Overview: You are going to do the following things

1. Install the Gnu Privacy Guard, also called GnuPG or GPG, on your computer
2. Determine a passphrase to guard your private key
3. Generate a public/private key pair for yourself
4. Export your *public* key to an ASCII document file, sometimes called "ASCII armored." (There is no real armor or other security advantage and besides, this is your public key; it doesn't need security.) Name the key file <yourname>_key.asc
5. Send a friend your public key. Your friend can use it to encrypt a document that only you can decrypt.
6. Get a friend's public key, use it to encrypt a document, and send it to your friend.

Optional steps: You may want to do the following:

- Generate a revocation certificate (You will probably have to use the command line interface to do this.)
- Upload your public key to a public key server. (Key servers talk to each other, so one is usually enough.)
- Set up both digital signature and encryption for your preferred email program, if supported.
- Export your private key and revocation certificate to a backup medium.
- Have your public key digitally signed by two or three other people, beginning a "web of trust" for y our key. Note: you should *only* sign the public key of someone you can absolutely identify; similarly, only people who know you or can identify you should sign your key. For a counter-example, see this. (Contains vulgar language, so be warned.)

The handout doesn't contain instructions for doing these things, but you will have learned enough to figure most of them out by the time you've completed the assignment. GnuPG does work as a command line program in all operating systems. In general, you must be "in" the directory containing the gpg binary. For actions not supported by the GUI interface, check http://www.gnupg.org/gph/en/manual/book1.html (This was written in 1999; remarks about the encryption algorithms are out of date, but the procedures are correct.)

Beware: If you start to use GnuPG, and one hopes you will, you will need to guard both your private key file and your passphrase. If you lose either, you will lose access to everything encrypted with your public key. If your revocation certificate is compromised, Evil Eve can revoke your public key. Be sure to take appropriate precautions.

Some terminology: You will likely do some research on the web. The terminology used in some web articles is a bit confusing. Here are definitions to help you.

OpenPGP

OpenPGP is a standard describing a mechanism for both encrypting and digitally signing files. Those files may be email messages or, as in this exercise, a "plain" data file. There is no "OpenPGP" program; two programs that implement the OpenPGP standard are described below.

PGP

PGP is a company and also the name of that company's products. The PGP products implement the OpenPGP standard. They're commercial products; they cost money. People pay PGP Corp. money to get technical support, regular product upgrades, etc. There was a free version of PGP, but it is now very out of date and should not be used.

GnuPG

GnuPG, also called Gnu Privacy Guard or GPG, is a free and open-source implementation of OpenPGP. As with other free software, support consists only of forums, mailing lists, and web articles. Upgrades and fixes are contributed by a dedicated group of volunteers.

Certificate

GnuPG refers to your public key as a *certificat*e because it is. What's produced is your public key with a digital signature signed with your private key. That's a self-signed digital certificate. While it doesn't provide any assurance of correct binding to an identity, it *does* provide protection against tampering.

Step 1: Install Gnu Privacy Guard

Windows users: Download and install GPG4Win (http://www.gpg4win.org/) and go through the documentation at http://www.gpg4win.org/doc/en/gpg4win-compendium.html. Be sure to install and use Kleopatra. You can do everything needed for this assignment with Kleopatra.

Mac OS users: Download and install GPGTools (https://gpgtools.org/). You will find documentation at the same link.

Linux users: You can get binaries and documentation directly from the GnuPG page (http://www.gnupg.org/)

If you work in the lab, but want to save your work, there's some pretty minimal information about moving GPG4Win files to a USB drive here: http://superuser.com/questions/246177/how-to-store-kleopatra-pgp-keys-on-usb-drive.

Step 2: Determine a Pass Phrase

When you generate a GnuPG key pair in the next step, your private key will be stored in encrypted form on your hard disk. Someone who gains access to your hard disk or a backup of it can unlock your private key if they can guess or otherwise determine your pass phrase. What is needed is a phrase that you will remember easily, but that would be difficult for most others to guess. An example might be: *My paternal uncle's name was George.* I won't forget that, and even someone who knows about my family is unlikely to guess exactly that.

Some password crackers have incorporated the rules of English grammar into their cracking programs. If you re-cast your pass phrase into "Yoda speak" or otherwise mangle the word order, it is just as easy to remember and type, but no longer follows the rules of grammar and sentence structure: *George my paternal uncle's name was.*

You can make guessing a *lot* harder by "lying" when you create a pass phrase. My actual paternal uncle is Bill, not George, although neither one appears in any of my pass phrases

If there's any chance you will use GnuPG other than for fun, spend some time and take some care with your pass phrase.

If you forget your pass phrase, you will not be able to decrypt information that others encrypt with your public key. Depending upon just how confidential your encrypted information is likely to be, consider writing down your passphrase and putting it in a safe place, such as within an infrequently used book. Or not, as the case may be.

Step 3: Generate a public/private key pair

Follow the instructions for your version of the software to generate an OpenPGP public/private key pair. You will use the pass phrase from step 3 to lock your private key, and you'll identify the key pair with an email address. Consider picking a reasonably permanent email address for this exercise. You do not necessarily need to use your SPSU address. Choose the maximum key size supported by the software you have, but *at least* 2,048 bits as the key size.

Caution: GPG4Win and possibly the other programs allow one to create more than one kind of key pair. For this exercise, only an **OpenPGP** key pair will do.

Step 4: Export Your Public Key

Export your *public* key to an ASCII file following the directions for the software product you are using. (Windows users: Use File -> Export Certificates. Others, see the instructions for the software you are using.) Name your file <yourname>_key.asc, like bobbrown_ key.asc. Be sure you have a dot-asc extension. You can pen the file with a text editor like Windows Notepad and look at it.

Be sure the file you get says "BEGIN PGP **PUBLIC** KEY BLOCK" because if you release your private key you will have lost all confidentiality.

Step 5: Send a Friend Your Public Key

Possibly the best way to do this is to send the key as an *attachment* to an email message. Your friend can use your public key to encrypt a document, send it to you as an attachment. Only you will be able to decrypt it.

Step 6: Receive a Friend's Public Key and Encrypt a Document

Receive a friend's public key, import it into GPG, and encrypt a document. Send it as an *attachment* to your friend.