# Lab 12: PGP and S/MIME

**Introduction**

This lab is based on introduction to email security using Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME).

**Objectives**

Students will learn about email security and configure the email client (Thunderbird/Outlook).

**Tools/Software Requirement**

Thunderbird/Outlook, Windows/Linux/OSX

**Description**

Pretty Good Privacy uses a variation of the [public key](http://searchsecurity.techtarget.com/definition/public-key) system. In this system, each user has an encryption [key](http://searchsecurity.techtarget.com/definition/key) that is publicly known and a [private key](http://searchsecurity.techtarget.com/definition/private-key) that is known only to that user. You encrypt a message you send to someone else using their public key. When they receive it, they decrypt it using their private key. Since encrypting an entire message can be time-consuming, PGP uses a faster encryption [algorithm](http://whatis.techtarget.com/definition/algorithm) to encrypt the message and then uses the public key to encrypt the shorter key that was used to encrypt the entire message. Both the encrypted message and the short key are sent to the receiver who first uses the receiver's private key to decrypt the short key and then uses that key to decrypt the message.

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a widely accepted method, or more precisely a protocol, for sending digitally signed and encrypted messages. S/MIME allows you to encrypt emails and digitally sign them. When you use S/MIME with an email message, it helps the people who receive that message to be certain that what they see in their inbox is the exact message that started with the sender. It will also help people who receive messages to be certain that the message came from the specific sender and not from someone pretending to be the sender. To do this, S/MIME provides for cryptographic security services such as authentication, message integrity, and non-repudiation of origin (using digital signatures). It also helps enhance privacy and data security (using encryption) for electronic messaging.

**Instructions**

Complete the tasks below and insert the solution/answer in this document as directed below. You must show the execution of below tasks (by adding the snapshots), along with your required commands to get your work graded. You must also submit the completed Word document on LMS before the deadline. You can get help from the Internet, but copying is not allowed.

**Lab Tasks**

**Task 1:** Identify in your own words, the difference between PGP and S/MIME?

|  |
| --- |
| PGP vs S/MIME |
| In PGP the key is shared between two entities but in case of S/MIME the certificate is downloaded from a secure server.  In S/MIME the attachments are also encrypted while in PGP the attachments aren’t encrypted. |

**Task 2:** Configure PGP on Thunderbird/Outlook, show the steps of configuration along with the secure email sent to the other entities.

|  |
| --- |
| PGP Configuration |
|  |

**Task 3:** Configure S/MIME on Thunderbird/Outlook, show the steps of configuration along with the secure email sent to the other entities.

|  |
| --- |
| S/MIME Configuration |
|  |

**Deliverables**

Compile a single Word document by filling in the solution/answer part (as directed) along with the snapshots. Name your submission file as given below and submit this Word file on LMS before the deadline.

**Hadaiq Ahmad– 112807 – Bscs-4 Gp 1**