CS 4293

Tutorial 10 Solution

Q1

a) Symantec Corporation.
b) National Science Foundation.
c) Symantec Corporation (CA); The signature can be verified through the subject publick key info, including modulus and exponent.
d) e:65537 ; N: 00:ca:fb:26
e) Signing is more expensive. d is much larger than e and it takes more time compute module exponentiation.
f) Verification of the identity of the subject. To prevent others impersonating and to give detailed credit report for the certification.

Q2

We cannot connect to the web server, because the issued certificate can only be used for the exact same URL specified in the certificate request.

Q3

For public normal usage, the web browser need to verify the validity of CA after checking the certificate of a https server. PKI ensures https can prevent MITM in this case.

How a local https proxy server works. First, a local certification authority can be setup and the administrator tells your browser that this CA is trustworthy. The proxy server uses this local CA to sign his forged certificates. Overall, this is just a local bypass to monitor https traffic.