How to: **Encrypted E-mail** over **Tor** [Spring 2015]

*Premise:* this guide is to assist the user in encrypting messages via the open source and widely used PGP standard for asymmetric cryptography and sending said messages over e-mail without compromising their IP address (ie: geographical location) or allowing their ISP to see who they correspond with.

*Wait, what? How? Why?:* When you send an e-mail, you do so over an internet connection that is provided by your ISP (internet service provider) who has access to the information you send over their connection. This includes the content of your correspondence, as well as the recipient and the e-mail provider you used to handle the exchange. Furthermore, the e-mail provider, who handles the actual transmission of the message, can store and consult the same information at any point, or pass it on to a third party. In short, your entire conversation is privy to (for example) Telus & Google and may be stored for any length of time by either corporation and distributed without your knowledge. Lastly, both companies will log your IP address (internet protocol) which quite literally tells them precisely where in the world you are; it's a unique code that identifies a specific internet connection. Think of it as a mailing address for your internet router.

Counteracting this is not as difficult as it may seem. Firstly, one can route one's traffic over the Tor network (torproject.org), assigning you a new IP provided by a relay network of global volunteers. This prevents your e-mail provider from assessing your geographical location. While you probably can't hide that information from your ISP (presumably they have your address as they are responsible for connecting you to the internet in the first place), you can, with the same technology (that is to say TOR), encrypt your traffic so they cannot see anything you do online. While that takes them out of the equation for all intents and purposes relating to this guide, we also want to encrypt the content of the conversation itself to prevent the e-mail provider from maintaining a record of what we said to whom, or to prevent rogue Tor nodes (ie: malicious volunteers) from accessing the content of our communications. That's where PGP comes in; it allows users to garble text and render it indecipherable to all but the specified recipient. The result: your ISP does not know what you are doing online and your e-mail provider knows only that you are sending e-mails to another e-mail address. By using a trustworthy e-mail provider with strong privacy policies, we can further nullify the effects of the latter and finally communicate without fretting over who else might be listening. Openmailbox.org is my provider of choice, but, time allowing for the sing up process to complete, a service like RiseUp.net or Autistici.org may be preferable.

*Requirements:*

* Mozilla Thunderbird e-mail client (mozilla.org/downloads)
* Enigmail add-on (via tools/add-ons in thunderbird)
* Torbirdy add-on (via tools/add-ons in thunderbird)
* Tor Browser bundle (torproject.org)
* Secure e-mail account (like autistici.org)
* PGP implementation (gpgtools.org for mac, gpg4win for Windows)

NB: the software/e-mail provider above are suggested and easy to use, but there are a number of options depending on the operating system you use or the software you prefer. The ones listed above work great on MACs as well as Windows while Unix based systems have much of this software built in.

(see prism-break.org for more options all around, as well as ways to port all of these features to Android devices)

*Methodology*

* Launch the Tor browser bundle and create a new e-mail account at the provider of your choosing. It may take a few days for your application to be processed depending on who you choose. Re Autistici.org: installing their SSL certificate is a good step but it won't persist through separate Tor browser sessions.
* Through GPG keychain assistant (on mac, GPA on windows and linux), create a private and public key pair. (optional: associate the key with your e-mail for better integration with Thunderbird)
* After installing Thunderbird with appropriate add-ons, configure your e-mail account with the parameters specified on your email providers web site.

*Implementation*

In order to send or receive encrypted e-mail with PGP, both parties need to have created a key pair (ie: public and private keys) and exchanged PUBLIC keys only. “GPG keychain assistant” makes both tasks easy. At the top left, select “new” to create a keypair and then select the key you've just created (remember your password! Or use KeyPassX to manage your passwords (recommended!)). With the key selected, hit export and DO NOT select “export secret key”. The outputed file will end in .asc. This is your Public key. You may want to name it something like mypublickey.asc to ensure you don't lose track of it. E-mail this file to your friend and have them e-mail you theirs. Double click the .asc file to import the key.

With their key in your keychain, you can now click the key icon in the 'Compose message' window of Thunderbird to activate encryption for that message. You'll need to match the key you've imported to the contact you are writing to. This is where Thunderbird can automatically detect which key to use if the e-mail associated with the key matches an address in the “to:” field. Furthermore, you can also enable “default rules” for contacts. That is to say, Thunderbird can encrypt the message each time you write to a contact using the key you associated with that contact, or, again, by automatically detecting which key to use if the e-mails match. Default rules can always be deactivated if you don't need to encrypt or the default could be to leave the message in plain text, but that can lead to errors if you forget to encrypt a sensitive messages! So, imo, defaults should be set to the secure option and let the insecure option

rely on your agency.

Torbirdy note: while Torbirdy is installed and enabled, Thunderbird will send all e-mail traffic over a Tor connection. Thus, the Tor Browser needs to be launched for anything to come in or go out. It handles this on its own, but will prevent any e-mails from being sent (or being loaded) if a Tor browser is not running! Click “TorBirdy” (bottom right) to deactivate if needed.

Additional resource: <https://securityinabox.org/en/guide/thunderbird/windows>

More extensive guide for step by step stuff:

[http://en.flossmanuals.net/basic-internet-security](http://en.flossmanuals.net/basic-internet-security/ch035_introduction-to-securing-personal-data/)