

# Laboratory assignment 1

## Gnu Privacy Guard (GPG)

April 2, 2008

### 1 Purpose

In this laboratory assignment you will learn how to setup and use gpg to sign and encrypt emails. The tool you will use is Gpg4win[[gpg08](#)] (GNU Privacy Guard for Windows), which is an free email encryption software for windows including the following components: GnuPG, GPA, WinPT, GPGol, etc.

### 2 Preparations

Recommended reading is specified as below.

1. An introduction to Cryptography (Course book, Chapter 5.1)
2. Gpg4win for Novices (<http://www.gpg4win.org/handbuecher/novices.html>)

### 3 Reporting

To pass this assignment you have to send an encrypted and signed email to your teacher at [yan.wang@hh.se](mailto:yan.wang@hh.se). The message should contain a report(2-3 pages) with at least the following items:

1. **Your names and IDs;**
2. **Introduction** giving an overview of the assignment and content of the report;
3. **Answers** for the questions that you can find in the next Section Questions;
4. **Conclusions** containing your reflections about the email security problem and the assignment;
5. **Appendix** containing your public key.

## 4 Questions

1. When GPG has finished creating your keys, it will print out a summary in the *Detail* tag. What does "Owner Trust: Ultimate" mean?
2. What is the fingerprint of your key?
3. Will you use GPG in the future? Why or why not?
4. Explain briefly how encryption and decryption works in PGP (not GPG). What are the five principal services provided by PGP?
5. How does signing work? What is the utility of a detached signature?

## 5 Exercises

The following exercises are to be done in the laboratory.

### 5.1 Create your new key with GPG.

1. Start the GPA program (GNU Privacy Assistant) from your Windows start menu.
2. Generate a new key pair by inputting your name, email address and a passphrase to protect your key. To pick up a good passphrase, you can have a look on <http://world.std.com/~reinhold/diceware.html> to get some suggestions.
3. Create a backup copy of your new key. You can store the backup in H: disk, so that you can reuse it from another computer. You can also create back-up copies later by *Key – Backup*.
4. Edit your key if necessary by setting, for example, new validity period, new passphrase.

### 5.2 Export your public key with GPG.

Before you can encrypt an email for other students, you need to ask their public keys (they need yours as well).

1. Select your key on your list.
2. Click Export of the GPA menu.
3. Choose a file to export your key, e.g., YournamePubKey.txt.

### 5.3 Send your public key to other students.

1. Open YournamePubKey.txt with a text editor.
2. Copy and paste all the content including "—BEGIN PGP PUBLIC KEY BLOCK—" as the content of your email.
3. Send the mail to one or more students.

### 5.4 Receive others' keys

If the received message started from "—BEGIN PGP PUBLIC KEY BLOCK—", skip the first 3 steps.

1. Start the WinPT program from your Windows start menu.
2. Copy the encrypted message into clipboard
3. Decrypt the message by right clicking WinPT icon - *clipboard* - *decrypt/verify*. You will be asked for the passphrase. The decrypted result will be in clipboard.
4. Copy from "—BEGIN PGP PUBLIC KEY BLOCK—" to "—END PGP PUBLIC KEY BLOCK—" and paste it in text format to a file e.g., OthernamePubKey.txt.

### 5.5 Attach a key to your key ring

1. Start the GPA again, if you shut it down.
2. Click *Keys* then *Import keys* of the GPA menu to import OthernamePubKey.txt.
3. Import OthernamePubKey.txt into GPG.
4. Ask the fingerprint from senders in person to make sure that the key you get actually belongs to them.
5. Sign their key, if the fingerprints are identical.
6. Set the owner trust of their key.
7. Export their key into another file and email it back to the owners.

***Your public key have to be signed by two groups to pass this lab.***

### 5.6 Receive your key back

Import your key back into your key ring, which will update the original key with others' signatures that vouches the key validity.

## 5.7 Send your report to your teacher

1. Fetch your teacher's public key from  
<http://www2.hh.se/staff/yanwan/networksecurity/lab/Yanpublickey.txt>
2. Import it to your key ring.
3. Encrypt your report by using this key and send it by email.

## References

[gpg08] <http://www.gpg4win.org/handbuecher/novices.html>, April 2008.