

Hand in a stapled, printed copy with your answers.

Homework: /SI110/Models and Tools/X.509 Certificates

1. In the context of secure web traffic (i.e. HTTPS,) X.509 certificates certify the mapping of _____ to _____.

2. Suppose a bad guy sets up a replica of **www.navyfcu.org** at **www.navyfcj.org**. This way, an unwary user (who types poorly) might enter their real Navy Federal password into his fake site, so that he can then log into the real Navy Federal site and steal all their money! Will X.509 certificates protect you against this? Explain!

3. You have an online bank account with Barclays, a British bank. You want to access your account, so you put **https://bank.barclays.co.uk/** in the browser's address bar. Match the following:

___ is responsible for making sure the encrypted messages your browser receives really come from the owner of public key K.

a. RSA public key cryptosystem

___ is responsible for verifying that the domain Name **bank.barclays.co.uk** really belongs to the Barclays Bank - the big British bank.

b. X.509 Certificate system

___ is responsible for verifying that public key K really belongs to **bank.barclays.co.uk**.

c. the user