How to use the GNU PG encryption software

Chun-Jen Tsai 4-10-2012

This document describes how you can use the GNU public key encryption tools to encode a message so that you can email the encrypted message to other people securely. Please follow the following instructions:

1. Download and install the GnuPG 2.0 binary installation package from the web page:

   http://www.gnupg.org/download/

   Note that, there are binary packages for different OS's, including Linux, MacOS, and Microsoft Windows. The following instructions are written for MS Windows. However, since gpg.exe is a command line program, the instructions are similar for other OS's.

2. Make sure that you have installed the software. Make sure you have added the command path: C:\Program Files\GNU\GnuPG to your PATH environment variable.

3. You can now initialize your own public and private keys using the following command:

   ```
   C:\> gpg --gen-key
   ```

   Note that it will ask you to type in your name and email address (as part of your user ID), please type in those information so that when other people try to encrypt a file for you, they can use your email address to look up your public key.

4. Generate an ASCII text file with your public key so that you can email your public key to others.

   ```
   C:\> gpg --export --armor > my_public_key.txt
   ```

   Whoever has your public key can email you secured messages.

5. After receiving other people's public key, you should import their keys into your system by the following command:

   ```
   C:\> gpg --import --armor < others_public_key.txt
   ```

6. Now, you can encrypt your message and send it to others using their public keys as follows.

   ```
   C:\> gpg --encrypt input_file.doc
   ```

   When gpg ask you for the user ID, just type in the recipient's email address. A file with the suffix ".gpg" will be generated and you can email this file to the recipient. By the way, gpg will keep asking you for the next recipient (and encrypt different files for them) until you type in an empty line.

7. If you receive other people's encrypted file (encrypted using your public key), you can decrypt it using the following command:

   ```
   C:\> gpg --decrypt input_file.doc.gpg > input_file.doc
   ```

8. Finally, if you want to send the TA a secure message, his public key is as follows. You can copy-and-past the key (start from the "-----BEGIN PGP PUBLIC KEY BLOCK-----" line to the "-----END PGP PUBLIC KEY BLOCK-----" line) into a text file for import into your system. The email address (TA's) registered in this public key is fox.shc@gmail.com .

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.17 (MingW32)

mQENBE+D5+MBCACqq7C1Hab8xV/a2VvuXEO6HbYROoXVloP0mNnfCEucggqyU16Q
xEtBNUeEO4KthxHjdW5NBQq3ne/Zg6DVOV9F5Rc9SJsy6qRZPbsEFzDAMpAx8PH9
Uidn1hv6ht5RjxBZQGixzeuhuhr7oyD3pf4Wyuq50FOe7R15SQQfJOwPDZqkoaG9
ZkOnqz6+zl0H2PR4yRr/fiV3ZSHiimyqg9BoulJIyfG5qjTD7Nt57SBefJU8k+Bg
k9I9RrembvEg9Pgg3J+81p9pJcUQf3SB4RJv0XlAfCKaU2DynBNtAq5j3I0mfmlP
Z9biCM7INlUMHM7qJPLh2gw96YKzPwb8XJBJABEBAAG0HUh1bmdDaGVuZyA8Zm94
LnNoY0BnbWFpbC5jb20+iQE4BBMBAgAiBQJPg+fjAhsDBgsJCAcDAgYVCAIJCgsE
FgIDAQIeAQIXgAAKCRClKNdyKHhVl4qqCACb18COI9nzcyif/65hUuB7fRBgSW/n
Kv77j5RE53k/XcCwgIXSbOR2Cx4yIRPScMLP1BsYpvqcMx+uaATWioBI5Q1zMqPC
atFQq5o0jl+b38yMPOztYK+DmlqWWcdXkAjX5jEn182mnd9scMSdwFz8RrYfHhsr
4VBrYl6Cs4/RgGIFvHM5rLLVEYOCeVHroxxh+xrdMpsewHW0WHdQKPs/RZjDcloc
7PqJ+24F9N6Jd4hAdAWTxPGtOfA7WxDnjHE7xeRJnqQJYntNR8ST0j8SyYRY1BTw
5yQBLRcaZFULG+kEe3Xd10RhqQ4c8AMGSDGOfuWsA/8xzrwIgUr8AXAzuQENBE+D
5+MBCAC3fyuJyoJjz1sW7p0Iqk7taV/1AmFmH4rTx5XAGTM31vNPHAmNPz1/qW2s
pWzBzwjkpwuFEXDmcsXRRiRyj40oLe0GdXeKZLQst65jlXuhEykyeDb67uh7FnyF
/8B2qqNjmd4rRrN3jpXn+t/nFez+fplvhCXZlnSCKDZAZuu4pUBSC+/iOOkqexhC
6vU6eBNGFe2EEDu40Bydkb4Ctg9veitmUk23i9u/WQYTSwWQYm+ccv1LUv9nxJaH
8UryIuDr6XkebFVxJl1T6GSRyRtqdEr7XPOTH2KXjeQPFCAUVQmOYA6FL5F2TGET
d50kF/UhHEZhmycLUOCOfBAXFgXnABEBAAGJAR8EGAECAAkFAk+D5+MCGwwACgkQ
pSjXcih4VZe+Owf+JBmhztN52/tuzieohx4/m/rFVSRZSZK3sShhjs4CKb+cIsTu
RqpAd493IOim4cdd8Z2g60SutVk7pLNFP0FjFkoioqYFT4d1Kgpa/beUJmJW0vEI
ukIeSwQ478mr34ryEgZFaPVl/4un6uXaE3g3U/Z3kSVvxCfO9gE2UniRgZUGSzGH
YUNw0oPuw20USeTAlhveh1y0VkC9/GFnFL9Iy80qIlzwHlMIeZxTHT0LTPzv2bfN
WES7eQJiDIKwnXA4TUZ/Bm67StX1DDzaNk/Oj1j9oK1NXI5X8Q40xXgCgRbZ3u3v
Npw5e0trizO8xHFE49WSoromRYFz2uHgMEYnSg==
=F8hj
-----END PGP PUBLIC KEY BLOCK-----
```