

## Chapter 2

# GNU Privacy Guard

*Cryptography in history is interesting, cryptography in theory is fun, cryptography in practice is important. And hard.*

This book contains descriptions of some of the most sophisticated cryptosystems ever devised. A cryptosystem as a theoretical construct is one thing, actually moving bits around in a secure manner is another. More on this later; for now, install and use the Gnu Privacy Guard (GnuPG).

### 2.1 Getting Started

First, run some updated anti-virus software. There are viruses whose payload is to intercept text between the keyboard and the computer, and forward them to third-world internet locations. Good cryptography doesn't help if your correspondence is intercepted pre-encryption.

Second, get and run some reliable anti-spyware software (Ad-Aware, for example). Every time you install a new piece of software, you are exposing yourself to a security problem. However, spyware is so prevalent and malignant that it is a greater risk to you and your privacy.

### On Windows

Here are my recommendations for preparing your Windows PC for some heavy-duty cryptographic action.

- First, download and install GnuPG (currently at version 1.4.1):

`http://www.gnupg.org`

- You should now adjust the "PATH" variable to include the GnuPG folder, and restart your computer
- You should install GPGshell (currently at version 3.4.0):

`http://www.jumaros.de/rsoft`

- Use GPGshell to create a new key. It's okay to use the default options, have it expire during the summer. Then send your key to

`hkp://sks.keyserver.penguin.de`

using GPGshell. Next, use my key ID 0xA2D17932 to download my key from the same keyserver.

- If you use Outlook or Eudora, then you can get a toolbar through the GnuPG website.
- I recommend using Mozilla Thunderbird (currently at version 1.0.2) as your email client. You can download it from

`http://www.mozilla.org/`

If you use Thunderbird, then you will want to install Enigmail (currently at version 0.91.0).

`http://enigmail.mozdev.org`

We will talk about keyrings, rings of trust, and “good cryptographic practice” in due course.

## 2.2 My Public Key

You should export your public key, and print it out. Hand me a printout (I will check your ID), and also send it to me by email. Next, use GPGshell to send your key to the keyserver

`hkp://sks.keyserver.penguin.de`

Mine is on the website, and in Figure 2.2, and on the keyserver listed above. Mine is probably bigger than yours: *c’est la vie*. By the way, mine is set to expire in August 2005, so you shouldn’t use it after that.

