Jeff Kremer
11524078
CptS 427
Homework 2

1.
   a) wsu.edu
   b) 2048 bit, per NIST_SP800-57 this is the minimum size a key should be for non-classified use. Therefore the key is adequately secure.
   c) TLSv1.2
   d) Cipher is DHE-RSA-AES256-GCM-SHA384.
      1.
   e) The master key value is:
      83158C822B8E53AA2C87ACCBC9DD2E13D2304DAAC141328A94B362F8558734
      B9996B2D59EF06E828F6B0548E6AA739CC

2.
   a) wsu.edu
   b) Let's Encrypt Authority x3, and yes they are trusted.
   c) 00:ba:f4:86:ac:55:6f:10:44:e3:41:4a:b8:5b:d1:
      a8:d9:49:5a:8e:7d:ab:da:ab:56:8e:4d:8f:82:a4:
      9c:d4:13:a4:0e:56:b0:d8:27:9e:3c:97:c1:d7:91:
      f7:17:61:e0:fc:9b:cb:38:7b:3d:13:2c:f9:49:1a:
      bb:ce:44:de:d0:bf:11:fd:0a:39:8f:30:4d:f2:99:
      1a:c7:aa:85:77:c7:5a:e6:59:97:78:ac:2c:30:72:
      fc:6a:b6:38:a9:6f:3b:98:34:5f:a5:ee:24:c7:73:
      e1:39:11:f8:9e:19:d3:ac:3e:38:42:11:ad:4c:e5:
      dd:6d:3c:a1:cc:98:a9:72:0b:82:d6:69:24:28:b5:
      3f:a8:7b:2c:4c:09:e9:b7:4b:06:bc:12:a8:0e:80:
      eb:b9:01:8b:0f:81:1f:86:ed:f9:16:63:3a:cc:ea:
      bf:9b:d7:95:3e:1b:a0:e8:ce:24:e8:4d:42:63:06:
      40:60:bd:a8:96:1e:98:95:3e:56:0d:7d:c9:a2:87:
      dc:37:48:b9:d7:81:0b:c6:c6:14:8f:a5:e7:3b:13:
      30:14:e5:f7:a2:2b:6a:a4:48:05:69:dc:c7:d5:22:
      6e:e0:d5:9a:cc:e9:5b:b3:42:47:30:e6:ce:ec:a5:
      d4:45:0e:8c:cb:81:6b:6c:ab:01:26:05:2e:48:d1:
      8e:cf
   d) the certificate Is valid from 08/20/2019 to 11/18/2019, so yes the cert is valid

3.
   a) TLS versions 1.0, 1.1, 1.2 are all supported.
   b) Only ECDHE-RSA-AES256-SHA is on the server. AES ciphers are theoretically susceptible to man in the middle attacks (source: *Andrey Bogdanov; Dmitry Khovratovich; Christian Rechberger (2011-08-17).* *"Biclique Cryptanalysis of the Full AES"*)

4. DES operates on 64-bit blocks, and have a 56-bit key. AES operates on 128-bit blocks, and has keys of length 128, 192, or 256 bits. The key length is tied to the upper bound of the algorithm's security, and thus the security of the cipher.

5. Commands:
   a) DES decrypt: openssl enc -d -des-ecb -in message_des.enc -out file_decrypt.txt -K 01234567
   b) AES decrypt: openssl enc -aes-128-ecb -d -in message_aes.enc -out file.txt -K 0123456789abcde

6. Yes and no, the AES encrypted text does not provide any information about the original message, no matter how much of the encrypted text you have, without the key. However, the DES encrypted text has repeating characters for “attack...”, thus giving clues to the message. Therefore, AES provides perfect secrecy, while DES does not.

7. HMAC
   a) initial HMAC: b113196f33866ada27c9a2650d2edd6c8277e106
   b) changed message HMAC: 6b720f9ce6ff233b453aafbad34bd3eb58f071f9
   c) changed key HMAC: 4412529627442acb9372144c64014e80f697c905