CS380 — Exercise 5

March 2, 2016

Due: Friday, March 11, 2016 before midnight (40 points)

1 Background

This will be a short exercise. The goal will be to send me a signed and encrypted email to my `nmpantic@cpp.edu` email address.

2 Method 1: PGP (or GPG)

Some email clients have support for PGP or GPG, for example Thunderbird has an addon called Enigmail that will handle PGP/GPG. If you would like a simple solution, I would recommend installing Enigmail on Thunderbird, generating a key pair, thne sending me an email by encrypting with my public key, providing your public key, and signing the message with your private key.

You can also create a text file then use PGP/GPG to sign and encrypt it, then attach the encrypted and signed file along with your public key in an email.

My PGP public key has been attached on Blackboard as `nmpantic@cpp.edu.asc`.

3 Method 2: Valid Certificate

Comodo offers a free email certificate at:

https://www.comodo.com/home/email-security/free-email-certificate.php.

You provide your information and a recovery link will be sent to the email specified. Once you have retrieved the certificate, you will need to find out how to properly import it in to your email client of choice.

With Thunderbird, you would do this by going to Account Settings, then Security, then View Certificates, then choose Import at the bottom of the "Your Certificates" tab. Once it has been imported, you can sign emails that you send. Once you send me a signed email, I will respond with a signed email. You can then send me an encrypted email because we have exchanged certificate information.

You may already have my certificate, I sign almost all of my email coming from `nmpantic@cpp.edu`. In that case, you should be able to immediately send me an encrypted email.

If you would prefer not to use Comodo as the certificate authority, you can also try any other certificate authority that offers a free certificate (or pay for one).