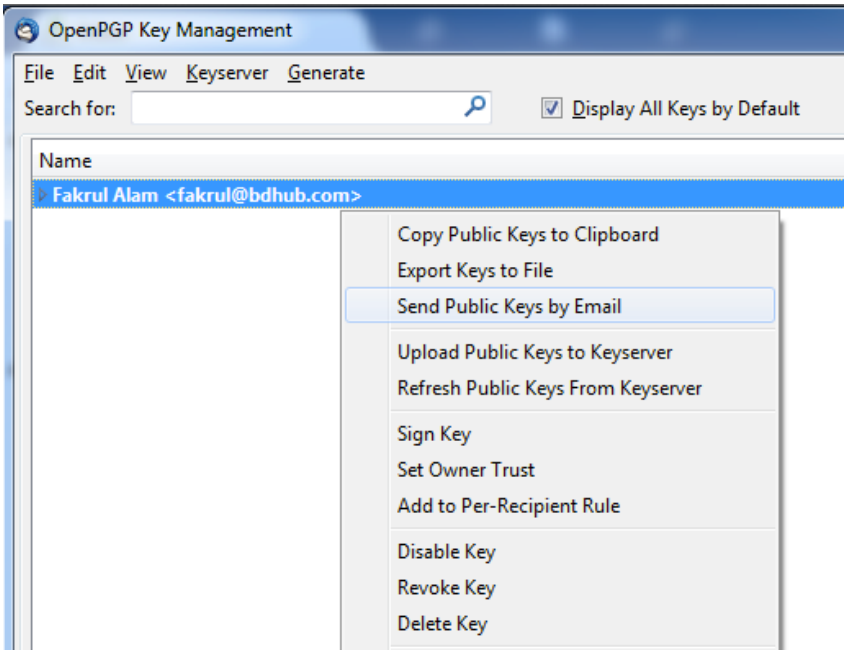
Publish Your Public Key

Note that you can upload your public key to public key servers, but in this training environment is internal use only, please do not do this at this time.

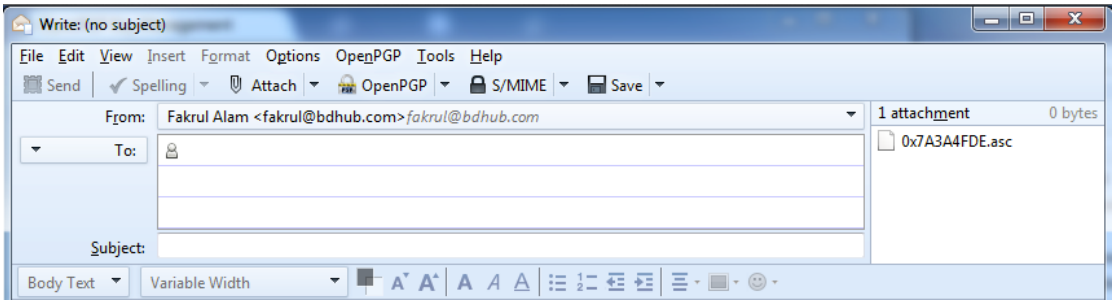


Export and send your public key

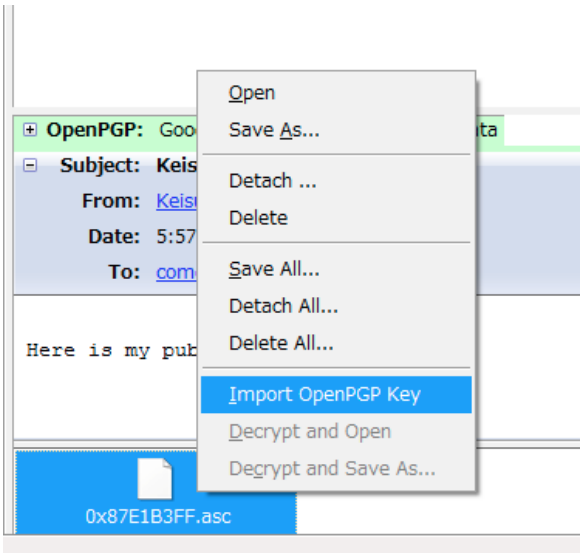
Right click on Key Manager window and chose "Send Public Keys by Email"



Your public key will be automatically attached in your email.



