Keys to the Kingdom

Assignment Due Date: 2/13/16

As you learned in class, asymmetric encryption involves using a public key to encrypt messages and a private key to decrypt messages. This is often referred to as a **key pair**. For this homework assignment, you will be creating a key pair using OpenPGP. OpenPGP is the most widely used e-mail cryptography protocol in the world, so it's safe to assume that the protocol is mature enough for secure e-mail encryption and decryption.

If you are using a Windows machine, download the most recent release of Gpg4win here: http://gpg4win.org/download.html

If you are using an OS X machine, download the GPGTools Suite here: https://www.gpgtools.org/gpgsuite.html

If you're using a Linux machine, you probably already have the capability to generate OpenPGP keys; look up instructions for your particular Linux distribution and let me know if you need any help.

Follow the instructions below for Windows or OS X.

Setting up OpenPGP Keys on Windows

If you are using a lab computer, skip to step 2

1. Install Gpg4win using the link above
    a. When prompted, be sure to check *all* of the components for installation
2. Open Outlook and create a new mailbox with your student e-mail credentials
    a. Your account information is stored on your local profile here in the AT&T lab, so nobody will be able to access your e-mail account except you
3. Once your student e-mail is setup within Outlook, open the "GPA" application that you installed with Gpg4win
4. In GPA, click "Keys", followed by "New Key"

a. Enter your name
b. Enter your student e-mail address
c. When prompted about making a backup, make sure the “Do it later” button is selected
d. Enter a passphrase: this should be a sentence that you can easily remember.
e. Re-enter your passphrase

You should now have a pair of encryption keys for your student e-mail! Let’s send an encrypted message.

1. Go back to Outlook (or re-open Outlook if you closed it)
    a. If you re-open Outlook and are prompted for credentials, enter your student e-mail and password once again
2. Click “New Email” in the top left corner
3. In the “To” field, put mu.it2910.sp16@gmail.com
    a. Don’t forget to download and import my public OpenPGP key! You can find it attached to the assignment on Blackboard
4. For the “Subject” field, put “IT 2910 Encrypted Email Test”
5. Write a short message; a single word is fine, just keep it safe and smart. ☺
6. At the top of the Outlook window, you should see the “GpgOL” tab; click it
7. Click “Encrypt”
8. You should see both your certificate and my certificate in the window that pops up; if you see the correct certificates, click “OK”
9. The e-mail should change to what looks like a large amount of garbled characters that starts with “-----BEGIN PGP MESSAGE-----“; if the e-mail looks like that, good job! Hit “Send” and you should be done (you may be asked to enter your certificate passphrase one more time)

Setting up OpenPGP Keys on OS X

1. Install the GPGTools Suite from the link above
2. After installing, GPGTools Suite will open and prompt you to generate a new key pair
    a. Enter your name
    b. Enter your student e-mail address

    c. Enter a passphrase: this should be a sentence that you can easily remember.
    d. Re-enter your passphrase and click “Generate Key”
3. Now that your key has been generated, you need to import my public key; download my public key (attached to the Blackboard assignment) and click “Import”
4. Open the Mail app and ensure that you’ve linked it to your student e-mail account
    a. If you haven’t, go to System Preferences > Internet Accounts and click on “Exchange”; you should then be able to enter your student e-mail info and link your student webmail with the Mail app
5. Start a new e-mail
6. In the “To” field, put mu.it2910.sp16@gmail.com
7. For the “Subject” field, put “IT 2910 Encrypted Email Test”
8. Write a short message; a single word is fine, just keep it safe and smart. ☺
9. Click on the broken padlock button in the e-mail composition window; this will encrypt the message using the recipient’s public key
10. If the padlock icon is now blue and a locked padlock, congratulations! You can send your message.