Project 1

Due Tuesday, October 19th, in class

Overview. This part of the project is quite straightforward: you want to obtain a certificate from our CA, Mazdak. To do this, first generate a 1024-bit RSA key pair, depositing the keys in a passphrase-protected PEM file. Then generate a CSR as shown in lecture, with all the relevant information as given in lecture.

Next, send your CSR to our CA, Mazdak. His email address is `Mazdak.Hashemi@colorado.edu`. Allow up to 4 days for processing. If you have done this correctly, you will receive a certificate in reply. Extract your certificate and put it in a safe place (though you don't need to worry about someone else getting ahold of it, of course).

Here is what you turn in to me (in class):

- A copy of your certificate in textual form (using `-text`)
- Proof that you have the correct CA certificate from our website (ie, use OpenSSL to print out the fingerprint of the CA certificate and state it matches the fingerprint you got in class).
- Show a command that demonstrates that your certificate was signed by the CA.

Distance students may email their answers directly to Mazdak.