3308 Cyber Security Authentication Project

Minhchau
Andre
Brennon
Paris
Dominic

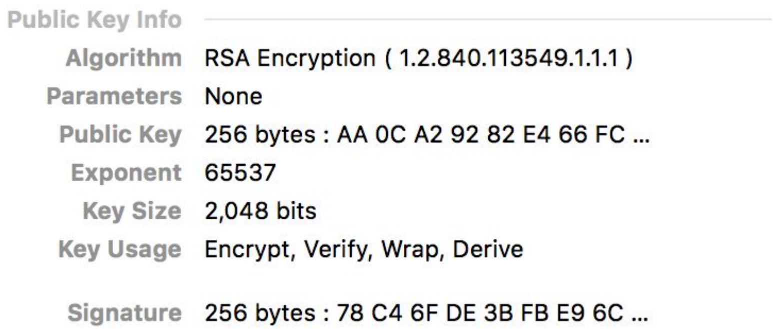
Part 1: Certificates

The course regularly uses canvas.colorado.edu. Your browser is able to authenticate this website using a certificate. You must find the certificate for the canvas.colorad.edu website and answer the following questions

a. When does the canvas.colorado.edu certificate expire?
b. According to certificate (ignoring extensions), what can this public key be used for?
c. 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?
d. What is the modulus? List the modulus in hexadecimal format.
e. What is the exponent?
f. 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.

Answers:

a. This certificate expires Friday, April 17, 2020 at 6:00 am Mountain Daylight Time.
b. Under Public Key Info -> Key Usage: The public key is used to **Encrypt, Verify, Wrap, and Derive.**



Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	256 bytes : AA 0C A2 92 82 E4 66 FC ...
Exponent	65537
Key Size	2,048 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	256 bytes : 78 C4 6F DE 3B FB E9 6C ...

c. There are 2048 bits in the modulus.
d. The modulus is:

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

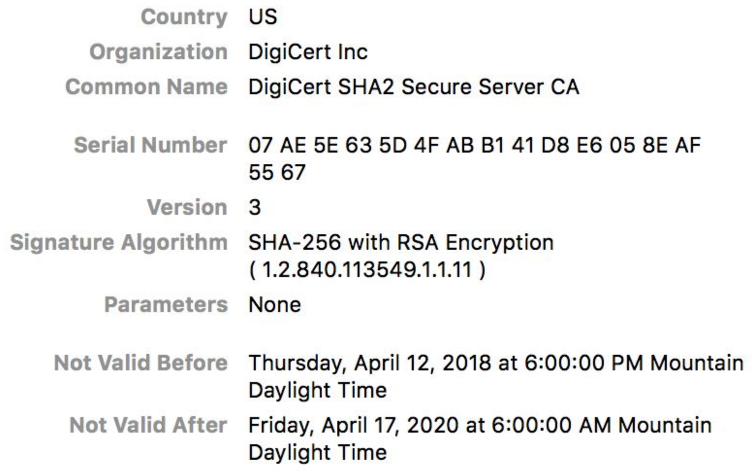
```
32 B9 B9 1B A8 B4 23 9E 24 BD A6 81 B6 C3 AA A2 56 6B A4 1A B8 CB
9F 93 D2 B7 D4 D8 FD 2E 3F 25 84 96 4F 7F 50 E4 87 94 F0 57 45 1D
0F 67 35 5A 44 88 C4 78 BF 7F DD 68 0A 95 B5 1B 00 06 D4 82 3D 59
CE 4B EF 98 72 E2 AE 18 EF DD E5 60 47 55 24 D0 B6 96 5D 64 65 D0
F5 4E 07 B2 A3 EE 2C BC B1 8C 3E 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
```

