

ECE646 – Fall 2007

Lab 1: Pretty Good Privacy

PLEASE READ THE FOLLOWING INSTRUCTIONS CAREFULLY:

1. PART I, must be performed before the lecture on **Wednesday, September 26th**.
2. A LAB REPORT must be handed in at the beginning of class on **Wednesday, October 3rd**.
3. You are required to address all the questions listed in this manual, in your final report.
4. All e-mails exchanged with other students as a part of this lab should be CC: to **gmuece646@gmail.com**

In order to perform the following lab, you are required to have an understanding of **LECTURES 1-4**

and have read the following sections:

- **Stallings, 4th ed., Chapter 15.1 and appendices 15 A, B, C, or**
- **Stallings, 3rd ed., Chapter 15.1 and appendices 15 A, B, C, or**
- **Stallings, 2nd ed., Chapter 12.1 and appendices 12 A, B, C and**
- **Additional slides posted together with this instruction.**

PART I

1. INSTALLATION

In order to complete this lab you have to install Gnu Privacy Guard on your personal computer/notebook or you can use the GPG installation in some GMU ECE Labs.

Unix or Linux Users might already have GPG installed on their systems. Otherwise, you can download and install it from: <http://www.gnupg.org/>

Windows users can download Gpg4win Light v1.1.1 from: <http://www.gpg4win.org/>. Select all components including **Sylpheed-Claws**. GPG should be ready to use after you reboot. You will find a GnuPG folder installed in your Start Menu. GnuPG FAQ will serve as a manual for GnuPG command line utilities. The application that you will be using for the lab is called **WinPT - Windows Privacy Tray**.

Labs: You may use computers located in the GMU ECE labs, ST2 Rooms 203 and 265, in order to complete tasks described in Sections 2 through 7.

2. KEY GENERATION

First, you need to create an email account on any of the free mail service providers, such as Yahoo!, Hotmail, Gmail, etc. The recommended service provider is GMAIL.

YOU ARE NOT ALLOWED TO USE YOUR GMU EMAIL FOR THIS LAB!!

Generate your private-public key pair, and associate it with your full name and a newly established e-mail address. Instructions for GnuPG key Generation are as follows:

1. Start the program WinPT.
2. Select: **Generate a new key pair**.
3. Enter your full name, e.g. John Smith and your e-mail address.
4. Enter a passphrase. The passphrase should be long but easy to memorize and hard to guess by others.
5. The select to create a backup copy which will generate a backup of your public key and a backup of your secret key.
6. Then WinPT will close and install itself in the Windows tray on the bottom right of your screen. Double click the WinPT icon and WinPT will open and show your key.

Instructions to add your public key to the GPG Global Directory:

1. Right-click your key and select "Send to Keyserver"
2. In the following dialog make sure that <http://subkeys.pgp.net> is selected.

Questions:

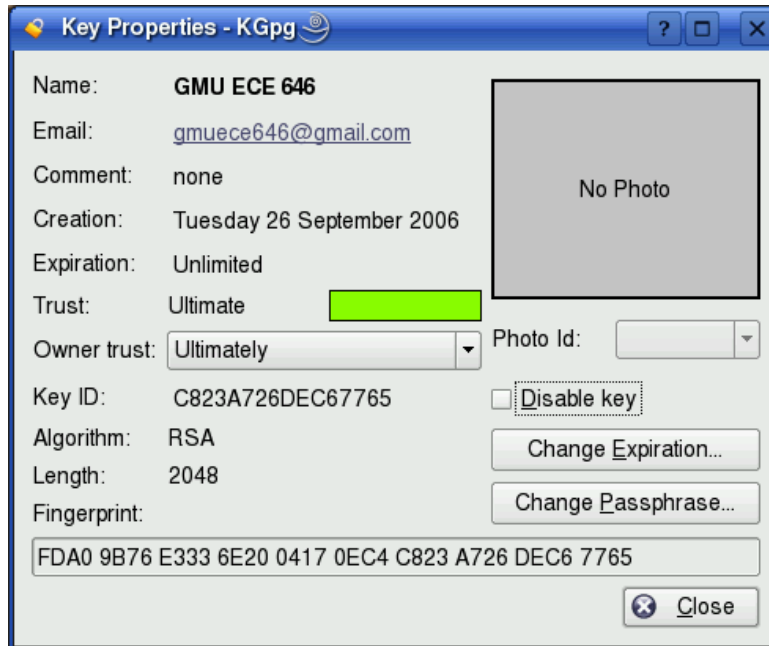
1. List all the steps of the process performed so far.
2. In each step, clearly identify all your choices with a brief explanation of the reason behind them e.g. type of key, etc.
3. How is the key pair stored? Can you copy/cut/delete these files?
4. How can you export your public/private keys to another machine?

