CS4293 Tutorial 10

Section 1

Group discussion

Q1. The following is an X.509 certificate.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            3d:0e:98:b2:bf:af:fa:9e:99:91:05:64:69:6e:11:2a
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, O=Symantec Corporation,
        OU=Symantec Trust Network,
        CN=Symantec Class 3 EV SSL CA - G3
    Validity
        Not Before: Aug 14 00:00:00 2017 GMT
        Not After : Sep 13 23:59:59 2018 GMT
    Subject: ... C=US/postalCode=22230, ST=Virginia,
        L=Arlington/street=4201 Wilson Blvd,
        O=National Science Foundation, OU=DIS,
        CN=www.nsf.gov
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
                Modulus:
                    00:ca:fb:26:78:06:25:b1:9e:67:1d:69:0b:10:06:
                    cf:25:b6:7d:de:8e:56:80:e1:1c:38:52:62:43:fd:
                    ...
                Exponent: 65537 (0x10001)
Signature Algorithm: sha256WithRSAEncryption
    4b:0d:62:11:b4:dc:78:09:12:c1:1b:24:ff:98:43:58:1c:54:
    0a:34:be:8f:3f:12:8f:17:4a:fe:5b:26:13:1a:5f:a7:87:ad:
    ...
    ba:2c:10:c7:bc:8b:2c:15:6e:0c:d2:d0:8b:74:52:c8:ed:05:
    0b:9b:62:41
```

(a) Who issues the certificate?

(b) Who is the owner of the certificate?

(c) Who generated the signature on this certificate, and how can this signature be verified?

(d) The public key contained in this certificate is based on the RSA algorithm. Using the RSA algorithm, to encrypt a message M, we calculate M^e mod n. What is the value of e and n in this public key? If a number is too large, you only need to write down its first four bytes.

(e) Which one is more computationally expensive, the signing process of the above digital signature or the verification process of the above digital signature? Please briefly explain.

(f) Before issuing the certificate, the CA needs to do a verification regarding the subject field. Please describe what this verification is, and why it is necessary.

Q2. Instead of typing https://www.example.com in the URL field of a browser, we first get the IP address of the web server, which is 93.184.216.34, and we then directly type https://93.184.216.34 into the browser. Describe whether we will be able to connect to the web server.

Q3. We know that HTTPS can defeat man-in-the-middle attacks. However, we also know that HTTPS proxy can be installed to monitor and modify HTTPS traffic. A proxy is basically a “man” in the middle. Does this mean that HTTPS is still subject to man-in-the-middle attacks? Please explain.

Section 2

Hands-on exploration (see Assignment 3)

Procedures:

1. **Become a Certificate Authority (CA)**
2. **Create a Certificate for an organization.**
3. **Set up a local web server to try the certificate.**