MAS433 Cryptography: Assignment 2
Deadline: 08:30am 01.12.2010

Submission Instructions:

1. Deadline: 08:30 am, 01 December 2010 (Wednesday).
2. You need to email your answers to the instructor (wuhj@ntu.edu.sg) with the email subject "MAS433 Assignment 2 Answers".

Problems: TLS/SSL is used to protect the communication between the NTU edventure server and its users.

1. Briefly describe the difference between TLS and SSL. (10 Marks)
2. Briefly describe the contents in a public key certificate. (10 Marks)
3. Describe the details of the simple TLS handshake. (10 Marks)
4. When you connect to the edventure server,
   - 4.1 ClientHello. (10 Marks)
     - 4.1.1 Which browser are you using?
     - 4.1.2 What is the highest TLS protocol version your browser is supporting?
     - 4.1.3 What are the CipherSuites supported by your browser?
   - 4.2 ServerHello. (10 Marks)
     - 4.2.1 What is the TLS version being used between the edventure server and your browser?
     - 4.2.2 What is the CipherSuite being used between the edventure server and your browser?

4.3 Public key certificate. (20 Marks)

4.3.1 What are the cryptosystems being used for generating the public key certificate of the NTU edventure server?

4.3.2 What is the name of the company that issued the public key certificate of the NTU edventure server?

4.3.3 What is the validity period of the current public key certificate of the NTU edventure server?

4.3.4 What is the public key of the NTU edventure server? Is it strong?

4.3.5 (Bonus Problem) What is the private key of the NTU edventure server? (100 marks)

4.4 List the cryptosystems that are used to protect the communication between your computer and the NTU edventure server. (10 Marks)

4.5 Explain why the public key certificate is needed in TLS/SSL. (10 Marks)

4.6 Explain how the secret keys are established between your computer and the edventure server. (10 Marks)

Hints:

1. Google
2. Wikipedia: TLS/SSL, public key certificate, ...
3. You need to install a network traffic analyzer to capture and analyze the internet traffic between your computer and the NTU edventure server.

   3.1 You may install the network analyzer "WIRESHARK" on your computer. You can install all the features of WIRESHARK. You may search the tutorial of WIRESHARK for detail instruction on how to use WIRESHARK. Some brief introduction is given below.

3.2 After starting the WIRESHARK for the first time, from the menu, click “capture”, click “options”, unmark “capture packets in promiscuous mode”, then click “start”, then WIRESHARK starts capturing the packets.

3.3 To capture the communication data between your computer and the eventure server, you may start the capturing of the WIRESHARK, then type the URL of eventure server in your browser, press ”enter” key, then you can stop the capturing of the WIRESHARK, and start analyzing those packets.

3.4 After packet capturing, the WIRESHARK window is divided into three parts. The upper part lists those packets, the middle part shows the “translated” content of each packet (you can find the detailed packet information there), the lower part gives the hexadecimal data in each packet.

3.5 To simply the analysis, you can organize the order of packets by clicking “protocol” in the “WIRESHARK” window. You only need to analyze those TLS/SSL packets.