Homework #2

You must submit your work to your instructor before midnight on due date. Failure to do so will result in late penalties, see the syllabus for grading detail.

Submit your work on the Blackboard before midnight the day the homework is due. Here are the requirements for your Blackboard submission:

- Attach the assignment as a compressed archive file (.zip, .tgz, .tbz2, .rar) Include in the archive a copy of any code you've written in order to get the assignment done.
- The name of the file should be: *firstName-lastName*-HW-*assignmentNumber*.*extension* (e.g. Jane-Doe-HW-2.zip)
- Include your e-mail address in the Comment field when submitting the assignment through the Digital Drop Box
- If for any reason you are submitting the assignment more than once, indicate this in the Comment field by including the word COMPLEMENT

The purpose of this homework is to give you a chance to get familiar with using public-key cryptography and encrypt/decript files.

Here is what you have to do:

- Download and install GnuPG, free software, from www.gnupg.org
- Run the executable (gpg) and generate a pair of public/private keys that will be stored under a directory called .gnupg in your home directory:
  - make sure you select a key type that allows you to encrypt and sign
  - the key size must be at least 2048 bits
  - the email address you use should be your official IIT student email
  - choose a passphrase
- Once you're done generating your keys, do the following:
  - add your instructor's public key (see below) to your keyring
  - export your public key in ASCII format

NOTE: You can find documentation GnuPG documentation at http://www.gnupg.org/documentation/

Part (i), 50 points: Create a plain text file (named *firstName-lastName*-HW2-part-i.txt) that has three parts:

- your favorite poem (could be Shakespeare, a modern poet, a Haiku or some other form of poetry, it is ok with me either way); however, please don't give me what comes at the top of your Google search, chances are I've already seen it a number of times and have no patience to see it again. Be yourself, don't just try to knock this assignment off! Here is a list of poetry you should avoid in your submission. (10 points)
- your (ASCII) public key (20 points)
- a link to your public key on MIT's Public Key Server (20 points)

Encrypt the file (ASCII armor) and send it by email to your instructor.

NOTE: In addition to posting your public key to a key server you may want to make it available in your web page.

Part (ii), 50 points: Create a plain text file (named *firstName-lastName*-HW2-part-ii.txt) that includes an explanation of what you found hard about getting this assignment done. Encrypt and sign the file and send it by email to your instructor. You should complete this part within 24 hours from completing part (i)

Here is your instructor's public key, you can also find it on MIT's key server.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.6 (GNU/Linux)

mQGiBEc6dVIRBACgU4rxGnWFlBVO+qJodGdZ0beILw+tmju8k4UwoKxXBa6thdAy
a8xy6rfx+ORLjridsI9HT42RKDhgRigbXnt48u6vYXQdjBXXPI96AAUzleqlESfA
/Kw7Wb3mu6aBWIBUc7E8/QIHfmA+HnPR0szaD7Rpd3W72EQ0loTKtCuefwCgj+4u
CkQtggV4j9fYJYBtRcPwx50D/0BKheW+50nU7Z6z2UL/ZoXONTjx4+x6FjS/NUq0
HVeIRQ6fKDU2fPjKH2xDVj0RrCIaKDFXy/CBfOM57Yn2sAEAzLpSMmxq2qV3j/zT
wrgi6s+BM0xqDqopBQxt936AO9lNwCGKJTf8V2Jf9G0s6E3fG/mpUYWgEzPI0yzo
0HXpA/9o4CuaPqAKHyxIadN3Y9zcd6D6duzTKhc+kTSWpUoD32HqdeQnJVnTjkgd
eFNPhyF7w4RMEuZcc72SDU3cUjxqkiZ1vhU0DvvykI3fBghPbMiLW0yLJ7/ja1pN
S0/B2ckaCiwP8V2rKVvcx9y6tqvoe0wo4JweAn4V7P8r2VxhWLQ3VmlyZ2lsIEJp
c3RyaWNlYW51ICh0aGVTbGVlcGxlc3MpIDxiaXN0cmljZWFudUBpaXQuZWR1Pohg
BBMRAgAgBQJHOnVSAhsDBgsJCAcDAgQVAggDBBYCAwECHgECF4AACgkQDviO1WSs
9g0obACdHUfT6c2VTJ8deCMH2CGhJe6CulAAn3nc8P8htEvWLvsTWICbXa0LG73T
uQINBEc6dWIQCAC64MUxVKGBHXFnFTFWDgH3msvlkeBgF60LIsaCYxzwAWxi4cu0
edQ09mF+SnppJ5LLTPU5TJQH2pHoleMMcZcN2RQVrXpI4bkiHs2zqNpUfl6ohDSL
A06iPkY9qOiRsP5nFN/TW936xzPS8j5S+xhg/uagG06MopRqngpScooG4qJ1g22T
AYluciLISutuFjMMWXdMzffUYFFEYT/tRTyEZ7BWBbWGuDyR2t7UPXVS1q9cWN1s
B6NjgLm1MmzN59A/mRXi2Kf1+i87eumRk1+HAY1vq395YcBl7h4SStbRz1zfqgRJ
K+0J2sHHSuwP452zny9ubr7lof2qAffRszUbAAMFB/sG+F8KQhAkkKz9Xb56sMNR
9uZjUQVdTdusno8PQbZJeXqKhKZuYwOVP0wOIdxFj+yKgPy5d1sH4q9OBbK0epJu
pBYJdOyKVfMLgN9d1+VL7DgYY2ZjM+OuN3PmjpwbeDU/L8NgdXlK8vzOjguGEXA7
hijJNtDj6Q+KtXIciUGF66dsEhXgSAOCo6aS3om6DOXt6HoSJ7JNLZydM8ZSabhH
pAald7A1/Gpr/f0P/vj943akEWWnAp0cxkKU7T9pD8bOyejwOpvjzJzBce7okjrU
HIK+cDmvXv7VySj0EsWvYpM++ut0Nx1qhO2IbJzZk+jzQlKaeXAaiSeFSOkSKoMI
iEkEGBECAAkFAkc6dWICGwwACgkQDviO1WSs9g1gUQCfTI9JfDR1kBIu2ZZTQeYj
+XAXOBwAn0gnzS7D18QNbP2a7lUFLKkdfu6d
=ihFR
-----END PGP PUBLIC KEY BLOCK-----
```

Last update: Aug 31, 2008 Virgil Bistriceanu cs458 Computer Science

---

$Id: hw2.html,v 1.2 2008/09/08 00:08:42 virgil Exp $