# 20HT-2DV702 - Internet Security
# Assignment 2 - Email Security

## PGP/GPG, Digital Signatures and Anonymity, S/MIME


**Faculty of Technology**
**Department of Computer Science**

This document builds on the work by:
**Uraz Odyurt**

**Instructor:** Paolo Molinaro
pm222py@student.lnu.se

24-03-2023

# I. INTRODUCTION

In this practical work, you will investigate and test different security and privacy aspects on the Internet, mainly email security. You will get to try out encryption and digital signage of messages, giving you cryptographic privacy and authentication when communicating online. For you to achieve this, you will use a computer program for encryption, decryption and signing, which is provided by *Pretty Good Privacy (PGP)*, or *GNU Privacy Guard (GPG)*. You will also experiment with the more recent developments in available key-servers for PGP. In the second part of the lab, you will also get familiar with different possibilities of being anonymous on the Internet, focusing on anonymous email.

We expect you to use a GNU/Linux system for this lab, as it will be most convenient when working with required tools. If you are a Windows user, there are several options such as installing Linux virtually on a hypervisor, e.g., VirtualBox, using a LiveCD of a GNU/Linux distribution of choice, e.g., Ubuntu, or connecting to https://cscloud.lnu.se, where you can run a virtual machine directly from your web browser.

# II. DEADLINE & SUBMISSION

The deadline for the second assignment is **Monday the 1st of May at 23:59**. The individual report should be **limited to 9 pages** and should clearly describe the steps you have taken to solve the problem for each section and answer the questions related to each task. It is advisable to include screenshots for the important steps in your report. To support your answers to the questions, you may need to use references, i.e., to state where you got the information from. Examples of this has been given in the document *"Introduction to Practical Work"* and also in the *"Report Template"*, which must be used for the report.

Submission of the report is done on *MyMoodle*; **observe that you must upload the report before the deadline as the system will not accept your file after this time**. Do not forget to put your name and student id on the front page of the Report Template and to convert it to `.pdf` before sending it in.

# III. EMAIL SECURITY

**1.** Start by reading Why do you need PGP? by Phil Zimmermann and give some reasons in your report for using PGP. You should then install GPG on a computer that you have administrator rights on. Carefully read the documentation and make sure you set options wisely. You can install GPG from here.

Give a short description of GPG and the software allowing you to use it. What distinguishes GPG from PGP? State which one would you install for personal use and explain why you prefer it over the other?

**2.** Create a key-pair and submit your public-key to a public PGP key-server. For now, use this key-server for your tasks. You are required to include more than one identity in your key-pair (one is your LNU identity), since it is a convenient feature. Exchange your public-keys with at least two other students in the course. Sign each other's keys after you have validated them. Make sure to make the result available publicly. Paste the direct URL to your public-key and the URLs to your classmates' public-keys into your report (three URLs).

*Note that we want the search index URL, not the public-key content. The URLs must include "`op=vindex&fingerprint=on`" in them.*

**3.** You should now exchange emails with the two students, whose keys you just signed. You should send emails using the services, encryption, and authentication, to each other. Make sure that everyone can correctly send and receive encrypted and signed emails. Also test to sign attached files using detached signatures. Do not proceed until you are satisfied that everything works!

**4.** Find your instructor's public GPG key on any online public-key server. Make sure that it matches the one given on *MyMoodle*. How did you verify this? Is this enough to relate a certificate to its owner? Explain what might happen if you fail to verify the public-key to a claimed identity?

**5.** Make sure to send your public-key fingerprint through the provided link, *"List of Fingerprints"*, before the deadline. Explain the importance of this step against man-in-the-middle attacks.

*Note that you have only one chance for fingerprint submission, so make sure that it is the correct one.*

**6.** The next step is to send your instructor an encrypted and signed email. Again, make sure that it is the right key, corresponding to the fingerprint submitted in the previous task.

Download the document *"Responsibility.odt"* from *MyMoodle* and carefully read it along with the following documents, both accessible on the course page:
(a) LNU Liability Obligations
(b) LNU User Agreement

Complete the document *"Responsibility.odt"* with a date and your name. You should now digitally sign the document with a *detached signature*, which will give you two files, *"Responsibility.odt"* and *"Responsibility.odt.sig"*. Package them in a `zip` archive and send your instructor the email message with the `zip` archive attached. Do not forget to also attach your public-key to the email, making it possible to verify your own identity. **The subject of the email should be *"2DV702 - Key and Responsibility"***.

**7.** Choose two of the following three email services: *LNU student mail*, *GMX* and *Gmail*. These services use email authentication and validation measures. Setup accounts with these (unless you already have them) and send messages to and from these accounts. Which one of these messages are verified and which method is used? How can you in each service see that incoming emails have been verified? Show the header lines that are added and describe the different details in them in your lab report.

**8.** There has been some improvements around GPG/PGP and the workflow of public-key submission. This time, generate a GPG public-key and submit it to a new type of key-server. Now try using this key-server. What is the major difference(s) compared to the previous key-server and the workflow involved with it? Make a comparison.

**9.** Another option to have secure email communication is S/MIME. Explain in a few sentences how it works. What is the main difference between S/MIME and GPG? Explain the steps between two parties communicating via email and S/MIME. Clarify whose public or private keys are being used at each step.

# IV. ANONYMITY

**1.** Search the Internet for different methods on how to achieve anonymity when sending emails. Test at least one of the methods by sending emails between two email accounts that you own. Describe in your report about the options you found and the services you tested.