e. The exponent is 65537

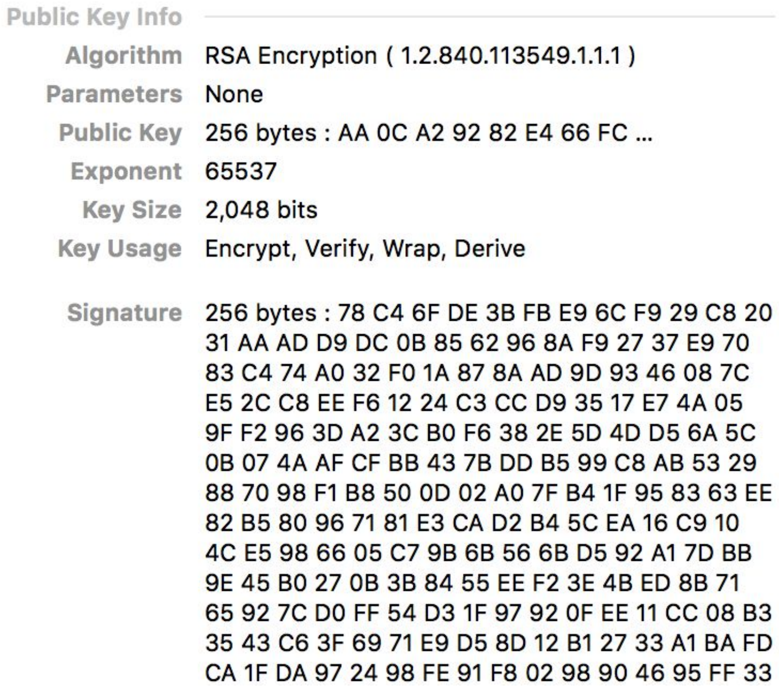
Part 2: Authenticating Certificates

An adversary can produce a false canvas.colorado.edu certificate. Your browser must have some way to authenticate the certificate and this role performed by a Certificate Authority (CA).

a. What is the Certificate Authority for canvas.colorado.edu?
b. Explain how the certificate authority is used to authenticate the canvas.colorado.edu certificate.
c. What algorithm is used to sign the canvas.colorado.edu certificate?
d. How many bytes are in the signature?
e. List the signature that was produced by the CA (use hexadecimal to represent the signature).



Country	US
Organization	DigiCert Inc
Common Name	DigiCert SHA2 Secure Server CA
Serial Number	07 AE 5E 63 5D 4F AB B1 41 D8 E6 05 8E AF 55 67
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None
Not Valid Before	Thursday, April 12, 2018 at 6:00:00 PM Mountain Daylight Time
Not Valid After	Friday, April 17, 2020 at 6:00:00 AM Mountain Daylight Time



Public Key Info

Algorithm RSA Encryption (1.2.840.113549.1.1.1)

Parameters None

Public Key 256 bytes : AA 0C A2 92 82 E4 66 FC ...

Exponent 65537

Key Size 2,048 bits

Key Usage Encrypt, Verify, Wrap, Derive

Signature 256 bytes : 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

Answers:

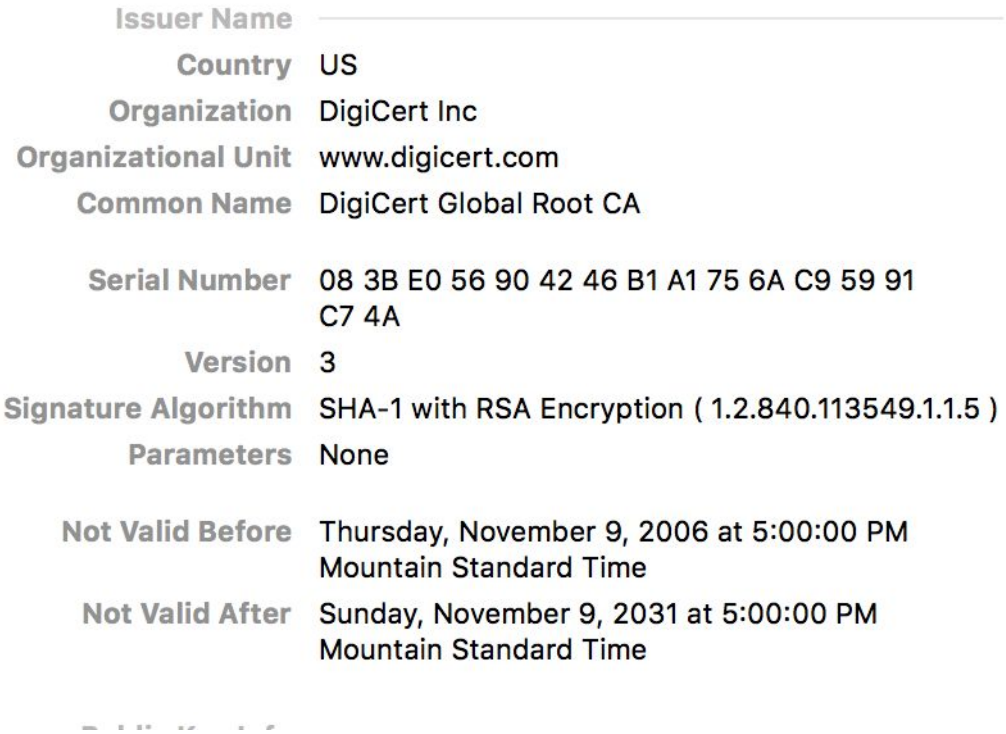
a. The certificate authority for Canvas is a company called DigiCert Inc.
b. The certificate authority prevents man in the middle attacks by authenticating the validity of the site. The CA verifies the identity of the site requesting authentication, and when the site sends the user the site's public key, it is digitally signed with a signature generated with the CA's private key. The user then verifies the signature with the CA's public key to see if the signature is valid. This prevents fake sites from authenticating because the CA would not accept the fake site's identity, and if the site tries to add a fake digital signature, it will be incorrect since they would need the CA's private key to do so.
c. DigiCert has used SHA-256 with RSA encryption to sign the Canvas certificate.
d. The signature is 256 bytes long.
e. 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

