

Homework 3

Due date: Oct 24

In this homework, you will be using GnuPG (The GNU Privacy Guard), a tool for secure communication. Information about GnuPG is available on the homepage

<http://www.gnupg.org/> .

Reading the GnuPG manual at

<http://www.gnupg.org/gph/en/manual.html>

and the references posted at the discussion board is very helpful for you to work on this problem. GnuPG is installed in the Linux systems at the instructional lab. Here is the list of computer hostnames in the EECS Linux lab.

```
ics7055.vuse.vanderbilt.edu
ics7056.vuse.vanderbilt.edu
ics7057.vuse.vanderbilt.edu
ics7058.vuse.vanderbilt.edu
ics7059.vuse.vanderbilt.edu
ics7060.vuse.vanderbilt.edu
ics7061.vuse.vanderbilt.edu
ics7062.vuse.vanderbilt.edu
ics7063.vuse.vanderbilt.edu
ics7064.vuse.vanderbilt.edu
ics7065.vuse.vanderbilt.edu
ics7066.vuse.vanderbilt.edu
ics7067.vuse.vanderbilt.edu
ics7069.vuse.vanderbilt.edu
ics7070.vuse.vanderbilt.edu
ics7072.vuse.vanderbilt.edu
```

An account has been established for you on these machines. Please refer to the post at the discussion board for your login information. For each of the machine problems below, please include the *commands you use and the system output* in your answer.

1. GnuPG uses Elgamal algorithm. Please describe Elgamal algorithm and show how it works (Reference: (1) Problem 10.4 in textbook [WS]). (10 pts)
2. Generate a new pair of keys. Make sure your keysize is at least 1024 bits. Export your public key into ASCII-armored format and post it in the discussion board. (10 pts)
3. Extract the fingerprint of your public key. The fingerprint is a long string of about 40 hex digits which can uniquely identify your public key. It is generated by applying a collision-resistant hash function to your public key so that no two public keys have the same fingerprint. Fingerprint can help to authenticate public key. For instance, Bob can publish his public key

in a key server. Alice, once retrieves Bob's public key, can call Bob to compare the fingerprint, making sure that the key is not a forged one. Your job is to write down the fingerprint of your public key. (10 pts).

4. To communicate with your friends, you need to exchange public keys. The GnuPGP uses public *keyring* to provide local public key management. Get all the public keys of the instructor from the discussion board, and import them into your keyring. List the public keys in your keyring after you import the keys. Please note that all the keys share the same user name, so you need to identify them using their key IDs. (10 pts).
5. There are 3 announcement files on our discussion board: announce1.txt.asc, announce2.txt.gpg and announce3.txt.asc. Only one of the files is authenticated and signed by the instructor. Here is the fingerprint of the public key which signs the document.

BFF1 3D65 59DC 295E 383C 165F A740 45E4 6C4C DBA5

Please identify the key in your public keyring that is used for signing the file, and write down the message in the authenticated announcement. (10 pts)

6. After identifying the right key that signs the announcement, please sign it, trust it ultimately, and list its signatures. Explain the purpose of key signature. (5 pts)
7. Please list all the keys you trust in your key ring. Discuss the pros and cons of the *Web of Trust* model, in comparison with key certification. (5 pts)
8. Finally create a text file containing a short message for the teaching staff of CS291. Encrypt the file with a *trusted public key*, and sign it with your private key. Save it in the ASCII-armored format, and post the resulting ciphertext to the discussion board. (10 pts)