Assignment 4: Key Generation

1 OpenSSL and Apache

Using OpenSSL, create a public key pair for a certificate authority "University of Denver". Create another public key pair for "Department of Computer Science". Certify the department key using the university certificate. Using the certified department key, setup an Apache webserver that claims to be the secure webserver for the computer science department.

2 GnuPG

Create a personal public key pair using GnuPG. Publish the (armored) public key on your fake CS department webserver. Use the private key to sign a textfile with the URL of your webserver.

3 Submission

You must submit a file `url.asc` that contains the URL of your SSL-enabled Apache Webserver signed with your private GPG key. At the URL, the webserver should host a webpage with your public GNUPG key.

Note that you must keep your webserver running after the due date until the assignment has been graded. You can use any machine in the HP lab to run Apache (on a port ≥ 1024).