Welcome to Securing Your Digital Footprint-

Email Encryption (PGP)

With nearly all of the other security/privacy methods, you decide if you will implement them or not. Email and the decision to make is secure must be agreed upon with one or more parties. You will find that most people will agree that taking a step towards stronger security/privacy is the right thing to do. But when it comes to email most people will argue, “it’s too hard.” Or “it’s not necessary, since I’m not saying anything that Big Brother is interested in.” Since you can’t have secure email without it being secure from sender to receiver these people have determined how secure/private your conversations will be. You will see as you read this lesson that implementing email security is no more difficult that installing a program. But change as we all know is hard for people to grasp. It is on each one of us to be vigilant about getting friends and family to get on board. Don’t let Big Brother steal your right to privacy.

(PGP) Pretty Good Privacy has been around a long time. It is used to protect your email communications from being read by anyone except their intended recipients. It can also be used to prove that an email came from a particular person, instead of being a fake message sent by another sender. Both of these are important defenses if you're being targeted for surveillance or misinformation.

Think of encrypting your mail like the process of sending a 'sealed' snail-mail letter in real life. The recipient would be able to tell if the 'seal' was broken. With encrypted email, if anyone has been fiddling with your ‘seal,’ message, your recipients will immediately see that the signature is invalid. This happens by creating a secret key. Simplistically both parties, sender and recipient, each have 1/2 of the secret key. When the message arrives the key is then verified and the email is descrambled and readable. Because of this, it is EXTREMELY IMPORTANT to keep your secret key and your passphrase(created for each secret key) safe.

The down side, only the body of the email is encrypted. ‘From’ and ‘To’ are visible to any gov’t watching.

There are two main types of PGP encryption that can be used, S/MIME and PGP. Unfortunately they don’t mix. Verify with friends and family which type they are using.

When you create a secret key in your encryption program, it can be read by anyone through their encryption program. In other words you don’t have to have the same encryption program your friends and family do.

We’re big believer of 'use what you have,' which is easy with Apple, since they provide nearly everything in their Operating System (OS). Which is why we will use Apple's Mail program. For Windows we will use Mozilla’s Thunderbird, free email program. If you are running Mac and want to

use Thunderbird it is possible. Note:If you are an Outlook fan, here are instructions, but I was not able to verify the contents. For Apple/iOS (phones) ipgmail will be used, unfortunately this is not a free program. For Android phones you'll be using PGP Mail

Apple Mail:

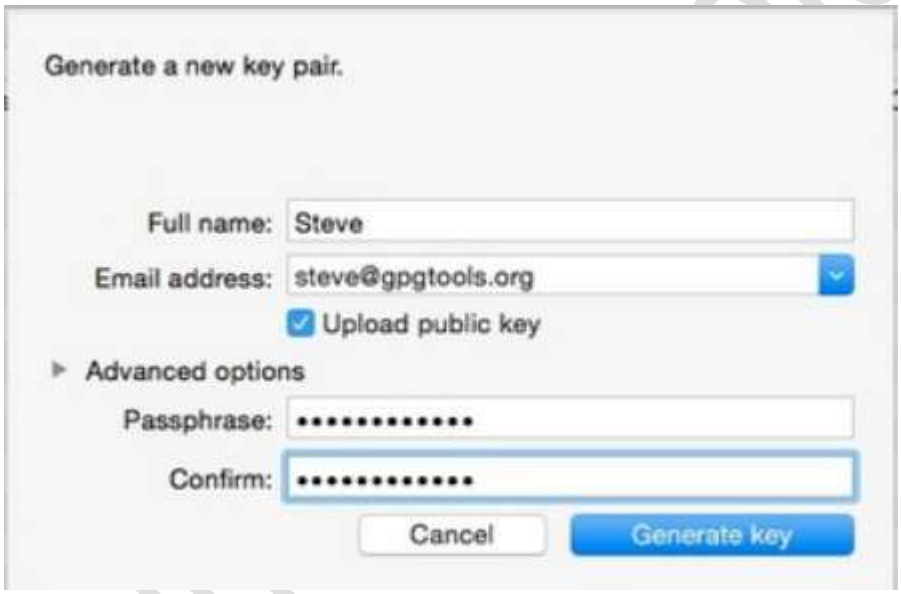
(Note: if you have upgraded to Sierra (10.12.2), this apparently doesn't work with it, at the time of this writing.