Finally, send me an encrypted email. Since I’m actually going to read it, make sure you write something interesting!

```

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.1 (MingW32) - GPGshell v3.30

mQGibEJHAUERBACURi6sMfBj+d6JtvUYSM1uA4ytZykEiabgkGbiuukE5SwbFQOK
Pc3XCS/EbHOSxt7dwrZ+EUFpIJ2a4KchQ8VWDsLoyCRrQFYmlStmBmb92uadmHUS
FW9W4Z2go4W4HauLIAYIXu10Jg9Kx3hMAkvWYrXTWmqIdHF8t4wTbvzUcwCgi5hQ
4V6ZZDJUADC85H1Qx13oKX8D/isI/NtGBGVkoihAKrXk10P1kAOYkdsPwMkgrFQA
KHxBR+b0Lc4U0AfoAbF0iUps9w8rvkwnlSeGOoZm0j659rF3h7zx/kuRub0v00rF
emOXvU1Eo9vNcPqQS9sLmKLR9Mg+o+QtMqnyIyQWJ0yGCSXqpcnqWcV5L7HSqCC
gCIEA/9pU60GQuDrEa7i+IRe0mQiFV1uVY7b0w00LefirrmisrU5F/9quqy+lfQa
PtQL8F/Ao7zQLg13YrY3EmS60V6siWLe5eFPSbkphsfEJ8zk3Dr/pAbIAp950VES
ws3o9krbSK43hsuhe+gy0Gn1mVKZBXjrHLqAt+8UW//+2vbrHbQ3S2V2aW4gTydC
cnlhbnQgKfVDU0QgTWF0aCAxODcpIDxrb2JyewFudEBtYXR0LnVjc2QuZWR1Pohj
BBMRAGakBQJCRwFBAhsDBQkAxcEABGsjCAcDAGMVAgMDFgIBAh4BAheAAAOJEDwt
lPuiOXky5MoA13hVMCwtDb+Yw4rFXFTYmJc1tdsAnR1ctXOX86dzD35N6B6+OBBy
DmknuQQNBEJHAd8QEACvjzSc8W5aPswTtnBtgCMKVwF4QwmeUj45r64otyfr173T
B8FbLlvj18XqbiAr0zppJtchDyPJGEEKHWk8EsmXnOMdsCb1DxAq2r1Mj4wueprBD
LEqRBYpPY2JS2wTpBr9qQn028v5YAsItCYA5rXw4d3bWtt7euNtUfIF36VhsELU
dgsW20VWs+VvOSA9hjHwDqFPnT+FgVRoK7M/rfzMiBcFOE0AFS2Qg9U9UfIVInmk
v5bkfvBwKsG1Fi9Zg5BFxwRklcNpJ7QIWeJ7K50zYpPpx078QKnivQiE/eqGdQv/7
sj0zuIGYx8pj2z6z+YZa05Nz0rsAdVjaYYZIfjjgeEiu3l9wghNmnVidZQCuTP0w
6XhM1ZiiXvHFhmB0+btIPsXV9VCFRk0p5IPS01/3I+g0XSJmXVwhehikpnhqBmk
NZLDqkldj1PvcycMnxDV4CKUR2no5JJbr/ybeDbQTJJORGNegwqWvz0S0s8gv6bg
jZfy0Q/y0E9fDg7UmtsXizQMj5j3YI6VWr+J/kQLGZilHMbvH71H7Dlnn9pn8EU1
db3CgZ+Hc/URTN26ZABDpZf1EeBP3TVVEprtJTH2fNDAUkKc/S5gkpcqWyjDT5Z0
z1xe7hnlJ/m4zjE3vgpcTo7aIjNadaaFiMz1Q/65j7Zc6j76tdFJ2qheMqbGkwAD
BhAAkHh/N9fk4FDQDX8LRandMbrMnsq/ErPE8AInaJBFzvqu5ZPn9zJWrwulLr8q
oQIjM/HnjtuiLcEaUxAJHrZ3VK67ml+p1/pVHutunBfmGtKlxY7SPxGSNBm6LjS
dT4+F4+jHqrPo7XZFoR7JOC0vQABkTUWM9RxtTxh5Ep1BNg2uiEZSL/JfNg5MqJB
yYKpf5E4uD33tqiSIFGjTBFZGZtphy4etUQoH5UTVvQYLRYMJKiy0lS2ubd3P0qsj
bKIit0Awykf/U9/OQRXXV7XkN64RgRPXbmN4wsFW78QC011Y/AzGqoFOAMqJdoZo
SB6Jxlgw3kFGIRhBxhgweP/8GGOM5Tk06kgkykPIrel08HxtNuS0JZCQ0HDL5NEv
7j5K/r05yhWnlS14c4cgIYsIn2rr4Mj5+vubu1dox8T+WDYXyVIp0yIOUS8pWW7s
Hk2mJphglgBa8qMW6nWs9c1RrSrg1ptROXYuV12b5xbqxBrxn+eFw1tVdD6gnjF
phhMIpMrNEN7CSbVwowJs/3G3fv1EGqKGcP4B2SDdyLB00J07iCvD3A+dIyeVcYz
rp5BHAMHgQJqo1lKXi0UeCsi0jbpr8P7qjrj5ySP8oTcnc5KvTJ1zTvMXfG00dX2
NWEXN/MtzJ0hr7Fw44yKnpMku8Jo90b00Dw/aA+YDgUpcXSITwQYEQIADwUCQkcB
3wIbDAUJAMXBAAAKCRA8LZT7otF5MgziAJ9Ue5XjX9yEJwIyANBptq5Xv0UsFwCf
fkK/e8gBYLUNeK7v/T9rCX61vCQ=
=7ord
-----END PGP PUBLIC KEY BLOCK-----

```

Figure 2.1: Kevin O'Bryant's Public Key, valid through July 2005

