Incident Response Technology
Homework 1 (networking and encryption)
Cliff C. Zou

1. **Knowledge-based Questions**:

   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?

   g). What is/are the public IP subnet(s) allocated to UCF network? How many IP addresses are contained in the allocated IP subnet(s)?

   e). What is the IP subnet allocated to IBM?

2. **IP subnet**:

   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?
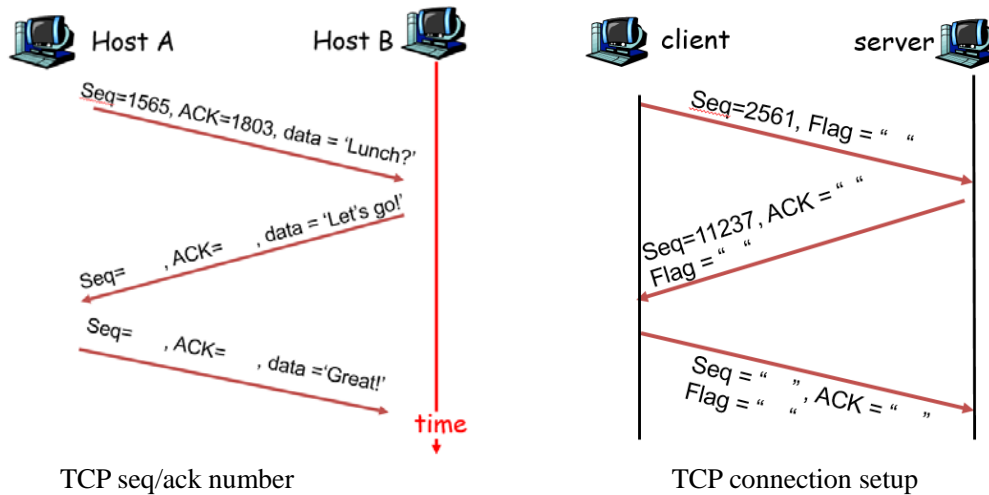
3. **Public Key Utilization:**

   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:

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   client   server

Seq=1565, ACK=1803, data = 'Lunch?'

, ACK=   , data = 'Let's go!'
Seq=

Seq=
, ACK=   , data ='Great!'

time

Seq=2561, Flag = " "

Seq=11237, ACK = " "
Flag = " "

Seq = " ", ACK = " "
Flag = " "

TCP seq/ack number   TCP connection setup

5. Virtual Machine Setup and Networking between VMs:

Please install VirtualBox on your own machine, then import the following two VM images in your VirtualBox: Kali Linux VM, and Windows 7 VM (with any version of IE you want).

1). Set up these two VMs in "Nat Network" mode and put them in one LAN so that they can reach each other. What are these two VMs IP addresses? Please use screenshot images to show how you know each VM's IP address.

2). Use screenshot images to show that you can Ping from Win7 VM to your Kali Linux VM successfully, and you can also Ping from Kali Linux VM to your Win7 VM successfully (hint: if the ping to Win7 VM fails but the other direction succeeds, then you need to configure Win7 firewall to allow Ping to go through as I explained in class).