If you want to do things with Terminal (by the command line) GnuPG1 is for you.)

For everyone else, start by downloading and installing GPG_Tools.

You will need to have at least one email account set up in Mail (click here to see instructions on how to do that).

Once you install GPG_Suit and it opens it will be ready to create a key for your email address.



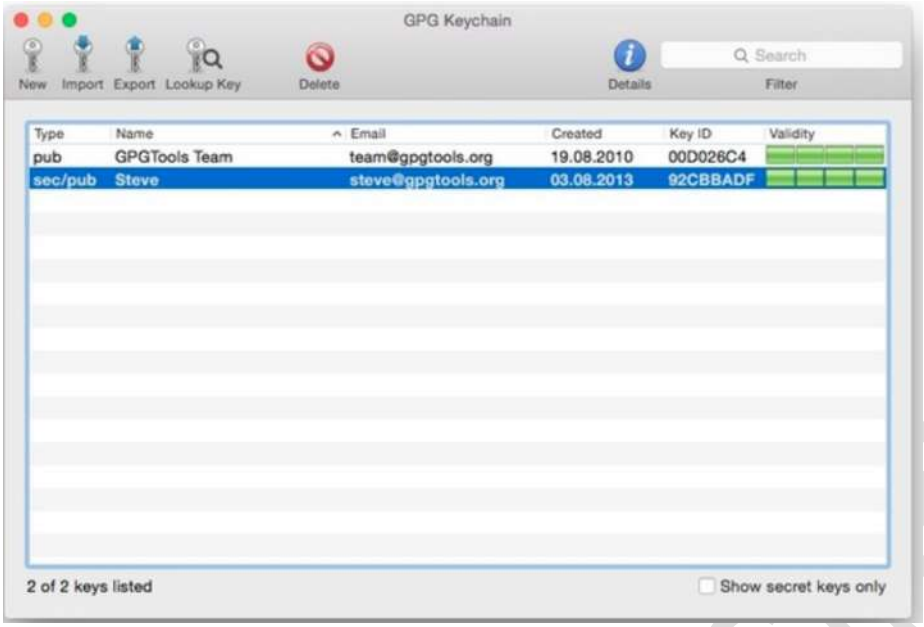
1.Type in the name for the key you are creating

2.Pick the email address from the down arrow, if you have more than one

3.Type in a password phrase (**Make sure you make note of this or you won't be able to get into this key again. Which you are going to have to do, every time you send or receive a mail.**)

Note: The image shows the box "Upload public key" checked. The instructions for the program explains this makes it easier for friends to search the 'key server' to find your key and send you a message. This sounds great, if you forget to send a key to someone. But from a security stand point it is a really bad idea. Take Lavabit for instance, they where forced by governments to allow access to their customers' encrypted email messages. The US government even demanded Lavabit's own private keys, allowing them access to ALL customers' encrypted emails. This is the same reason that Gmail and Yahoo don't have built in encryption.

4.Once you have confirmed the phrase, click the 'Generate Key' button.



