Massachusetts Institute of Technology
Sloan School of Management

15.564 **Information Technology I** **Spring 2003**

Problem Set 4

Computer Networks / Public Key Cryptography

Due: Tuesday, April 29, 2003

IMPORTANT: Problem 5 requires some advance preparation. Please read it carefully at least one week before the due date!!!!

PROBLEM 1: ETHERNET VERSUS TOKEN RING (10%)

Ethernet is sometimes said to be inappropriate for real-time computing because the worst case retransmission interval is not bounded.

Task 1: Briefly describe a scenario in which a machine connected on an Ethernet (a local network using CSMA/CD for conflict recovery) ends up waiting a very long amount of time before it is allowed to send its next packet.

Suppose your machine is connected to a token ring network. There are n machines connected to the ring network. The circulating token takes time t to circulate between one node and the next one in the ring. Whenever a node receives the token, if it has nothing to send at that time, it passes the token on immediately to the next node in the ring. If, on the other hand, the receiving node has a packet to send, then it sends that packet instead of the token. The packet sent circulates around the ring taking time p. In the meantime, the node to which the packet is addressed has the opportunity to read it. When the packet returns to the original sender, the sender removes the packet from the ring and reinserts the token. The token will then flow to the next node in the ring and the above algorithm will be repeated.

Task 2: Describe the worst case scenario in the case of the above token ring. What is the maximum time that a node will have to wait before it is allowed to send its next packet? Why is the worst case behavior of a token ring considered to be superior to that of an Ethernet network?

PROBLEM 2: OSI PROTOCOLS (15%)

As discussed in class and in the notes, a protocol data unit (PDU) is a combination of control information for a certain protocol layer and data from the next higher layer. Peer layers communicate by exchanging PDUs. For example, the network layers in two nodes will communicate by exchanging network-layer PDUs, each of which will contain control information used by the network layers plus information coming from the source transport layer and going to the destination transport layer. The attached diagrams in the Appendix illustrate the operation of the OSI architecture, and how the different layers exchange data and construct and take apart PDUs. Study the diagram, and answer the following question:

A session layer protocol data unit (PDU) consisting of 1500 bits of data and 160 bits of header is sent to a transport layer, which appends another 160 bits of header. Then it is transmitted through the network layer, which uses a 24-bit packet header, and a maximum packet size of 800 bits. Finally, the data link layer wraps each packet into a frame, adding a 3-byte header before each packet and a 2-byte checksum after it.

Task 1: How many bits, including headers, are delivered to the network layer protocol at the destination? Explain your calculations so that we can give you partial credit if you miss something!

Task 2: What fraction of the physical network's bandwidth is filled with overhead (header and checksum) data in the above example? In your answer you can assume that the layers above the session layer (i.e. the application and presentation layers) do not introduce any more overhead. What would be the effective data rate of a 10-Mbps Ethernet network using the above protocols? How much time would it take to transmit a 4MB file through that network (assuming there were no collisions or other delays)?

PROBLEM 3: TCP/IP PROTOCOL (10%)

One way to define what it means to "be on the Internet" is the following:

> A machine is on the Internet if it runs the TCP/IP protocol stack, has an IP address, and has the ability to send IP packets to all other machines on the Internet.

In this assignment, you will familiarize yourselves with the various parameters of the TCP/IP protocol. Under Windows you can normally examine the TCP/IP parameters of your machine by going to the DOS prompt and typing:

ipconfig /all

Task 1: What is the IP address of your machine? How does a machine get assigned an IP address? Can you take the PC you are using for this assignment to another location at MIT (say, your dorm room) and keep the same IP address?

Task 2: What is the IP address of your gateway? What is the role of the gateway in the case of the PC that you are using to do this assignment?

Task 3: What is the IP address of your Domain Name Server? Why does your PC need to know the address of a Domain Server?

