PEILC 2016 Workshop: Making Email Encryption Work for Security and Confidentiality

PART I – download, install, & configure OpenPGP

☐ **1.** Download & Install OpenPGP:
– for Apple/OSX (GPG Suite at gpgtools.org)
– for Windows (gpg4win.org – install all components)

☐ **2.** Restart your computer

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

☐ **4.** Launch Thunderbird (Wizard starts automatically: select "Skip this and use my existing email" or, without the Wizard, from the menu: *File* → *New* → *Existing Mail Account*)

☐ a) Enter your name as you would like it to appear, your Email address & Password
* *If you don't see "Configuration found at email provider" – please ask for help!*

☐ b) Select IMAP (remote folders), click Done

☐ c) Begin syncing your email (*File* → *Get New Messages for* → *All Accounts*)

☐ **5.** Get the enigmail extension (*Tools* → *Add-ons*; Get Add-ons, search "Enigmail", click Install)

☐ **6.** Restart Thunderbird

PART II – make a PGP key pair

☐ **7.** Enigmail Setup Wizard will start automatically to generate a key pair: your private ("secret") key and your public key ("public lock") – "Start setup now", then "I prefer a standard configuration"
* *if the Wizard doesn't appear, select* Enigmail→Key Management*; then* Generate→New Key Pair

☐ **8.** Enter a name you want to use and the email address you used in Thunderbird

☐ **9.** Choose a **strong passphrase** – e.g. with Diceware (world.std.com/~reinhold/dicewarewordlist.pdf)

☐ **10.** **Write down** this passphrase & keep it separate from your computer and backups

☐ **11.** Generate a revocation certificate, save it to your disk & copy it to a USB key

☐ **12.** Click next then Done/Finish; Close the Add-ons Manager tab

☐ **13.** **Back up your key pair** to a **safe & secure** location: *Enigmail→Key Management*; right-click on your key, select "Export Keys to File", choose "Export Secret Keys"

PART III – Exchange, fingerprint and sign public keys

☐ **14.** Write a new email message (ctrl-N or command-N)

☐ **15.** Select "Attach My Public Key" and send an email to your neighbor

☐ **16.** Send an email to a neighbor

☐ **17.** Open an email from your neighbor

☐ **18.** Right-click on the attachment (0x########.asc) and choose "Import OpenPGP key"

☐ **19.** Verify that you have your neighbor's correct key: *Enigmail→Key Management*, right-click on their key and choose "Key Properties"
* *If you don't see your neighbor's key, select* File→Reload Key Cache

☐ **20.** Read the whole fingerprint aloud and have your neighbor confirm it by right-clicking and choosing "Key Properties" to reveal their own key's fingerprint (if you are sharing keys remotely, you can read the fingerprints over the phone). **Please don't neglect this step, since an adversary could substitute a false key, and read or modify your emails!**

☐ **21.** Once you've verified that the fingerprints match, in the "Select action …" box, choose "Sign Key" – in the pop-up window, "Key for Signing" should be your key. Select "I have done very careful checking" (since you've done this in person). Check the box "Local signature (cannot be exported)". You will be prompted for your passphrase.

☐ **22.** Now write a new email message, the lock icon should be selected and closed, this means it will be encrypted to your neighbor.