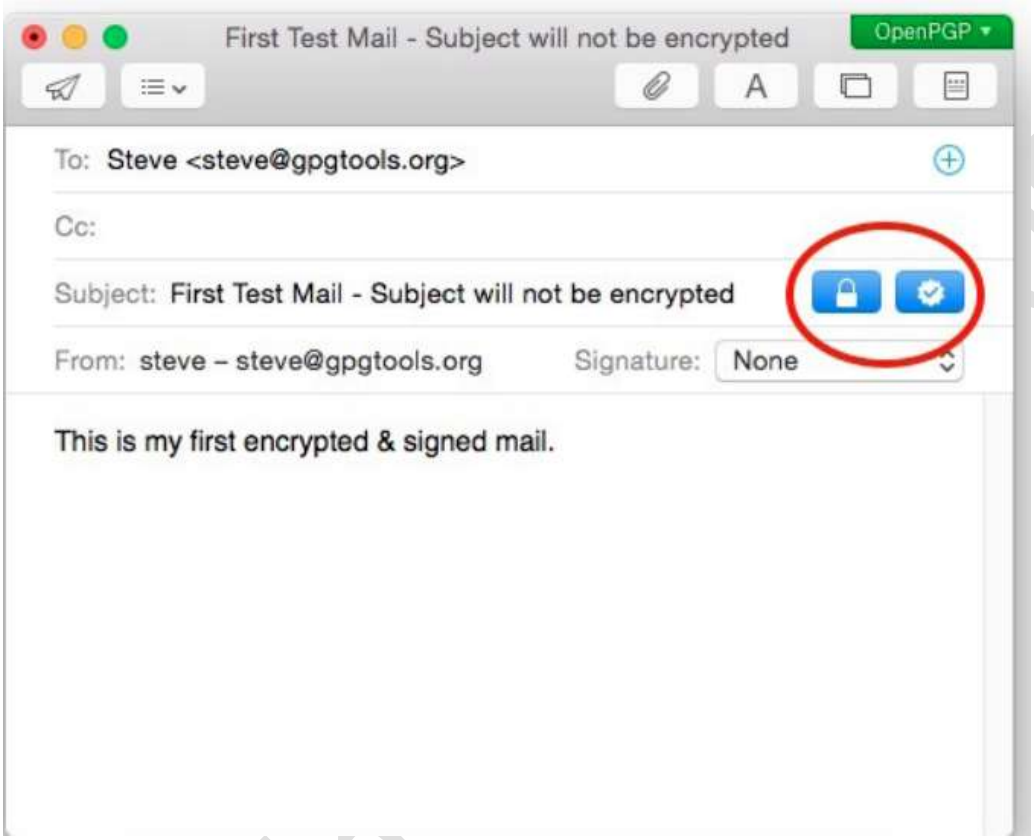
Your key created, we move on to the Apple's Mail program.

Located in the Dock (bottom of your screen) click on the icon and open the program.

Create a new mail, on the right hand side of the compose box, a grayed out 'pad lock' and 'star' can be seen.

In order to send an encrypted mail you will need the address of someone who you have shared a key with. (more on that later).

Compose a mail as you normally would, but before you send, click the grayed out symbols, they should turn blue. Up in the right corner of the email you will see it turn green.



Your recipient will receive the email as before, but if they open it, a popup will appear saying is locked and the key needs to be entered. Also in the inbox it will say, “This email has no content.” There are two small boxes you should check, ‘show typing’ and ‘save to keychain.’ We’ve already talked about Password managers, hopefully you are using it?

Sharing your Key - Once you create a key, from inside of GPGKeychain if you right click on your key, choose the option to ‘export it.’ This will allow it to be emailed, attache it in the compose box. Once they receive it they will need to import it into their encryption program. Which is as easy as clicking on it in the email, GPGKeychain opens and installs the key. When they receive your email their program should have the key and depending on how their program works it should allow you to enter it, and read the email.

Remember, if you have encrypted your email account, but are sending an email to someone that isn’t using it, after you open the compose window, click on the little wheel, it should turn black and

white or gray out. Turning off the encryption. If you don't do this **Before** you being to type, the compose box will not go away, forcing you to close Mail.

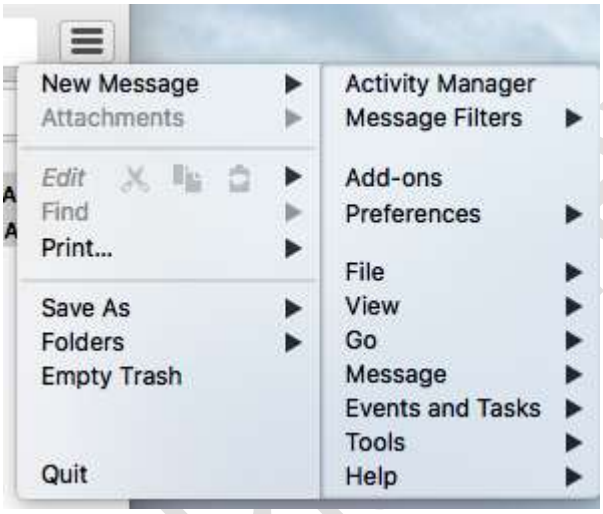
Windows Mail:

(This isn't a tutorial on setting up and using Thunderbird. If you aren't familiar with the program I have included instructions.)

