CME 451 – Transport Networks – Winter 2015
Assignment 6
Due Date: April 7, 2016

This assignment contains 9 problems. Completed assignments must be submitted on the specified due date by 4:30pm in the CME451 assignment box (second floor, across Room 2C94E). Late assignments will not be marked, and will be given a mark of zero.

Marking scheme:

- 30% completion mark
- 70% based on a selected set of problems (to be determined by the marker)

Note to students: in the following you will NOT find full solutions, but instead sufficient hints towards the full solutions. When appropriate, pointers to appropriate lecture slides are provided in parentheses. When in doubt, feel free to contact the teaching assistant or the instructor for further help on your assignments.

---

1. Read chapters 23, 30, 31 (Forouzan textbook).
2. Utilizing appropriate block diagrams (identifying at least plaintext, ciphertext, encryption, decryption, and keys), compare and contrast symmetric-key vs. asymmetric-key cryptography schemes.

   Solution: (C30, Slide 9) Should note whether the decryption keys are related to the encryption keys.

3. In asymmetric-key cryptography, how many keys are needed if Alice and Bob want to communicate with each other?

   Solution: (C30, Slides 7-9) Find the requirements for full duplex communications (i.e., both directions).

4. In the context of network security, what are the (five) services provided by cryptography? Briefly describe them.

Solution: (C31, Slide 11)

5. Suppose a message is made of 10 numbers between 00 and 99. A function is created to compute a digest by adding all numbers modulo 100. Does this function satisfy the criteria for a (good) hash function?

Solution: (C31, Slide 20)

6. At a party, which is more probable: (i) a person with a particular birthday; (ii) two (or more) persons having the same birthday? How are these two cases related to the criteria of a hash function?

Solution: (C31, Slide 20)

7. Compare the following: (i) creating a MAC; (ii) signing a hash.

Solution: (C31, Slides 27, 33)

8.

(a) Describe the concept of a SYN flood, and explain why/when it is a problem.

Solution: (C05, Part 2, Slide 33; C05, Part 3, Slide 21) Describe the potential abuse in a three-way handshaking system in TCP.

(b) Design a system (with suitable pseudo-codes and/or block diagrams) to counteract SYN flooding. Explain the assumptions and requirements necessary to adopt and deploy your design.

Solution: (C05, Part 3, Slide 21) (C31, Slide 20) Utilize HMAC to implement the cookie.

9. In the context of entity authentication, explain the challenge-response approach.

Solution: (C31, Slides 38-40) Briefly define entity authentication, and explain the time-varying nature of this approach.