**CIS6395: Homework 1 (networking and encryption basics)**

**University of Central Florida**

**Cliff C. Zou**

**Assigned: Sept. 7, 2022; Due: midnight Sept. 18, 2022**

**U**

1. **Knowledge-based Questions (32 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?

The typical size of a…

TCP header is 20 bytes.

UDP header is 8 bytes

ip header is between 20 and 24 bytes

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?

Five. Application, transport, network, data link, and physical layer

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

Application: SMTP

transport: TCP

network: IP

link: Ethernet

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

Yes. One for each network interface

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

source IP address

source port number

dest IP address

dest port number

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

Symmetric (private) and asymmetric (public) keys

g). What is the private network subnet used by UCF internal network? How many IP addresses are contained in this private IP subnet?

10.0.0.0/8 which contains space for 224 ip spaces

h). What is the /8 subnet IP space allocated to Apple Computer Inc. (note that IPv4 has overall 256 /8 subnet)?

According to Wikipedia, it is 17.0.0.0/8

Source: https://en.wikipedia.org/wiki/List\_of\_assigned\_/8\_IPv4\_address\_blocks

i). Why DNS usually uses UDP instead of TCP for its communication?

Because with UDP a DNS repsonse makes one round-trip time, which is better than the response time of TCP

1. **IP subnet (18 points)**:

A /19 block of addresses is granted to an organization. We know that one of the addresses is 129.117.74.11. How many IP addresses are contained in this subnet? What is its a.b.c.d/n representation? What is the last IP address in this subnet?

There are 232-19 = 213 ip addresses

129.117.74.11 in binary format:

10000001 1110101 1001010 00001011

then set 32 – 19 = 13 rightmost bits to 0

10000001 1110101 1000000 00000000

or

129.117.64.0/19

The last ip address would just be flipping all the 13 rightmost bits from 0 to 1.

1. **Public Key Utilization (20 points):**

Suppose a host A communicates with another host B. Host A has its public/private key pair (; B has its own public/private key pair (. A certificate authority (CA) has its public/private key pair (. 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?

Digital signature: KA-KA-(m)

key needed by host B: KA+

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?

Notation for host A: KCA- (KA+)

key needed by host B: KCA-

1. **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). You can either fill on the graph, or use words to explain the values you fill in for each required field.

Diagram

Description automatically generated

TCP seq/ack number TCP connection setup

For host A and B:

row 2:

ACK = 52 + len(data) = 52 + 5 = 57

Seq = 115

row 3:

ACK = 115 + len(data) = 115 + 5 = 120

Seq = 57

For client and server:

row 1:

flag always starts off as SYN

client\_seq = 236

row 2:

ACK = client\_seq + 1 = 236 + 1 = 237

Flag = SYN/ACK

Server\_seq = 11245

Row 3:

ACK = server\_seq + 1 = 11245 + 1 = 11246

Flag = ACK

Seq = client\_seq + 1 = 236 + 1 = 237