CS 4001 – Using Public Key Cryptography

Task 1: Install an OpenPGP compatible encryption program. You are free to use any program that will encrypt/decrypt/sign/verify messages that follow the OpenPGP standard. We suggest you use GNU Privacy Guard (GPG). We also **strongly** suggest that you use the Enigmail plugin for Mozilla Thunderbird to easily integrate GPG with an e-mail client. The following link will prove useful: http://enigmail.mozdev.org/documentation/quickstart.php.html

Task 2: Generate a public/private key pair for yourself. Use your official GaTech email address as the primary email address. (You may add other user ID's associated with the key for non-official email addresses, but make your GaTech email the primary one.) *If you already have a PGP key, you may use it. Please make sure that your GaTech email address is one of the user ID's associated with it.*

Task 3: Find your instructor's current PGP key. (It should be available on most of the major keyserver, such as http://pgp.mit.edu/). Import this key so that you can use it for task 11. Note that your instructor may have several older keys that have been revoked. You should not use revoked keys.

Task 4: Publish your public key to a public keyserver (Enigmail makes this a one click operation). You may want to publish the key to several keyservers to make it easier to find. (Most keyservers share any new keys with all of the others, but sometimes it takes them a few days.)

Task 5: Determine your key's "Fingerprint", and write it down or print it out. Bring this paper to class.

Task 6: Pair up with at least one other person in class. If you are not 100% convinced of who they are, ask to verify their identity by seeing an official ID (You may determine for yourself if a Buzzcard is acceptable, but a drivers license or passport is more secure). Write down their key's fingerprint, and give them your key's fingerprint. *We suggest you actually pair up with 2 or 3 people, so that if one person fails to sign your key, somebody else will do so.*

Task 7: Go home, download their key(s) from the public key server. Verify that the fingerprints match. If they do, sign their key. This signature tells other people that you trust that the key actually matches up to the person.

Task 8: Upload their public key(s) (that you just signed) back to the public key server (use **pgp.mit.edu**, as this is the server your instructor will search). You may upload to other key servers as well, although all key servers typically share new key information eventually on their own. This should also serve to send your attached signature to the public keyserver. When you search for the key on the keyserver, it should now contain your signature.

Task 9: Verify that they have done the same for your key by searching for your key on the public keyserver and making sure that it has a signature from them. If you download your own key, ("Refresh Key from Keyserver") it will import the signature into your keyring.

Task 10: Send each person who's key you signed an encrypted and signed email telling them that you have signed their key. Also remind them to sign and upload your key if they have not already done so.

Task 11: Send your instructor an email that is both signed and encrypted. In this email, specify who has signed your key, and whose keys you have signed. Include the email addresses associated with each

key you have signed.

Grading:

50 points – Instructor receives a successfully encrypted/signed email from you (and can decode it!).
50 points – Instructor can find your public key in a public key server, at least one other person has signed it, and you have signed one other person's key.