pCPSC 313 Introduction to Computer Systems, Summer 2016
Carsten Hood, UIN: 922009787
Due August 10, 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.
The DNS server provides a set of IP addresses to the user's machine so that it can connect and communicate with the machine indicated by the domain name. Multiple IP addresses are returned when the given domain name is associated with multiple IP addresses; this allows for back-up attempts to connect with the desired target should connection attempts with the first IP address(es) fail.

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?
Yes; a browser can establish multiple TCP connections with a given server. Advantages include more efficient pipelining, faster subsequent requests (since the already-established first TCP connection can be used), and better congestion control. Disadvantages include poor performance when multiple connections are inactive and disproportionate utilization of server and network resources by multi-connection users at the expense of others.

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?
(A) symmetric key encryption: **N*(N-1)/2**
(B) public key encryption: **2*N**

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?
(A) SSL involves trusted third party "certificate authorities" in order to assure authenticity. Diffie-Hellman lacks such an authentication mechanism and is more vulnerable to man-in-the-middle attacks.
(B) SSL avoids man-in-the-middle attacks by using trusted third party entities to certify the authenticity of key pairs, i.e., a "public-key infrastructure".

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.
p = 5, q = 11
raw "hello" => 68 65 6C 6C 6F (hex) => **104 101 108 108 111** (decimal) **=> 39 36 43 43 46** (decimal adjusted –=65)
N = p*q = 5*11 = **55**
(p-1)*(q-1) = (5-1)*(11-1) = 4*10 = **40**
k_e = **3** // relatively prime to 40
k_d = **27** // from solving (k_e*k_d)%40 = 1
public key = (k_e, N) = **(3, 55)**
private key = (k_d, N) = **(27, 55)**
encrypting: (unencrypted^3)%55 **=> 29 16 32 32 41** (decimal pre-adjustment)
decrypting: (encrypted^27)%55 => **39 36 43 43 46** (not adjusted) => **104 101 108 108 111** (readjusted +=65) => **h e l l o**