

**Lab 5: *Hashes, Asymmetric Encryption & Digital Signatures* (2%)**

**Overview:**

In this lab you’ll be introduced to asymmetric encryption using Public and Private keys through sharing messages with a class mate. In addition, you’ll being signing a message and any of your group assignment groupmates will verify that it is your digital signature.

**Note:**

* This lab is to be individually; however you need to collaborate with others sending encrypted and signed messages with your groupmates. You then need to verify the signatures and decrypt the message.
* Where **MSU** is given in the lab text, this means you should use your **MySeneca Username** e.g. MSU\_data1.txt would become **Navid.Esfahani\_data1.txt**

**Objective:**

1. Applying asymmetric encryption to encrypt and decrypt messages
2. Applying and verifying a digital signature
3. Complete a lab report

**The Lab Activities**

**Part 1: Set-up and Education**

For this lab you’ll be using any version of PGP you choose to use based on your operating system. You can find about different options on [Electronic Frontier Foundation](https://ssd.eff.org/en/module-categories/tool-guides)’s website. For windows, you can use gpg4win with Kleopatra UI.

* Download it and install the application of your choice for PGP
* Create a folder called “BTN710 Lab 5” on your SSD. **Store all files used in this lab within this folder e.g. text files, encrypted files, partners public key, your public key, partner’s encrypted message, partners decrypted messages etc.**
* Create two (2) text files using MS WordPad and store them in the newly created folder.
  + Name one “MSU\_data1.txt” and have in it the text “This file will be encrypted with your Public key”
  + Name the other “MSU\_data2.txt”, “MSU\_data3.txt” , and “MSU\_data4.txt” (if you are in a group of three, then you don’t need the last file)and have in it the text “This file will be encrypted with your Public key and Signed with my Private key”.

**Part 2: Generate a Key pair and sharing your Public key**

* Generate a key-pair – when asked for name and email address use your MSU and email address
* Export your Public key and name it your “MSU\_PK.asc”
* Send a message to your group members that has your Public key attached

You should have received an email from your groupmates with their Public key.

* Take a screen shot of the message with the attached Public key and insert into your report under the heading: “Received Public key”, then import their Public key into the PGP application
* Take a screenshot of the PGP application window showing your generated pair and your partners imported Public key and insert the screenshot into the report under the heading “Keys”.

**Note: You should perform parts 3 and 4 once for each of your groupmates.**

**Part 3: Encrypting and decrypting**

Now that you have imported your partners’ Public keys:

* Using your partner’s Public key encrypt “MSU\_data1.txt” and send the encrypted message to all your group mates

Once you have received an email from your partner with the encrypted message

* Decrypt the message and open the decrypted message to confirm that it is decrypted. (read the slides if you are not sure which key you need to use for decryption)

**Part 4: Digital Signatures**

Now you can encrypt and decrypt a message, you’ll be sending a message that has been encrypted with one of your partners’ Public key and signed with your Private key.

* Encrypt and sign the “MSU\_data<2 to 4>.txt” – be sure to take a screen shot of the “Encrypt & Sign Results” window and insert it into your report under heading “Signing”
* Send the encrypted and signed document to your partners

You should have received an encrypted and signed messages from your partners.

* Decrypt and verify the messages – take a screenshot of the “Decrypt and Verify Results”, inserting it into your report under the heading “Decrypted and Verified”
* Finally, take a screen shot of the contents of your folder “BTN710 Lab 5” and insert it into your report under the heading “BTN710 Lab 5 files”

**Part 5: Last activity**

Get the instructor’s Public key from the lab folder, encrypt

“MSU\_data1.txt” using their Public key and email it to the instructor.

**Lab Assignment Write-up**

Create a lab template based on the early labs (i.e. including title, student name etc.) and use this for the basis of your lab report.

**Deliverable**

Note:

* Submissions deadlines are given through the lab submission link.
* A lab submitted late will be given a grade of 0%
* A lab not submitted or satisfactorily completed by Study Week will lead to a course grade of 'F'