CS 3339
Lab 1: Public and Private Keys and Sending Encrypted Messages

In this lab we will be creating a public and private key pair and sending encrypted messages. However, first we will be installing the software that we will be using for labs this semester.

1. Download and install Virtualbox if you do not already have it on your computer **https://www.virtualbox.org/wiki/Downloads** (or the hypervisor of your choice)

2. Download the Kali Linux VM. Kali is a distro of Linux that comes pre-installed with a variety of security tools. This is what we will be using for many of the labs in this class. An image that is already set up is available here: https://s2.smu.edu/~dphanekham/CS3339/CS3339.ova

3. Open Virtualbox. Go to file→Import appliance and find the CS3339.ova file that you have just downloaded. You can increase its RAM and change other configuration options in the Virtualbox settings.

4. Start the VM and log in.
   username: **root**
   password: **CS3339**

5. You should be able to change the display size in the Display settings in the virtual machine.

6. Once that is done enter the command
   gpg –gen-key

7. then it will ask for your information
   Enter your name, email, and a comment

8. It will then ask you to help create entropy (randomness). You can do this by opening up a text editor and randomly typing in characters until the process completes.

9. After this process completes, you now have a public/private key pair. We will be talking about how these work more in class, but in practice, you want to keep your private key private and you can publicly distribute your public key, as the names imply. If something is encrypted using your public key, then it can only be decrypted using your private key, this way people can send you encrypted messages that only you can read. Additionally, you can digitally sign files with your private key.

10. Run the following command to export your public key to a file.
    gpg --armor --export youremail@address.com > firstname_lastname_pubkey

11. Create a new file and name it plain.txt. At the top of this file, put your full name. Beneath that, write some lines of text (it doesn't matter what really) and save it.

12. Navigate to where you saved plain.txt and run the command
    gpg --encrypt --armor -r youremail@address.com plain.txt
    This command is encrypting the file plain.txt using your public key.

13. You now have a new file called plain.txt.asc. This is the encrypted text. If you open it, you can see it looks like random characters.

14. To decrypt the file, use the command
    gpg plain.txt.asc
    Save the decrypted file as decrypted.txt
    This command has decrypted the file using your private key.
    Only your private key can decrypt a file that was encrypted using your public key

15. In reality, you would send your public key to other people or publish it to make it known to everybody. Now whoever has your public key can send you a message that only you can read.

16. Now you are going to send me an encrypted message. First you need to add my public key. Download my public key from
    https://s2.smu.edu/~dphanekham/CS3339/dphanekham_pubkey
    and enter the command: **gpg --import dphanekham_pubkey**

17. Now encrypt plain.txt using my public key.
    gpg --encrypt --armor -r dphanekham@smu.edu plain.txt
    and save it as dphanekham_encrypted

    DELIVERABLES
    A .zip folder named LAB1_Lastname_Firstname.zip
    containing:
    - your public key (firstname_lastname_pubkey)
    - plain.txt
    - plain.txt.asc
    - decrypted.txt
    - dphanekham_encrypted