PROBLEM 4: EXPLORING THE INTERNET (15%)

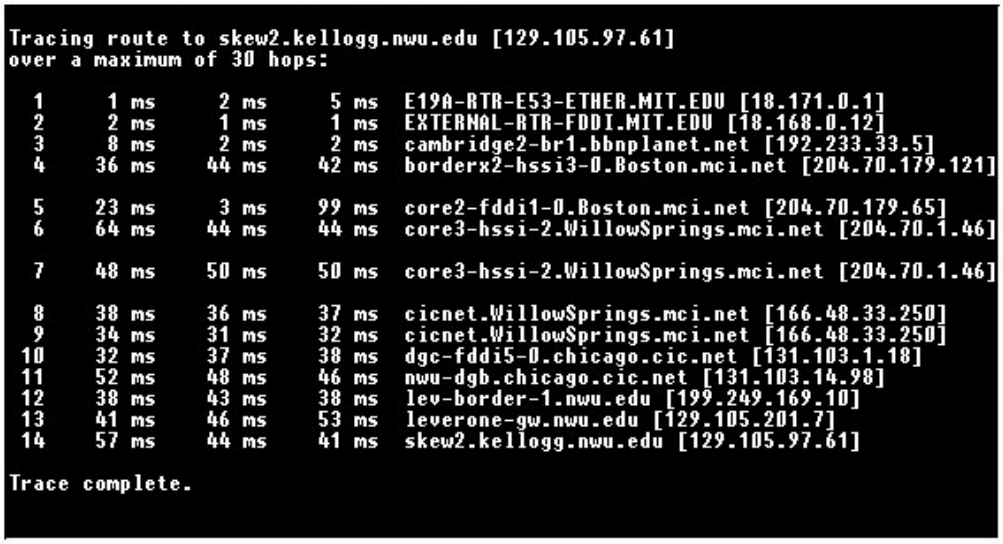
Windows provides a utility program that helps trace the route that connects your computer to any other computer on the Internet. The program is called **`tracert`** (stands for "trace route") and must be called from inside a DOS window. The syntax for using tracert is:

```
tracert <destination-host-name>
```

The results of executing tracert is a list of all the Internet nodes (i.e. computers visited) in the Internet path that connects our computer to the destination computer. For example, the result of executing:

`tracert skew.kellogg.nwu.edu` (a computer at the Kellogg Business School)

from a computer in building E53 is the following list of nodes:



```
Tracing route to skew2.kellogg.nwu.edu [129.105.97.61]
over a maximum of 30 hops:

  1     1 ms     2 ms     5 ms  E19A-RTR-E53-ETHER.MIT.EDU [18.171.0.1]
  2     2 ms     1 ms     1 ms  EXTERNAL-RTR-FDDI.MIT.EDU [18.168.0.12]
  3     8 ms     2 ms     2 ms  cambridge2-br1.bbnplanet.net [192.233.33.5]
  4    36 ms    44 ms    42 ms  borderx2-hssi3-0.Boston.mci.net [204.70.179.121]

  5    23 ms     3 ms    99 ms  core2-fddi1-0.Boston.mci.net [204.70.179.65]
  6    64 ms    44 ms    44 ms  core3-hssi-2.WillowSprings.mci.net [204.70.1.46]

  7    48 ms    50 ms    50 ms  core3-hssi-2.WillowSprings.mci.net [204.70.1.46]

  8    38 ms    36 ms    37 ms  cicnet.WillowSprings.mci.net [166.48.33.250]
  9    34 ms    31 ms    32 ms  cicnet.WillowSprings.mci.net [166.48.33.250]
 10    32 ms    37 ms    38 ms  dgc-fddi5-0.chicago.cic.net [131.103.1.18]
 11    52 ms    48 ms    46 ms  nwu-dgb.chicago.cic.net [131.103.14.98]
 12    38 ms    43 ms    38 ms  lev-border-1.nwu.edu [199.249.169.10]
 13    41 ms    46 ms    53 ms  leverone-gw.nwu.edu [129.105.201.7]
 14    57 ms    44 ms    41 ms  skew2.kellogg.nwu.edu [129.105.97.61]

Trace complete.
```

By studying the list above, you can find useful information such as

- what is the gateway of MIT to the external world
- who is operating the backbone that connects Boston to Chicago
- is there a direct connection between Boston and Chicago? If not, what are the intermediate hops?

