**COMPUTING SUBJECT:** Secure emails

**TYPE:** Assignment

**IDENTIFICATION:** PGP-EMAIL

**COPYRIGHT:** *Michael Claudius/Homayoon Fayez*

**LEVEL:** Medium

**TIME CONSUMPTION:** 1-2 hours

**EXTENT:** 50 lines

**OBJECTIVE:** Thunderbird, GnuPGP, Enigmail, Certificates

**PRECONDITIONS:** Computer Networking Ch. 8.5,
 Network Security Ch. 8.

**COMMANDS:**

**IDENTIFICATION:** PGP-EMAIL/MICL&MOFA

Mission

You are to make a secure email communication. This we shall do in six steps:

1. Install Gpg4win (GNU Privacy Guard for Windows)
2. Enable IMAP for your gmail account. It can be found in the settings.
3. Install Thunderbird
4. From Thunderbird search and install the Enigmail plugin
5. Create a key pair (public&private) certificates
6. Send and receive encrypted and signed emails

Purpose

The purpose of this assignment is to install tools providing secure email communication and use them. This is done by setting up an email client using PGP (Pretty Good Privacy), which can both encrypt/decrypt and sign e-mails and documents.

*Useful links*

<https://en.wikipedia.org/wiki/Mozilla_Thunderbird>

<https://www.thunderbird.net/en-GB/>

<http://www.enigmail.net/index.php/en/>

<https://www.gnupg.org/>
GnuPG (Gnu Privacy Guard) is a complete and free implementation of the OpenPGP standard as defined by [**RFC4880**](https://www.ietf.org/rfc/rfc4880.txt) (also known as *PGP*). GnuPG allows to encrypt and sign your data and communication, features a versatile key management. GnuPG also provides support for S/MIME and Secure Shell (ssh).

<https://www.gpg4win.org/>
For file and email encryption. Gpg4win (GNU Privacy Guard for Windows) is Free Software and can be installed with just a few mouse clicks.

Assignment 1: Install GnuPrivacyGuard

Download and install Gpg4win from <https://www.gpg4win.org/>

A few clicks and its done. Check Kleopatra but **don’t** create key-pairs!

Assignment 2: IMAP in email settings

Enable IMAP for your Gmail account. It can be found in the settings.

Assignment 3: Install Thunderbird email client

Download and install Thunderbird from <https://www.thunderbird.net/en-GB/> en-US

On another link, there is also a Danish version, **DON’T** use that!.

In the mail account setup, remember to choose as follows during installation:

1. Remove tick as Thunderbird as email
2. Thunderbird is **not** a set up standard/default email account
3. Use one of your normal email accounts (e.g. Gmail) instead
4. Use IMAP
5. Remove the tick mark at, “use Thunderbird as my default e-mail client”
6. If you get a pop up saying “use Thunderbird as the default client”

Choose “Skip Integration”

And you will get something like this:



*Skip integration!*

*If there are problems with the installation look at the Appendix A at the end of the assignment.*

4. Install Enigmail

To install the Enigmail plugin from your thunderbird email client ypou start to

Choose: Burger-menu top-right corner

Choose: Display Thunderbird Menu-> Add-ons manager -> Add-ons

Choose: Extensions

Then:

* 1. Search for Enigmail - and - find it on the list - usually the first one
	2. Click on Add to Thundirbird
	3. Click Add
	4. Click Ok
	5. Click on Restart

Install the plugin and then click on Restart.

On the way you will either see



If you already installed GnuPGP.

 Or you will be prompted to install GNUPGP from the OpenPGG Setup Wizard:



Choose install.

Finally, we are ready. Close all add-ons.

Assignment 5. Generate keys (public and private)

Make sure that a key-pair (certificate) is created for you. You can check it by either opening Kleopatra

If you you don’t see aKey-pair then create one!
Select Burger Menu in Thunderbird

Select: Enigmail -> Key Management -> Generate

Choose: Create a New Key Pair.



State the passphrase, if you like. Check out Advanced and finally click on Generate key.

6. Send signed and encrypted email to yourself

Select write:



Use your own email address as receiver.

Encrypt message: click Padlock.

Sign the message: click Pencil

Can you r*emember your passphrase.!, IF you generated one?*

Finally Send it.

Assignment 7: Receive an encrypted and signed e-mail from yourself.

Look at the inbox and decrypt the message and verify the signature.

For fun also see how it looks in your normal email.

Assignment 8: Export your public key to a PGP server (can be tricky)

Select: Enigmail -> Key Management -> Keyserver -> Upload Public Keys



Assignment 9: Import a friend's public key from a PGP server (can be tricky)

Need to know his keyserver ! Ask him for the possibilties. Or search…

Select: Key management -> Search keys.

Tip: Probably the Keyserver address is the same as yours:

 “vks://keys.openpgp.org”

Or old versions using:

“pool.dks-keyserver.net”.

Remember to remove the hkps://hkps in front of “pool.dks-keyserver.net”



Choose the key to import



Click Ok.
Now the key certificate will be listed in the Keyserver

10: Send and receive e-mails to / from him (your friend from before)

Also you can export and send your public key to your friend by mail

Assignment 11: Other PGP users
Try to import/sign the keys from other PGP users you know

Assignment 12: Send encrypted files

Look in PGP intro to encrypt a document (installed with the commercial PGP)

**Appendix A**

Problems with Gmail and some other providers

Several possibilities:

Use the local LAN at Maglegårdsvej instead of Easj Secure

Change settings in Gmail to accept use of Imap.

Also change to accept more unsecure apps.

Cannot see OpenPGP in menu

You have downloaded another version of Thunderbird

Just Select/Use Enigmail instead

Installation says not accepted passwords

Don’t care just click on Cancel and it will be there, hopefully….

Done didn’t work

Choose Manually.>Done instead