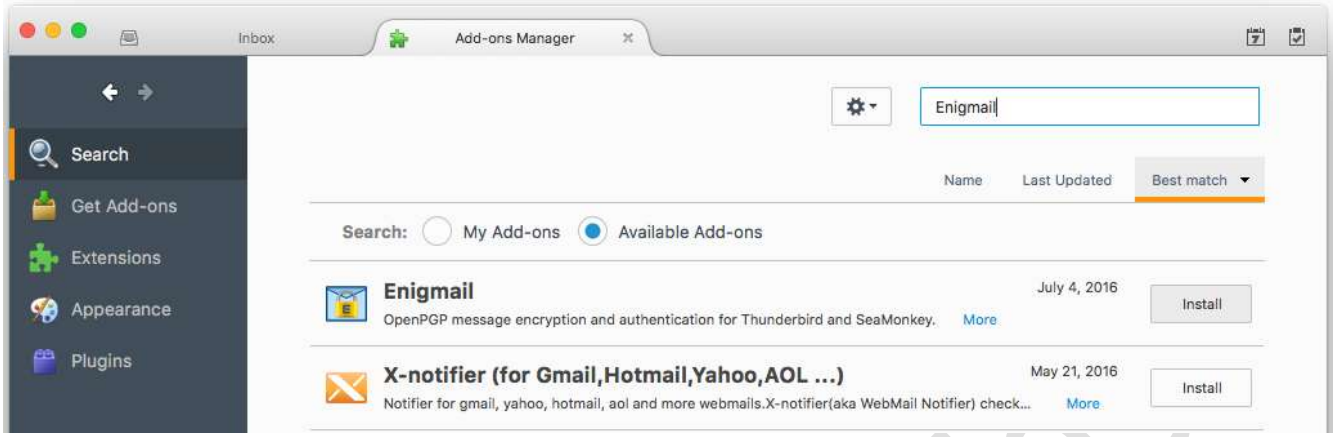
The first thing you need to do is down load and install gpg4win. Here are instructions on how to set it up.

Next download and install Thunderbird, which you can get it here. And instructions on installing it.

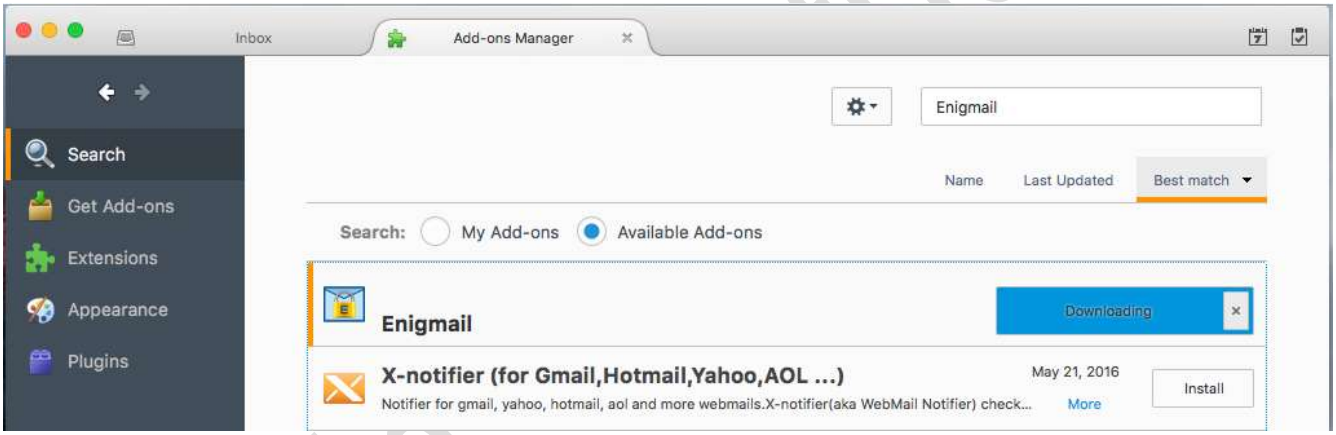
Download and install Enigmail, which is an 'add-on' to allow Thunderbird to use the PGP. After you begin the install process you will need to open Thunderbird, go to the add-on menu. It can be difficult to find in Windows - look for the 'hamburger' menu (3 lines stacked on top of each other).



