50.020 Network Security Lab 3 pt 1| 1002853 Wong Chi Seng

Q1: What's the Content-Type for a record containing "Application Data"?

Content-Type: 23

Q2: What's the version of the TLS protocol?

Version 1.0

Q3: What are the time (GMT seconds since midnight Jan 1, 1970) and random bytes (size 28) which are used later to generate the symmetric encryption key?

1,343,715,539 s, 16c25064f7cb0209b336ab332d969b8e091d26d4ccd04b731d7e550f

Q4: What is the list of cipher suites, which dictate the key exchange algorithm, bulk encryption algorithm (with key length), MAC, and a psuedo-random function?

Cipher Suites (23 suites)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
- Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
- Cipher Suite: TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
- Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
- Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- Cipher Suite: TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x009a)
- Cipher Suite: TLS_DHE_DSS_WITH_SEED_CBC_SHA (0x0099)
- Cipher Suite: TLS_RSA_WITH_SEED_CBC_SHA (0x0096)
- Cipher Suite: TLS_RSA_WITH_RC4_128_SHA (0x0005)
- Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
- Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
- Cipher Suite: TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
- Cipher Suite: TLS_RSA_WITH_DES_CBC_SHA (0x0009)
- Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0014)
- Cipher Suite: TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA (0x0011)
- Cipher Suite: TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x0008)
- Cipher Suite: TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x0006)
- Cipher Suite: TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x0003)
- Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Q5: How is the compression methods set? Why is it set like that?

Deflate, DEFLATE allows the sending compressor to select from among several options to provide varying compression ratios, processing speeds, and memory requirements.

Q6: What's the Cipher method chosen by the Server?

TLS_RSA_WITH_RC4_128_SHA

Q7: What's the certificates messages in this step?

The certificate messages indicate the types of certificates transferred from the client to the server

Q8: What's the Content-Type for Change Cipher Spec message?

22

Q9: What's the Change Cipher Spec message? What's its size?

Handshake message, 36