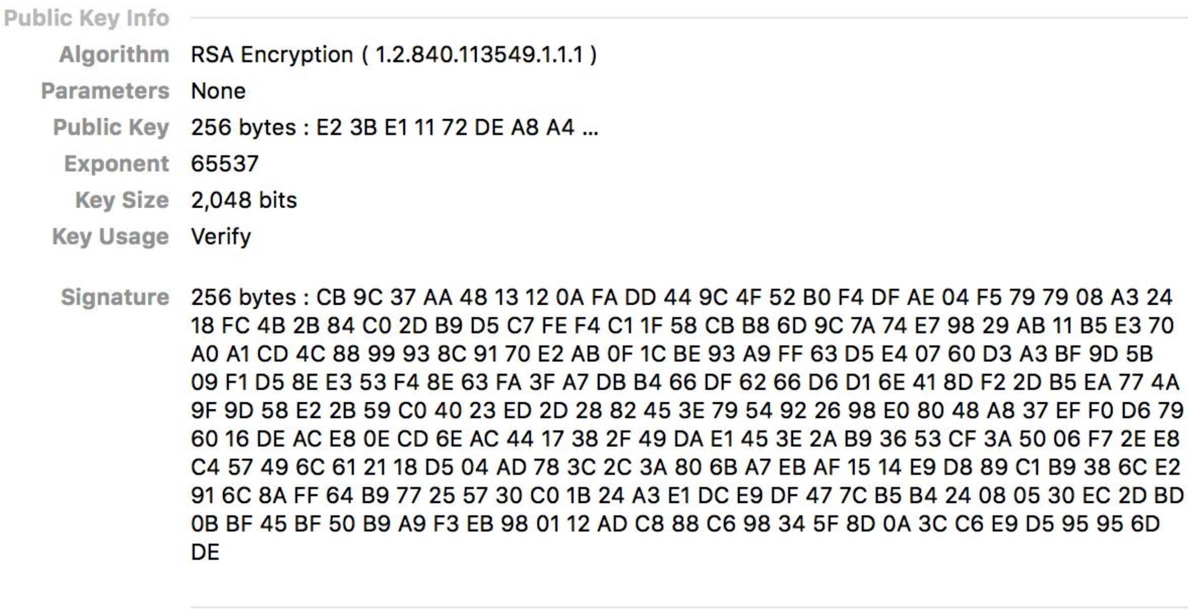
Part 3: Certificate Authorities

Having identified the Certificate Authority (CA) used to authenticate the canvas.colorado.edu certificate, let's examine the properties of the CA itself.

a. When does the CA certificate expire?
b. According to certificate (ignoring extensions), what can the CA public key be used for?
c. 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?
d. What is the modulus? List the modulus in hexadecimal format.
e. What is the exponent?
f. The CA's certificate includes a signature. Who produced that signature and what purpose does it serve?



Issuer Name	
Country	US
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Common Name	DigiCert Global Root CA
Serial Number	08 3B E0 56 90 42 46 B1 A1 75 6A C9 59 91 C7 4A
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters	None
Not Valid Before	Thursday, November 9, 2006 at 5:00:00 PM Mountain Standard Time
Not Valid After	Sunday, November 9, 2031 at 5:00:00 PM Mountain Standard Time