3. KEY DISTRIBUTION: KEY EXCHANGE IN CLASS

Prepare your public key card containing the following information:

- Your Name
- Email address: should be same as the one used to generate the public and private Key
- Public key ID
- HEX fingerprint of your public key

All fields should have exactly the same value and format as the corresponding fields listed by the GPG program.



- Bring four copies of your public key card, along with your GMU ID to the next lecture. Submit one copy to the instructor, and present your GMU ID for verification.
- Exchange public key cards with three of your classmates (preferably one friend and two "strangers"). If you do not know their names, ask them to show you their GMU IDs. The group of three classmates you exchanged public key cards with is your DIRECT TRUST GROUP.

AVOID FORMING CLOSED GROUPS OF 3 OR 4 PEOPLE WHO ALL EXCHANGE PUBLIC KEY CARDS AMONG ONE ANOTHER

PART II

4. KEY DISTRIBUTION: KEY EXCHANGE BY EMAIL

- Send your own public key to all members of your DIRECT TRUST GROUP by email. Please remember to CC: your communication to **gmuece646@gmail.com**
- Import public keys of your DIRECT TRUST GROUP to your public key ring.
- Verify the public keys fingerprints of imported keys against the fingerprints listed on the cards, you received from your classmates.
- Sign the keys of your DIRECT TRUST GROUP.

Questions:

5. Draw a hierarchal diagram showing your public key ring web of trust.

5. ENCRYPTION

- Prepare a relatively large text file to be sent to **ONE OF THE MEMBERS** of your DIRECT TRUST GROUP in the encrypted form.
- Encrypt this file, using the receiver's public key, and then again separately using your public key, with the following options
 - a. Default options,
 - b. Text output
- Send the obtained files to the intended recipient.
- Investigate the encrypted files, looking at their contents and length.

Questions:

6. How would you explain the relations between the length of the file before and after the encryption for each set of options?
7. What subset of ASCII characters is used within an enciphered message for each set of options?
8. What transformations are performed during the encryption for each set of options?
9. What keys are required to perform these transformations? Where are these keys stored? Which of these keys are protected using a passphrase?
10. Can you change the order of these transformations without affecting the program functionality or security?
11. Which algorithms are used during each of these transformations? What are the key sizes used in each of these algorithms?
12. If you send an encrypted file to the recipients what kind of security service are you using?

6. DECRYPTION

Try to decrypt all files you have created based on the instructions given in Section 5, and files you have received from the members of your DIRECT TRUST GROUP.

Questions:

13. How can you be sure of the authenticity and integrity of the file?
14. How can the receiver decrypt the file without having to agree with the sender in advance on using the same set of options and algorithms?

7. SIGNATURE GENERATION

Prepare a relatively small text file to be sent to **ONE OF THE MEMBERS** of your DIRECT TRUST GROUP. Sign this file using:

- a. default options,
- b. text output,
- c. text output + signature attached to the file.

Send the obtained files to the intended recipient. Investigate the output files, looking at their contents and the length.

Questions:

15. What transformations are performed during signing for each set of options?
16. Which algorithms are used during each of these transformations?
17. What keys are required to perform these transformations?
18. Where are these keys stored? Which of these keys are protected using a passphrase?
What are the pros and cons of passphrases?
19. Why for some options the text of the message is unreadable?
20. Compare the size of signatures.

8. SIGNATURE VERIFICATION

Verify the signatures you have generated and signed messages you have received from other members of your DIRECT TRUST GROUP.

Change a single character in the message or in the signature, and do the verification again.

Questions:

21. Explain the behavior of the program.
22. What transformations, algorithms, and keys are used during the signature verification?

9. PGP & E-MAIL PROGRAMS

GPG can be integrated into Outlook. You can also download **Enigmail** from <http://enigmail.mozdev.org/> to use GPG with Thunderbird. If you have neither of these programs use **Sylpheed-Claws** which is part of your GPG installations.

Questions:

23. Describe all steps necessary to plug-in PGP into a selected e-mail program.
24. Send a signed message to gmuece646@gmail.com, the message should contain at least, your name, email address and public key fingerprint in HEX. Include your e-mail in the final report.