Assignment #4 for Computer Networks (CNT 4004) for Fall 2018

Due October 11, 2018 at the start of class

This assignment primarily covers material from the remain of chapter 3 (so section 3.5 to end) and chapter 8 of the textbook and from class lecture. Each problem is worth 10 points.

Problem #1

Answer the following short-answer questions about TCP.

a) What does the FIN flag signify and what is used for?

b) What are two ways to close a connection – why is one way preferred?

c) Why is the TCP header longer than the UDP header?

d) We talked about the "old" and "new" RTO formulas. What was the incentive for the new RTO formulas?

e) Sketch the "sawtooth" throughput graph for a TCP connection and explain what it occurring. The answer for this question will be longer than the answers for (a) through (d) above.

Problem #2

Do Problem P29 (page 295) from the text book.

Problem #3

Do Problem P33 (page 296) from the text book.

Problem #4

Do Problem P42 (page 298) from the text book.

Problem #5

Fairness and throughput are often trade-offs in congestion control. Two definitions of fairness are proportional fair and max-min fair. Consider a link with bandwidth 10 Mb/s and four sources (call them A, B, C, and D) with the following bandwidth demand 2 Mb/s, 3 Mb/s, 10 Mb/s, and 1 Mb/s, respectively. Give the proportional fair and max-min fair allocations for each source. Which allocation scheme encourages "lying" and why?

Problem #6

Do Problem P12 (page 668) from the text book.

Problem #7

Do Problem P18 (page 669) from the text book.

Problem #8

Explain how SSL works such that 1) no previously (to the connection) shared secret is needed between sender and receiver, and 2) a PKC is not used for encrypting and decrypting the data flow in the SSL connection. Explain why using a PKC for the data flow is undesirable.

Problem #9

Take a look at tumbler here: http://tumbler.sourceforge.net/. Briefly describe (in your own words!) what service tumbler provides. Explain how tumbler maintains confidential communications between the sender and receiver. Explain how tumbler minimizes – but does not entirely prevent – the possibility of playback attack by an adversary. Explain how a playback attack could be achieved.

Problem #10

For your project may wish to use a hash function to generate signatures. MD5 and SHA256 are cryptographically strong hash functions. For this class you may use CRC32 as a hash function despite it not being strong. For this problem you may use the CRC32 code found here on the class source code page. Generate and give the CRC32 for the following string "TRANSFER" (encoded as ASCII). Now, find another string of length eight bytes that generates the same CRC32 (as "TRANSFER" generates). For full credit your new string should be valid ASCII characters A thru Z. If you cannot implement a method to find a the string with same CRC32, explain how you would do it to earn partial credit.