GPG/PGP encryption for emails using Thunderbird & enigmail: Σημειώσεις από το **CryptoParty**

Guides:
https://skytal.es/wiki/Οδηγός_εγκατάστασης_και_χρήσης_του_Thunderbird_με_Enigmail
https://securityinabox.org/en/guide/thunderbird/windows
http://www.tcij.org/resources/handbooks/infosec/chapter-5-email

Software:

Thunderbird (Windows, OS X, Linux)	https://www.mozilla.org/en-US/thunderbird/
Enigmail (encryption plugin for Thunderbird)	https://www.enigmail.net/home/index.php
GPG for windows:	http://gpg4win.org/download.html
Ubuntu/Debian	apt-get install gpg icedove-enigmail

https://skytal.es/wiki/Ασφαλής_επικοινωνία_μέσω_email
The problem: Your non-encrypted emails go through the internet almost like a postcard in snailmail: Not only the recipient, but other people can read it too & potentially change it. The email contents, metadata and attachments are probably mined (& stored). With **GPG encryption** the contents (and attachments, if you choose so) of your emails, appear like gibberish to 3rd parties and can be read only* by the intended recipient.

*provided s/he safeguards her/his private GPG key & PC

- Security/privacy is a process
- Using cryptography is legal, but not in every country
- CryptoParty is for beginners
- Journalist or activist? See EFF, Tactical Tech, AccessNow
- The recipient must have a GPG key-pair
- There is a trade-off with convenience

With GPG encryption you can have more privacy – not anonymity.

Only the content of your message is encrypted. Important information remains unencrypted and can be read by third parties, such as:
email subject line (never put sensitive info here)
time and location
email address/identity of the sender and recipients
attachment file names

You can use GPG encryption with your current mail account/provider.
Gmail specific: If you decide to use your Gmail account, you first have to login to your Gmail account using a browser from a PC (not mobile/tablet), go to **https://www.google.com/settings/security/lesssecureapps** and "Turn on" access for "less secure apps". Otherwise, Thunderbird won't connect.

What we will do during this workshop:

We will use the Thunderbird email client with the Enigmail plugin to:

1. Generate a GPG key–pair for our email account. This comprises of:

a 'private' key. Never send or allow access to it - **back it up securely.**

a 'public' key which you can share with anyone & you can upload to a keyserver

! Each key-pair has a unique fingerprint (string of 40 characters).

Important info for the initial generation of your keypair

You will generate a strong primary key (or transition to a stronger key if you have been using an old one)

It is recommend (March 2016) to make a 4096bit RSA key

Set an expiration date less than 2 years

Your private key can be compromised. An expiration date of a few years limits the value of stealing your keys. You can **always extend your expiration date, even after it has expired** if you have access to the secret key**.** This "expiration" is actually more of a safety valve or "dead-man switch" that will automatically trigger at some point. material, you can untrigger it. The point is to setup something to disable your key in case you lose access to it (and have no revocation certificate). **Set a calendar event to remind you about your expiration date.**

Generate a revocation certificate – back it up securely

If you forget your passphrase or if your private key is compromised or lost, the only hope you have is to wait for the key to expire (this is not a good solution), or to activate your revocation certificate by sending it to the keyservers. Doing this will notify others that this key has been revoked. A revoked key can still be used to verify old signatures, or decrypt data (if you still have access to the private key), but it cannot be used to encrypt new messages to you.

Do not include a "Comment" in your User ID

You probably don't need or want it, and having a comment field makes it harder for people to know what they're certifying.

2. Set a passphrase for your private key– remember it.

Your passphrase unlocks your private key and permits it to be used, in conjunction with your public key, to send and receive encrypted email. It should be at least 21 characters in length, should contain UPPER and lower case characters, as well as symbols (&$"{@).

3. Generate a revocation certificate – back it up securely

If you forget your passphrase or if your private key is compromised or lost, the only hope you have is to wait for the key to expire (this is not a good solution), or to activate your revocation certificate by sending it to the keyservers. Doing this will notify others that this key has been revoked. A revoked key can still be used to verify old signatures, or decrypt data (if you still have access to the private key), but it cannot be used to encrypt new messages to you.

4. Setting up Thunderbird:

Save drafts at local folders

Send emails in plain text, as HTML does not encrypt we

See the links to the guides (top of this document) for more info

5. Upload your public key to a keyserver (optional)

6. Import the public key of a friend & verify it with the full fingerprint that s/he has given you in person (1st time only)

<u>**Check key fingerprints before importing.**</u>

Want to use your friend's public key to send them an encrypted email for the first time? You found your friend's public key at a keyserver and you are ready to import it? **Do not blindly trust public keys from keyservers. Verify them with the full fingerprint in person.**

You can download public keys from a keyserver. However, anyone can upload keys there and there is no reason that you should trust that any key you download actually belongs to the individual listed in the key. You should therefore **verify** with the individual owner the full key fingerprint of their key. You should do this verification in real life (or with voice over the phone if you know the other person's voice & you or s/he is not in high risk) .

Don't rely on the short or long Key ID – use the full fingerprint.

- Short OpenPGP Key IDs, for example 0×2861A790, have been shown to be easily spoofed by another key with the same Key ID.
- Long OpenPGP Key IDs (for example 0xA1E6148633874A3D) are

trivially collidable, which is also a potentially serious problem.

If you want to deal with a cryptographically-strong identifier for a key, you should use the full fingerprint. You should never rely on the short, or even long, Key ID.

7. Send your first encrypted email :)

- When you **send** an email, you encrypt it with the YourFriend's public key.
- When you **receive** an encrypted email, you decrypt it with your private key (& you are asked for its' passphrase). You verify the signature of the encrypted email (if it is signed), with YourFriend's public key.

What you can use GPG for with your emails

There are three basic functions you can perform using GPG: **signing**, **encrypting** and **verifying**. You can sign an email and choose not to encrypt it (e.g. if you will send it to a public mailing list).

Encrypting: To encrypt a message, you need the public key of the recipient. You do not need a passphrase or even a gpg key of your own to encrypt something. However, most programs will also encrypt anything to your own public key when sending. Otherwise, once you encrypt a message, you would no longer be able to read it. Once it is encrypted, the contents of the email are no longer viewable in transit. **However, the subject, sender, and recipient are still visible.**

Signing: When you sign something, you use your private key and your passphrase to generate a signature block that is appended to the item you are signing. This signature block is generated from two things: (1) a numerical value computed from the contents of the message and (2) your private key.

Verifying: When someone receives something that has been signed, they can verify it using the public key with which it was encrypted. The public key could be downloaded from a keyserver, or perhaps emailed by the sender. Verifying establishes two things —> (1) the message was signed by someone who has access to the associated private key and (2) the contents of the message were not modified in transit.

Find out about upcoming events:
https://cryptoparty.in/Athens

Version 1605v3