Public Key Info

Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	256 bytes : E2 3B E1 11 72 DE A8 A4 ...
Exponent	65537
Key Size	2,048 bits
Key Usage	Verify
Signature	256 bytes : CB 9C 37 AA 48 13 12 0A FA DD 44 9C 4F 52 B0 F4 DF AE 04 F5 79 79 08 A3 24 18 FC 4B 2B 84 C0 2D B9 D5 C7 FE F4 C1 1F 58 CB B8 6D 9C 7A 74 E7 98 29 AB 11 B5 E3 70 A0 A1 CD 4C 88 99 93 8C 91 70 E2 AB 0F 1C BE 93 A9 FF 63 D5 E4 07 60 D3 A3 BF 9D 5B 09 F1 D5 8E E3 53 F4 8E 63 FA 3F A7 DB B4 66 DF 62 66 D6 D1 6E 41 8D F2 2D B5 EA 77 4A 9F 9D 58 E2 2B 59 C0 40 23 ED 2D 28 82 45 3E 79 54 92 26 98 E0 80 48 A8 37 EF F0 D6 79 60 16 DE AC E8 0E CD 6E AC 44 17 38 2F 49 DA E1 45 3E 2A B9 36 53 CF 3A 50 06 F7 2E E8 C4 57 49 6C 61 21 18 D5 04 AD 78 3C 2C 3A 80 6B A7 EB AF 15 14 E9 D8 89 C1 B9 38 6C E2 91 6C 8A FF 64 B9 77 25 57 30 C0 1B 24 A3 E1 DC E9 DF 47 7C B5 B4 24 08 05 30 EC 2D BD 0B BF 45 BF 50 B9 A9 F3 EB 98 01 12 AD C8 88 C6 98 34 5F 8D 0A 3C C6 E9 D5 95 95 6D DE

Answers:

a. The CA certificate expires Sunday, November 9, 2031 at 5:00 pm

b. The CA public key can be used for only verifying. So like explained in part 2B, the CA will sign the site's public key when being sent to the user. This allows the user to decrypt and verify that the site they are communicating with is real.

c. The modulus is 2,048 bits

d. The modulus is 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

e. The exponent is 65537

f. DigiCert Inc produced this signature. The purpose for this is that a user can receive this signature, decrypt it using the CA's public key and then they can verify that the site has been approved by this third party as a legit site.

Part 4: Authenticating You!

The answers above help explain how your web browser authenticates canvas.colorado.edu. But how does canvas.colorado.edu authenticate you?

a. Explain how the canvas.colorado.edu website authenticates you.

a. First, the server requests authentication from the user through something they know, eg. their username and password. Canvas uses the SSL protocol, which validates the server as we discussed above through the CA. SSL can also be used to encrypt data, as the server includes its public key with the certificate. The user generates a symmetric key for the session, and encrypts it with server's public key, and sends it across the network. The server uses its private key to decrypt the message, and now both parties have the session symmetric key. The user then sends their username and password within the SSL session encrypted with the symmetric session key. The server decrypts this with the shared session key, checks the username and password against its records to determine user authenticity and if authentic, allows access privileges.

Part 5: Certificate Challenges

Visit the website https://self-signed.badssl.com

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

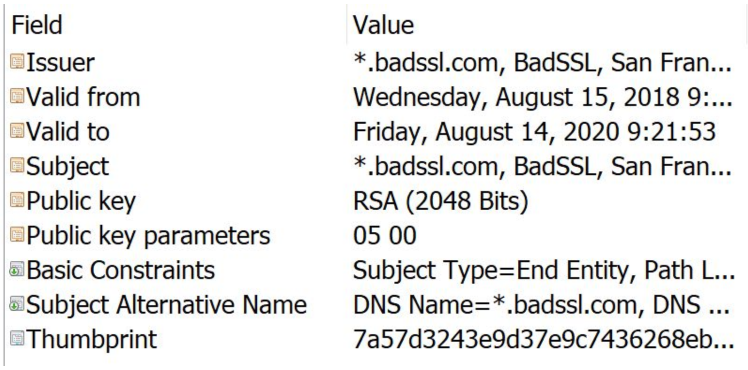
b. Again, the algorithm used is RSA and an RSA public key consists of a modulus and an exponent (see Lecture 6 slides 15-16). How many bits are in the modulus?

c. What is the modulus? List the modulus in hexadecimal format.

d. What is the exponent?

e. Explain why this certificate is not trusted.

Answers:



Field	Value
Issuer	*.badssl.com, BadSSL, San Fran...
Valid from	Wednesday, August 15, 2018 9:...
Valid to	Friday, August 14, 2020 9:21:53
Subject	*.badssl.com, BadSSL, San Fran...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Basic Constraints	Subject Type=End Entity, Path L...
Subject Alternative Name	DNS Name=*.badssl.com, DNS ...
Thumbprint	7a57d3243e9d37e9c7436268eb...

a. There is not any information on key usage for the public key nor the certificate.

b. There is 2,048 Bits in the modulus.

c. The modulus is:

```
02 82 01 01 00 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
```

d. The exponent is 65537.

e. This certificate is not trusted because it is a self-signed certificate. Self-signed certificates are not trusted by our browsers because they are generated by a server instead of a CA. In other words, the site has not been verified to be legitimate because it doesn't have a CA.