Email Security Workshop: PGP Encryption & Signing

PART I – download, install, & configure OpenPGP

☐ **1.** Download & Install GPG/OpenPGP*: - Mac/OSX (gpgtools.org)
- Windows (gpg4win.org)

** Most GNU/Linux distributions come with GPG/OpenPGP pre-installed. For Mac or Windows it is essential to regularly check the websites for updates!*

☐ **2.** Restart your computer

☐ **3.** Download & Install Thunderbird (mozilla.org/en-US/thunderbird)

☐ **4.** Launch Thunderbird — email account setup starts automatically, or start it from the menu: ☰ *File → New > Existing Mail Account*

☐ a) select "*Skip this and use my existing email*"

☐ b) Enter your name as others will see it, your Email address & Password
** If you don't see "Configuration found at email provider" - please ask for help!*

☐ c) Select *IMAP (remote folders)*, click *Done*.

☐ d) Sync your email: ☰ *File → Get New Messages for > All Accounts*

☐ **5.** Install the enigmail plug-in from the Thunderbird menu:
☰ *Tools → Add-ons*; Get Add-ons, search "enigmail", click *Install*

☐ **6.** Restart Thunderbird

PART II – make a PGP key pair

☐ **7.** Enigmail Setup Wizard starts automatically to generate a key pair: your private ("secret") key and your public key ("public lock"). Select "*Start setup now*", then "*I prefer a standard configuration*." In the future you can make new key pairs from the menu:
☰ *Enigmail → Key Management; Generate → New Key Pair*

☐ **8.** Enter the name and email address you entered in Thunderbird

☐ **9.** Enter a **strong passphrase** – use Diceware or a reliable password manager: world.std.com/~reinhold/dicewarewordlist.pdf

☐ **10. Write down** this passphrase & keep it safe, away from your computer

☐ **11.** Generate a revocation certificate & save it to a folder on your computer—you should copy it to a USB stick or backup drive, since you'll need this if you ever forget your passphrase or lose your key. You'll be prompted for your passphrase. Click *next* then *Done/Finish*

☐ **12. Back up your key pair** to a **safe & secure** location (ideally, an encrypted USB stick): ☰ *Enigmail → Key Management*; right-click on your key, select "*Export Keys to File*", choose "*Export Secret Keys*"

PART III – exchange, verify and sign public keys

☐ **13.** Compose a new email message (ctrl-N or command-N) to a comrade. In the Enigmail toolbar in the compose window above the "From" field select "*Attach My Public Key*". In red it will read "**This message will be unsigned and unencrypted**" – that is OK. Send the email, and ask your comrade to also follow this step and send you their public key.

☐ **14.** Open each other's email messages. Right-click the attached file (0x#######.asc) and select "*Import OpenPGP key*"

☐ **15.** Verify that you have your comrade's authentic public key. Each of you will reveal the key's fingerprint: ☰ *Enigmail → Key Management*, right-click the comrade's key and choose "*Key Properties*". If the imported key isn't listed, in this window menu: *File → Reload Key Cache*

☐ **16.** Read the entire fingerprint aloud and ask your comrade to confirm that it matches theirs — if exchanging keys remotely, read fingerprints over the phone. **Do not skip this step:** otherwise, an adversary could substitute a counterfeit public key to read or modify your emails!

☐ **17.** If the fingerprints match: in the "*Select action ...*" or "*Certify*" drop-down menu, choose "*Sign Key*" (in the pop-up window, "*Key for Signing*" is your own key). Select "*I have done very careful checking.*"

☐ **18.** Ask your comrade to verify your public key (following steps 15-17)

☐ **19.** Write a new email message to your comrade. When the lock icon is selected/highlighted & in the locked position, it will be encrypted.

PART IV – ensure email authenticity

☐ **20.** Email messages can easily be falsified. PGP can be used to validate email sender and contents. In the email compose window menu: *Enigmail → Preferences → Signing/Encryption Options...* under "*After Application of defaults and rules*" tick the box beside "*sign encrypted messages*". Your encrypted emails are now signed by default.

☐ **21.** Signed emails in Thunderbird/enigmail are indicated in the header:
* **[green] Good signature from ...** – everything checks out.
* **[cyan] UNTRUSTED Good signature from ...** – looks good, but you will need to verify/fingerprint (and sign) your contact's public key.
* **[red] Bad signature ...** – something is horribly wrong. Get in touch by a channel other than email to discuss this and check their key.

☐ **22.** This is especially useful for sharing public keys that you have verified/fingerprinted. Compose an email to a comrade who has verified your public key. In the compose window menu: *Enigmail → Attach Public Key...* select relevant keys. When receiving an email with the header "Good signature from ..." any attached keys can be trusted.