CPSC 313 Introduction to Computer Systems Summer 2016

# Homework 4

1. When the Domain Name System resolves a machine name, it returns a set of one or more IP addresses. Explain why.

2. Can you configure your browser to open multiple simultaneous connections to a Web site? What are the advantages and disadvantages of having a large number of simultaneous TCP connections?

3. Suppose $N$ people want to communicate with each of $N - 1$ other people using symmetric key encryption. All communication between any two people, $i$ and $j$, is visible to all other people in this group of $N$, and no other person in this group should be able to decode their communication. How many keys are required in the system as a whole? Now suppose that public key encryption is used. how many keys are required in this case?

4. In class we discussed the Diffie-Hellman key exchange algorithm and also an algorithm to establish secure socket-layer connections (SSL). How do the two algorithms differ? How does the SSL establishment algorithm avoid Man-In-the-Middle attacks?

5. Using the RSA public key encryption algorithm discussed in class, choose $p = 5$ and $q = 11$ to encrypt the word “hello”. (Represent the plaintext as a sequence of ASCII codes of the characters in the string.) Apply the decryption algorithm to recover the original plaintext message.