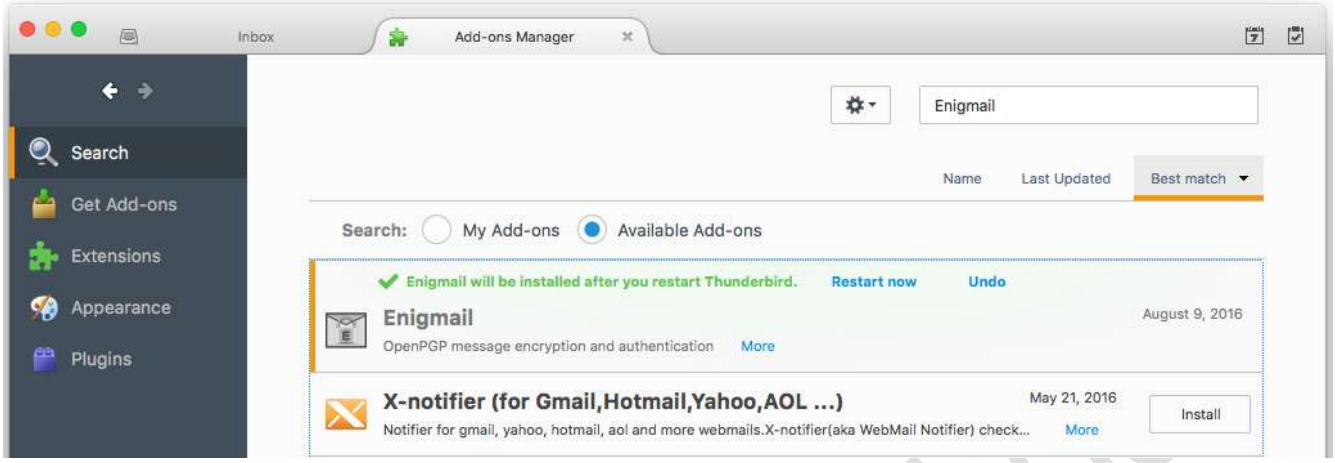
Click on 'add-on'



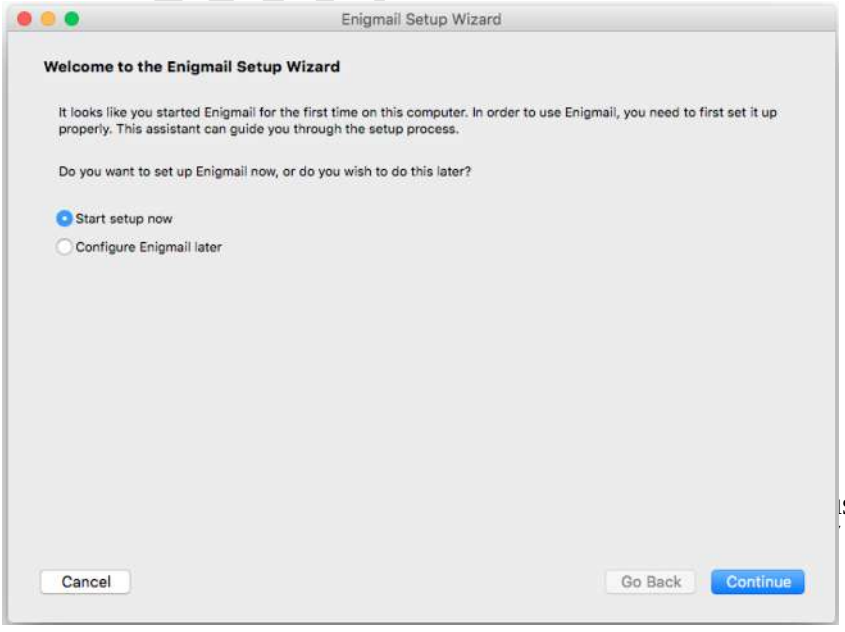
Enter "Enigmail" into the ‘add-on’ search field,