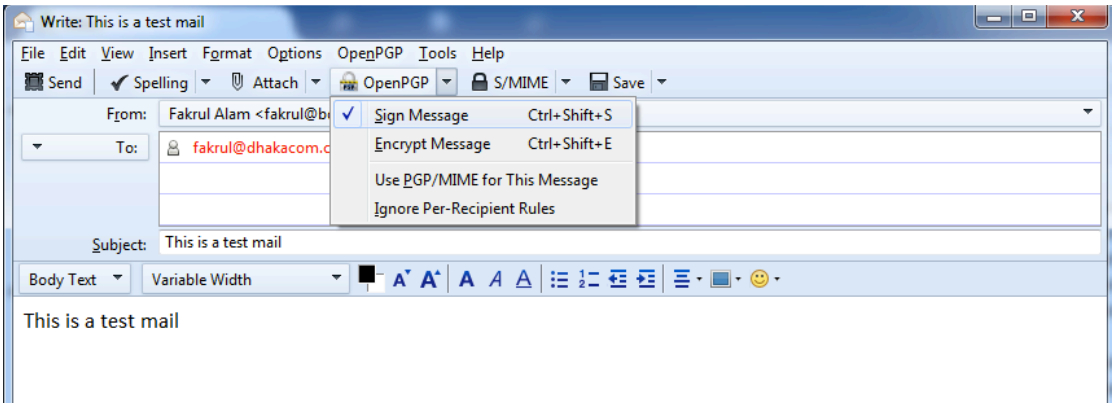
You can import the public key just by right click and choose “Import Open PGP Key”.



Your first signature

Now that you have your key created, let's try writing a signed piece of email.

1. Find a friendly face. Let's try to send signed e-mail.
2. Write a plain-text email. Write some short message to fakrul@bdhub.com.
3. Tell Enigmail to sing it. At the top of your compose window you will see a button reading "OpenPGP". Click on this. Make sure that the "Sign" option, and only that is checkd.

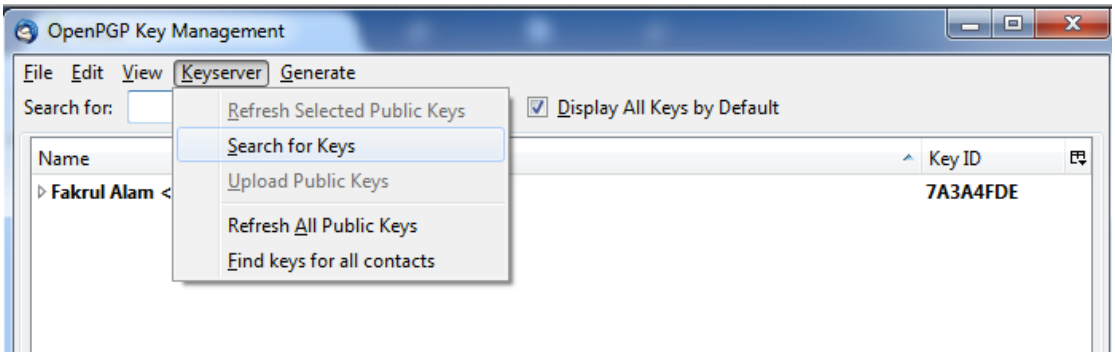


4. Hit "Send". You will be asked for your passphrase. Once you enter it, Eniingmail will sing your email and send it off to the list.
5. Congratulation! You've just sent your first signed email.

Your first encrypted email

Import PGP public keys of person sitting next to you, and make sure that is imported. You can use public key server to search public keys. Enigmail Key Manager (OpenPGP → Key Management" from the main window).

Note: You can not do this from this environment.



Findings Keys

From the Key Manager, click on "Keyserver → Search for keys". Entr the person's key ID in the search box, prefixing it with "0x", if necessary. For instance, if someone where to tell you their key ID was "ABCDEFGH", you'd enter it as "0xABCDEFGH".

Encrypting Email

Once you've obtained a copy of your correspondent's key, you're set to send encrypted email. Write an email to them just as you normally would, but before sending, click on the OpenPGP button and select "Encrypt". Once that's done, click "Send".