CSCI3403 Project 2

Practical Use of Public Keys and Certification Authorities

Jason Lubrano, Teagan Peters, Andrew Gitlin, Darian Valdez, Milan Formanek

Part 1: Certificates

1A. When does the canvas.colorado.edu certificate expire?

Friday, April 17, 2020

1B. According to the certificate (ignoring extensions), what can this public key be used for?

- Critical
- Signing
- Key Encipherment

1C. The algorithm used is RSA and an RSA public key consists of a modulus and an exponent (see Data Security slides on Public Key Cryptography). How many bits are in the modulus?

2048

1D. What is the modulus? List the modulus in the hexadecimal format.

```
Modulus (2048 bits):
aa 0c a2 92 82 e4 66 fc 5e 5a 5d d9 73 41 3e f3
b4 64 ef 83 b1 12 16 8a 45 77 a8 bb 1f f0 70 3d
6e ed 80 57 4d 2e ec d2 f9 f4 47 bc 32 b9 b9 1b
a8 b4 23 9e 24 bd a6 81 b6 c3 aa a2 56 6b a4 1a
b8 cb 9f 93 d2 b7 d4 d8 fd 2e 3f 25 84 96 4f 7f
50 e4 87 94 f0 57 45 1d 0f 67 35 5a 44 88 c4 78
bf 7f dd 68 0a 95 b5 1b 00 06 d4 82 3d 59 ce 4b
ef 98 72 e2 ae 18 ef dd e5 60 47 55 24 d0 b6 96
5d 64 65 d0 f5 4e 07 b2 a3 ee 2c bc b1 8c 3e 6f
ed 28 36 30 1c 0e 3f ef e0 57 99 21 ea 77 fc 09
a4 85 96 bb 9e bb 32 b8 09 b5 50 71 6a 38 c9 ee
68 d0 79 f8 a9 f0 ab 5d f9 0b 63 f5 37 d3 19 77
8f c3 72 70 3a c9 4d 21 c1 c7 19 b3 4a 9d 47 9d
```

```
0b e7 35 be d8 6e f9 ac ef 6a 27 8e 37 87 7d b2
a0 d6 5c b4 d7 93 ab d3 88 9d 59 1a 33 97 4b 39
eb 3c ad 62 62 ee 8a a6 ad b4 32 75 a4 83 d1 45
```

1E. What is the exponent?

Exponent (24 bits):
65537

1F. Extra Credit: we know the modulus is n = p*q where p and q are primes. We know n from problem 1C. For 100 extra credit points, find p and q.

P = 7
Q = 3
Proof: we bought 10000 GPUs and rented a server farm to break RSA
The way that it is.

Part 2: Authenticating Certificates

2A. What is the Certificate Authority for canvas.colorado.edu?

DigiCert Inc.

2B. Explain how the certificate authority is used to authenticate the canvas.colorado.edu certificate.

DigiCert serves as a trusted third party and they verify the authenticity of secure websites on behalf of a web browser. A trusted third party is trusted by both Canvas and the web browser and facilitates the interactions between the two.

2C. What algorithm is used to sign the canvas.colorado.edu certificate?

PKCS #1 SHA-256 With RSA Encryption

2D. How many bytes are in the signature?

Size: 256 Bytes / 2048 Bits

2E. List the signature that was produced by the CA (use hexadecimal to represent the signature).

```
Size: 256 Bytes / 2048 Bits
78 c4 6f de 3b fb e9 6c f9 29 c8 20 31 aa ad d9
dc 0b 85 62 96 8a f9 27 37 e9 70 83 c4 74 a0 32
f0 1a 87 8a ad 9d 93 46 08 7c e5 2c c8 ee f6 12
24 c3 cc d9 35 17 e7 4a 05 9f f2 96 3d a2 3c b0
f6 38 2e 5d 4d d5 6a 5c 0b 07 4a af cf bb 43 7b
dd b5 99 c8 ab 53 29 88 70 98 f1 b8 50 0d 02 a0
7f b4 1f 95 83 63 ee 82 b5 80 96 71 81 e3 ca d2
b4 5c ea 16 c9 10 4c e5 98 66 05 c7 9b 6b 56 6b
d5 92 a1 7d bb 9e 45 b0 27 0b 3b 84 55 ee f2 3e
4b ed 8b 71 65 92 7c d0 ff 54 d3 1f 97 92 0f ee
11 cc 08 b3 35 43 c6 3f 69 71 e9 d5 8d 12 b1 27
33 a1 ba fd ca 1f da 97 24 98 fe 91 f8 02 98 90
46 95 ff 33 5b 15 dd 27 73 49 e1 ce a5 f9 95 0c
88 ff 93 3a 22 a5 46 ac a7 17 ee 37 91 44 f3 99
a5 03 db 12 59 70 68 7e 4d ac cf 1d f5 8d bd f2
92 26 c7 de 90 cc c2 1a 19 97 91 dc 07 07 dc 67
```

Part 3: Certificate Authorities

3A. When does the CA certificate expire?

Sunday, November 9, 2031, 5:00:00 PM
(Monday, November 10, 2031, 12:00:00 AM GMT)

3B. According to the certificate (ignoring extensions), what can the CA public key be used for?

- Critical
- Signing
- Certificate Signer
- CRL Signer

3C. Again, the algorithm used is RSA and an RSA public key consists of a modulus and an exponent (see Lecture 6 slides 15-16). How many bits are in the modulus?