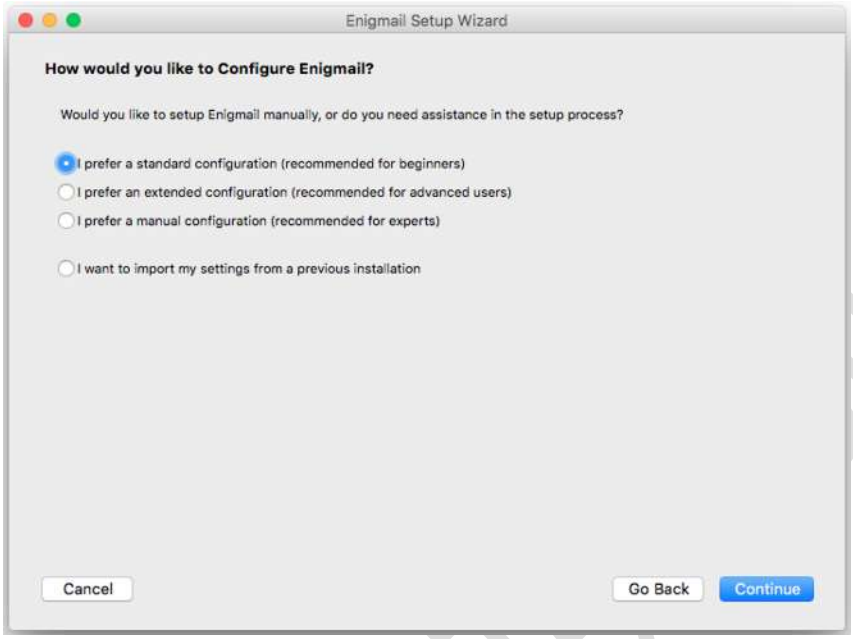
Enigmail will be the first option. Click the ‘Install’ button.



After the Enigmail add-on is installed Thunderbird will ask to restart the browser to activate Enigmail. Click “Restart Now” button and Thunderbird will restart.



When Thunderbird restarts an additional window will open up, starting the process of setting up the Enigmail add-on. Verify the radio “Start setup now” button is selected and click the “Continue” button.



Use Enigmail’s “standard configuration,” Click the “Continue” button.

Your private key and public key will be created. Select the account/User ID you want to use with Enigmail. (If you’d like to add accounts later you can)

Verify again ‘Standard Configuration’ is selected

Click ‘Continue’

The Wizard will now help you to get your ‘secret key’. There are several ways to obtain it:

1.Generating a new ‘secret key’

2.Using an already existing ‘secret key’

The wizard will guide you through the possibilities. If an already existing ‘secret key’ is on your computer, Enigmail will detect it and offer it to use. More likely, as this is the first time you use Enigmail, you will need to generate a new ‘secret key’.

The wizard will do this automatically for you: You will be asked to choose a passphrase to protect your ‘secret key’: you will need the passphrase for signing or decryption of a message. Please repeat the passphrase (just to be sure there's no typo).

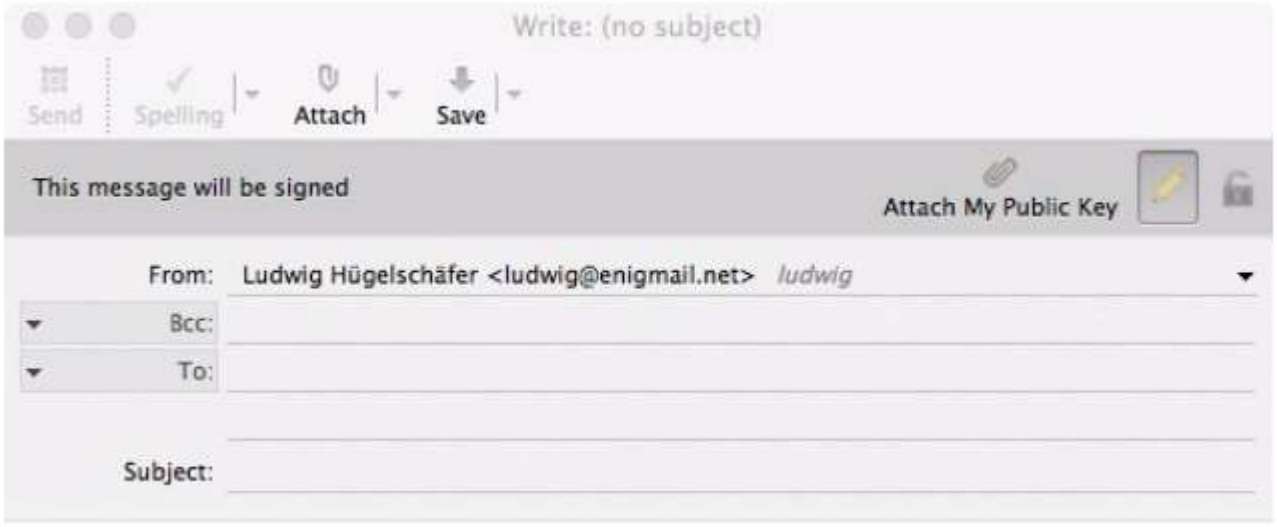
Important: Please make sure, that you remember that passphrase! If you forget it, you will not be able to use your ‘secret key’ any longer!

