PEILC 2016: Email Encryption for Security and Confidentiality

PART I – download, install, & configure OpenPGP

☐ **1.** Download & Install OpenPGP: – Apple/OSX (gpgtools.org — GPG Suite)
– Windows (gpg4win.org)

☐ **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: [*Alt-F*] or ☰ *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." Make a new key pair anytime from the menu:
☰ *Enigmail→Key Management; Generate→New Key Pair*

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

☐ **9.** Choose a **strong passphrase** – use Diceware or similar method:
world.std.com/~reinhold/dicewarewordlist.pdf

☐ **10. Write down** this passphrase & keep it separate from your key

☐ **11.** Generate a revocation certificate & save it to a USB stick. You'll be prompted for your passphrase.

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

☐ **13. Back up your key pair** to a **safe & secure** location (USB stick):
☰*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 a neighbor

☐ **16.** Open an email from the same neighbor

☐ **17.** Right-click the attached file (0x#######.asc)→"Import OpenPGP key"

☐ **18.** Verify that you and have your neighbor's authentic key by revealing its fingerprint: ☰ *Enigmail → Key Management*, right-click their key, choose "Key Properties" (** If the key isn't listed,* File→ Reload Key Cache)

☐ **19.** 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 exchanging keys remotely, read fingerprints over the phone). **Please don't neglect this step: an adversary could substitute a counterfeit key to read or modify your emails!**

☐ **20.** If the fingerprints match: in the "Select action ..." 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." and check the box "Local signature (cannot be exported)." Enter your passphrase.

☐ **21.** Repeat steps 18-20 to verify your neighbor has your authentic key.

☐ **22.** Write a new email message to your neighbor. Ensure the lock icon is selected & in the locked position, indicating it will be encrypted.

PART IV – ensure email authenticity

☐ **23.** You can also use PGP to confirm the author of an unaltered message. Write an email and select the pencil icon (between the lock and "Attach my public key"). Using your public key the recipient can:
a) confirm you (or someone else in possession of your private key and passphrase) authored the message;
b) be certain the message is identical to the email that was signed.

☐ **24.** While this guarantees that your message has not been altered from its original text, be sure that this is what you want to do: a signed email is unambiguously linked to your private key. Plausible deniability ("my email has been hacked") is rendered unconvincing.

☐ **25.** Signed emails in Thunderbird/enigmail are indicated by the header:
* [green] "Good signature from ..." – everything checks out
* [cyan] "UNTRUSTED Good signature from ..." – looks good, but you still need to fingerprint (and sign) your contact's public key
* [red] "Bad signature from ..." – something is horribly wrong. Get in touch by a channel other than email and ask if this email is truly theirs
* [grey] indicates an unsigned, decrypted, message