Pre Lab 7: Public Key Infrastructure (PKI): Key Generation

In this Pre-lab you'll be familiarizing yourself more with the concept of Certificates, public key & private. This will be preparation for the full lab on Thursday. We will ask that you do this lab on your own personal computer instead of using the RAVE VMs.

Here is a link to the core concept for which this lab is built off of:
https://www.linux.com/learn/pgp-web-trust-core-concepts-behind-trusted-communication
(a la Three Musketeers)

Step 1: Generating a Key Pair
Windows:

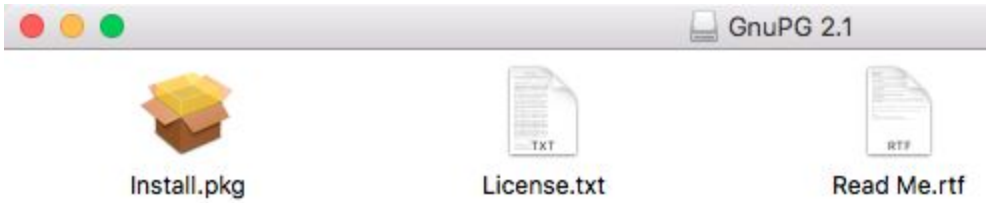
- Download the following:
  - https://www.gpg4win.org/get-gpg4win.html
  - (No need to donate anything)
  - Follow all Default installations steps
  - 

    - Check the Desktop option along the way
- Find "Kleopatra", which you just installed on your desktop
  - 

- Open Kleopatra
    - At the GUI, click on “File”
        - Select New Certificate
        - At the next step, choose “Create a personal OpenPGP key pair”
        - Enter your name and email address (your hawaii.edu is fine)
        - Under Advanced Settings, go to “certificate usage” and check “authentication”
        - Click “Next”
        - Click “Create Key” to generate your certificate Key Pair (Yay)

Mac/Linux:

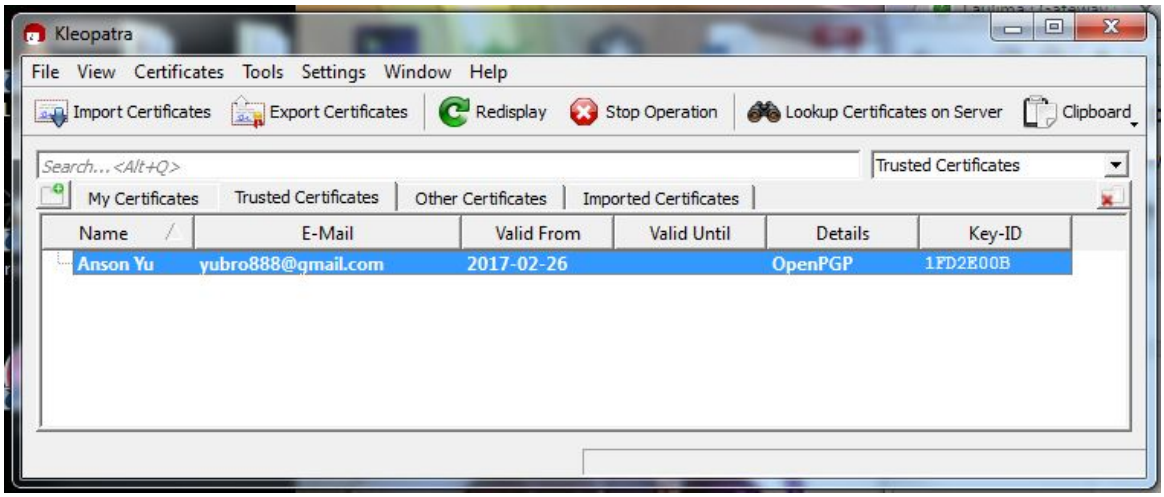
- (Mac) Download: https://sourceforge.net/p/gpgosx/docu/Download/
    - Install from the “Install.pkg” in the .dmg file you downloaded



- (Linux): Open a Terminal:
    - Type in “sudo apt-get update”
    - Type in “sudo apt-get install gnupg2”
- Open up a Terminal
    - Type in “ gpg2 --help”
        - Take note of the options you have
    - Type in “gpg2 --full-generate-key
        - Select (1) RSA and RSA (default)
        - Choose 2048 for keysize
        - Input the rest of the data (Name & Email [use hawaii.edu] required, Comment is optional)
        - Create a passphrase
    - You created a Key pair yay!
- NOTE: If you end up making multiple keys, use different emails
- Move to Step 2

Step 2: Export Key and email it to Anson
Windows:

- Open Kleopatra
    - Select the certificate you created



    - At the GUI, click on “File”
        - Select “Export Certificates”
        - At the next step, choose a directory to save your file and name it “<yourname>.asc”
    - Email your .asc file to me at ayu2@hawaii.edu
        - Subject Line: ICS355PLab7 <your name>
        - You Good!

Linux/Mac:

- In your terminal
    - Set your directory to an easily accessible place
        - E.g. My Documents, Desktop, etc.
        - Create a folder called Certificates
        - Set directory to inside that Certificates folder
    - Type “gpg2 --list-keys”
    - You will see your own key that you generated
    - You must export your public key now
        - Type in terminal
            - “Gpg2 --output <yourname>.asc --export <your hawaii.edu email>
    - You have just exported your public key to a .asc file
    - Email your .asc file to me at ayu2@hawaii.edu
        - Subject Line: ICS355PLab7 <your name>
        - You Good!