Once the key has been generated, the wizard will display a confirmation together with the button “Create Revocation Certificate.” Doing this is absolutely necessary! If you lose your key or forget your passphrase, you can use this revocation certificate to revoke your key. Write it down and keep it someplace safe. Or better yet, keep it in a password safe (I will be taking about these in another article.) Click on this button, and you will be prompted for a location on where to save the revocation certificate. Please save it in a safe location outside of your computer!

Clicking “Continue,” closes the window and you’re all set.

How to Use:

Open a new email in Thunderbird. Under the normal toolbar you will notice a new Enigmail tool bar. The toolbar allows you to sign and/or encrypt the message using a single click on the shown icons. On the right end of this extra toolbar, a pen and/or a key icon are displayed, to show if signing and/or encryption is enabled.



You can now send emails. However, in order to allow someone to verify your signature or to send an encrypted message, you must provide them with your public key. You can send your public key as an attachment by clicking the “Attach My Public Key” button in the Enigmail toolbar. In the compose window click on ‘Enigmail’
Click ‘Attach Public key’
Select your key in the ‘Key Selection’ window

To see all the stored keys, yours and the ones you have acquired:
From the menu click ‘Enigmail’
Click ‘Key Management’

Receiving:

When you receive a mail message that has been OpenPGP-secured (signed and/or encrypted), it will appear as such:

Get more information about Enigmail here.

Another option for iOS is Hushmail. They claim to offer site to site encryption through their 'site.' It can be accessed through any browser, with nothing to download. Problems, you have to use their site, where's the transparency, we don't really know how 'secure' their site is. Gmail is secure from point to point, but the email its self isn't secure and can still be read in-between. The other thing about Hushmail is the cost $60 a year.

iOS (iPhones) IpgMAIL:

To be completely honest there is no good solution for PGP for iPhones (iOS). This is the best of the worst solutions.

Dealing with encrypting or decrypting mail on your iPhone is going to take patiences, Go to iTunes and download and install the app.

You can do any of the following to transfer keys from your computer to your phone.

1. Email it to yourself
2. Through iTunes
3. Dropbox

To decipher an email, highlight and copy it. Once its in the clipboard IpgMail should access it and move it into the program.

Inside ipgMail, when you try to access the mail, you will be asked for the key. Once that is entered correctly, you'll be able to view the email. However you will not be able to send it from this program after opening it.

To encrypt, back in Apple's Mail program, you create a new mail then click the IpgMail button and as it's being sent will be encrypted.

Update:
Finding a solution for iOS pgp has been a long tough search. The easiest and cheapest solution is to simply put your messages inside of a txt file. But even here, Apple makes it difficult. The iOS included text editor, strips the text from the file and inserts it into the email. After an exhaustive search, we were able to determine that iEditor, a free text editor, will allow you to attach the text file into your email program. After receiving the email and embedded file you can click on it and the app will open, allowing you to read and edit the file, before attaching it to another email.

(Android)PGP MAIL:
Easy to use, write the email, click the 'cypher' button and its taken care of. You can email the keys to yourself, making deciphering just as easy.

Now you can protect email communications from being read by anyone except their intended recipients, prove an email came from a particular person, and know that you have a good defenses if you are targeted for surveillance or misinformation.