2048 bits

3D. What is the modulus? List the modulus in hexadecimal format.

```
Modulus (2048 bits):
e2 3b e1 11 72 de a8 a4 d3 a3 57 aa 50 a2 8f 0b
77 90 c9 a2 a5 ee 12 ce 96 5b 01 09 20 cc 01 93
a7 4e 30 b7 53 f7 43 c4 69 00 57 9d e2 8d 22 dd
87 06 40 00 81 09 ce ce 1b 83 bf df cd 3b 71 46
e2 d6 66 c7 05 b3 76 27 16 8f 7b 9e 1e 95 7d ee
b7 48 a3 08 da d6 af 7a 0c 39 06 65 7f 4a 5d 1f
bc 17 f8 ab be ee 28 d7 74 7f 7a 78 99 59 85 68
6e 5c 23 32 4b bf 4e c0 e8 5a 6d e3 70 bf 77 10
bf fc 01 f6 85 d9 a8 44 10 58 32 a9 75 18 d5 d1
a2 be 47 e2 27 6a f4 9a 33 f8 49 08 60 8b d4 5f
b4 3a 84 bf a1 aa 4a 4c 7d 3e cf 4f 5f 6c 76 5e
a0 4b 37 91 9e dc 22 e6 6d ce 14 1a 8e 6a cb fe
cd b3 14 64 17 c7 5b 29 9e 32 bf f2 ee fa d3 0b
42 d4 ab b7 41 32 da 0c d4 ef f8 81 d5 bb 8d 58
3f b5 1b e8 49 28 a2 70 da 31 04 dd f7 b2 16 f2
4c 0a 4e 07 a8 ed 4a 3d 5e b5 7f a3 90 c3 af 27
```

3E. What is the exponent?

Exponent (24 bits):
65537

3F. The CA's certificate includes a signature. Who produced that signature and what purpose does it serve?

DigiCert Inc

The purpose of the signature is to prove that the certificate belongs to who it claims to belong to. The CA has verified this and their signature says that you can trust the certificate. Since DigiCert is a known trusted authority, they can sign their own certificates.

Part 4: Authenticating You!

4A. Explain how the canvas.colorado.edu website authenticates you.

Canvas uses a similar procedure to verify a user as the user verifies them. Signatures generated using public key cryptography can be used to verify the origin and validity of messages. When the client wishes to communicate with Canvas. The book gives a few key steps that summarize the process.

1. User software creates a pair of keys, one public and one private
2. Client prepares an unsigned certificate that includes the user ID and user's public key
3. The user provides the unsigned certificates to a CA in some secure manner through a secured channel
4. The CA creates a signature:
    a. CA uses a hash function to calculate the hash code of the unsigned certificate. A hash function is one that maps a variable-length data block or message into a fixed-length value called a hash code, such as the SHA family.
    b. CA generates a digital signature using the CA's private key and a signature generation algorithm.
5. CA attaches the signature to the unsigned certificate to create a signed certificate.
6. CA returns the signed certificate to the client
7. The client may provide the signed certificate to any other user
8. Any user may verify that the certificate is valid by:
    a. The user calculates the hash code certificate (not including the signature).
    b. The user verifies the digital signature using CA's public key and the signature verification algorithm. The algorithm returns a result of either signature valid or invalid.

(Computer Security, Principles and Practice, Public Key Certificates p.52-53)

Part 5: Certificate Challenges

Visit the website https://self-signed.badssl.com
5A. According to the certificate (ignoring extensions), what can the certificate public key be used for?

This certificate does not contain the Usages field.

“The certificate is not trusted because it is self-signed”
HTTP Strict Transport Security: false
HTTP Public Key Pinning: false

A Self-Signed certificate is signed by the same entity whose identity it certifies.

5B. Again, the algorithm used is RSA and an RSA public key consists of a modulus and an exponent. How many bits are in the modulus?

2048 bits

5C. What is the modulus? List the modulus in the hexadecimal format.

```
Modulus (2048 bits):
c2 04 ec f8 8c ee 04 c2 b3 d8 50 d5 70 58 cc 93
18 eb 5c a8 68 49 b0 22 b5 f9 95 9e b1 2b 2c 76
3e 6c c0 4b 60 4c 4c ea b2 b4 c0 0f 80 b6 b0 f9
72 c9 86 02 f9 5c 41 5d 13 2b 7f 71 c4 4b bc e9
94 2e 50 37 a6 67 1c 61 8c f6 41 42 c5 46 d3 16
87 27 9f 74 eb 0a 9d 11 52 26 21 73 6c 84 4c 79
55 e4 d1 6b e8 06 3d 48 15 52 ad b3 28 db aa ff
6e ff 60 95 4a 77 6b 39 f1 24 d1 31 b6 dd 4d c0
c4 fc 53 b9 6d 42 ad b5 7c fe ae f5 15 d2 33 48
e7 22 71 c7 c2 14 7a 6c 28 ea 37 4a df ea 6c b5
72 b4 7e 5a a2 16 dc 69 b1 57 44 db 0a 12 ab de
c3 0f 47 74 5c 41 22 e1 9a f9 1b 93 e6 ad 22 06
29 2e b1 ba 49 1c 0c 27 9e a3 fb 8b f7 40 72 00
ac 92 08 d9 8c 57 84 53 81 05 cb e6 fe 6b 54 98
40 27 85 c7 10 bb 73 70 ef 69 18 41 07 45 55 7c
f9 64 3f 3d 2c c3 a9 7c eb 93 1a 4c 86 d1 ca 85
```

5D. What is the exponent?

Exponent (24 bits):
65537

5F. Explain why this certificate is not trusted.

This certificate is not trusted because the certificate was self-signed from an unauthorized, untrusted authority. In order to be valid, the certificate would have to come from somewhere like DigiCert who is a known trusted authority.