Bluestockings PGP Info Sheet – July 28, 2016

To print/save/share this file: `http://bit.ly/1RkHmd3`

Summary

PGP is an email encryption and authentication program that uses the RSA encryption algorithm. Instead of a single encryption key, each PGP user has two keys: a public key and a private key. PGP will use your public key to encrypt messages sent to you. Once you receive an encrypted message, you can use your private key to decrypt the message to plain text. It's safe to give out your public key to people you want to contact—they will need it to encrypt the emails they send to you—but the private key is for you only. The easiest way to set up PGP is to use the Enigmail program (a Thunderbird add-on). Enigmail comes with a key manager, and interfaces between the Thunderbird email client and GPGtools (the program that actually runs encryption and decryption).

PGP Setup

1. Install Thunderbird – `https://support.mozilla.org/en-US/kb/installing-thunderbird`
2. Install Enigmail – `https://enigmail.wiki/Installation_of_Enigmail`
3. Configure Enigmail and generate key pairs & passphrase – `https://enigmail.wiki/Quick_start`
4. Verify that PGP is working with Adele – `adele@gnupp.de`

Setting Up Communication With PGP

1. Swap fingerprint, public keys, and email addresses in person.

a. (less safe) Send each other unencrypted emails with your public keys attached.

2. Load public key and email contact into key manager
3. Send encrypted messages, and verify the person's encrypted email signature against the fingerprint given.

Best Practices

Verifying signatures w/ user fingerprint

For every user, PGP generates a unique fingerprint, which is shared by no one else in the world. This fingerprint is the best way to determine that you are actually communicating with the right person, that your emails aren't being redirected to someone else. To access a user's fingerprint, open the Key Manager, right-click on the user's entry and click *Details*. Check their listed fingerprint against the one that they've given you earlier / in-person.

(Continued on next page)

Set key expiration

In case your key pair is lost or compromised, you should set up an expiration date for your public and private key. Enigmail defaults to generating an expiration date for key pairs—You can check the current expiration in the Key Manager. Right-click your key pair and click *Details*. You can use the *Key Expiry* tab to change the expiration date.

Have a revocation certificate

If you are worried about your key pair being lost or compromised, it's a good idea to generate a revocation certificate, which will allow you to generate a new key pair and will invalidate your previous key pair, so no one else can use it. In the Enigmail Key Manager, go to *Generate → Revocation Certificate* to make a .asc file that can reset your key pair. You should store this file on a different computer from your computer with Enigmail, or on a USB drive, because it will allow anyone who has it to revoke your key pair. If you revoke your key pair, you should email all your contacts to let them know about your new key pair.

Misc / Warning

PGP can't encrypt email headers! Headers will be readable by anyone who can intercept your messages or get access to where the encrypted emails are stored. Make sure your headers don't give away any information that you would prefer to remain secret.

While the contents of your emails can be encrypted by PGP, if your computer is compromised in other ways, adversaries can use software like keyloggers to get your private key. Even though the encryption of PGP is almost impossible to break directly, weak passphrases, insecure internet connections, and unencrypted data storage (on hard drives or remote servers) can help someone find a way to bypass the PGP encryption. Using PGP is just one step towards making your communications safe.
