CIS6395: Homework 1 (networking and encryption)

University of Central Florida
Cliff C. Zou
Assigned: Aug. 31st, 2016;   Due: midnight Sept. 9th, 2016

1. **Knowledge-based Questions (24 points)**:

   a). What is the size of a typical TCP header? What is the size of a typical UDP header? What is the size of a typical IP header?

   b). How many layers does the Internet have according to the "top-down approach" textbook by J. Kurose and K. Ross? What are their names?

   c). Provide one example protocol or application for each layer of the Internet.

   d). Does an Internet router has IP addresses? If so, how many?

   e). A TCP connection is uniquely identified by what parameters?

   f). What are the two classes of cryptography used in our current Internet?

2. **IP subnet (22 points)**:

   A /20 block of addresses is granted to an organization. We know that one of the addresses is 129.118.78.11. How many IP addresses are contained in this subnet? What is its x.y.z.t/n representation? What is the last IP address in this subnet?

3. **Public Key Utilization (24 points):**

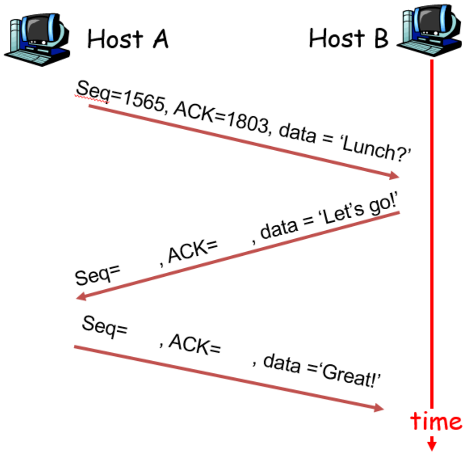
   Suppose a host A communicates with another host B. Host A has its public/private key pair (K_A^+, K_A^-); B has its own public/private key pair (K_B^+, K_B^-). A certificate authority (CA) has its public/private key pair (K_{ca}^+, K_{ca}^-). A message digest hash function is denoted as $H(.)$, message for transmission is denoted as m.

   a). If host A sends the message m to host B and wants to ensure authentication of the message, what is the notation to represent the message's "Digital Signature"? What key must host B have in order to verify the digital signature?

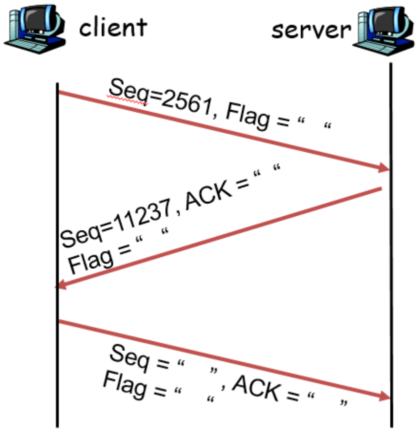
   b). What is the notation to represent the "Digital Certificate" for host A, certified by the certificate authority CA? In order for host B to verify this digital certificate, what key must host B have in order to do the verification?

4. TCP protocol (30 points):

Suppose the TCP packet transmission between host A and host B (or a client and a server) follow the following scenarios, fill in the missing sequence number and ack number (for the TCP connection setup scenario, fill in the TCP packet flag, which are the values used in TCP packet header flag field).


Host A
Host B
Seq=1565, ACK=1803, data = 'Lunch?'
Seq= , ACK= , data = 'Let's go!'
Seq= , ACK= , data ='Great!'
time

TCP seq/ack number



TCP connection setup