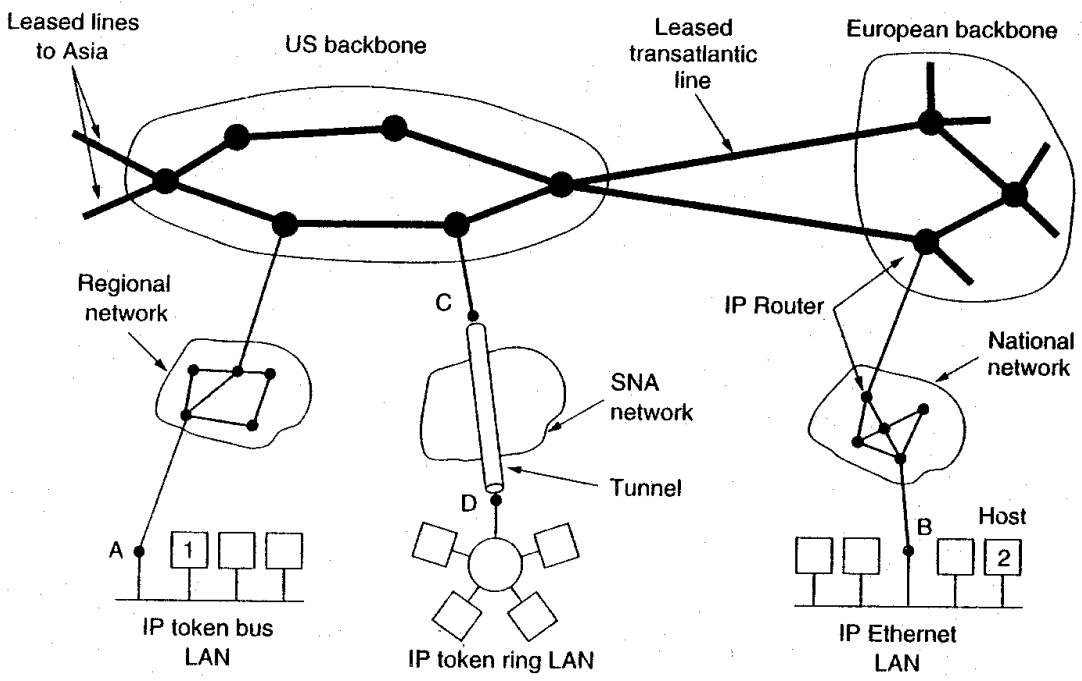


Figure 1: High-level structure of the Internet, showing LANs, gateways, regional networks and backbones.

The purpose of this problem is to give you the opportunity to use **`tracert`** to explore small parts of the structure of the Internet. The experience will help you get a better sense of how the various elements of the Internet connect together (see Figure 1).

Task: Use ***`tracert`*** *to carefully selected destinations in order to answer the following questions:*

1. What is the name and IP address of the gateway of MIT to the external world?
2. Who provides the regional network that connects MIT to the rest of the Internet?
3. Where is the company site of ebay (www.ebay.com) physically located? Who provides the backbone that connects together MIT and the location of www.ebay.com? What U.S. cities are visited by packets on route from MIT to www.ebay.com?
4. Which cities/countries are visited by packets on the Internet route from MIT to http://www.mptc.gov.kh/ , the Ministry of Posts and Telecommunications of the Kingdom of Cambodia? Who provides the backbone in each different country that is part of the route?
5. A friend's web site has an IP address of 209.132.75.133. Can you tell where that web site is physically located?

HINT: A very attractive graphical variant of tracert, called VisualRoute, can be downloaded (for a free trial) from **http://www.visualware.com/visualroute/index.html** Feel free to do this exercise using VisualRoute, if you want.

PROBLEM 5: PRETTY GOOD PRIVACY (PGP) (50%)

The purpose of this problem is to acquaint you with PGP, one of the most widely used programs for encrypting files using public key cryptography.

Retrieve PGP software from the MIT PGP distribution site. Since there are many versions around, we recommend using the MIT version (PGP 6.5.8) because it is the one your TAs have.

Install PGP on a computer (either on the PC lab or at your home). Versions of PGP exist for PCs, Macs, and Athena workstations. You can do this assignment on any type of computer. Instructions for installing the program are included in the software you will download. Learn how to use PGP. Use the documentation included in the PGP Freeware distribution. It is probably best to read the Introduction to Cryptography first and, if you still have questions, then consult the user guide.

*Task: Send a message **to the entire class** (**via the course server**) that satisfies the following constraints:*

a) The message title is "PGP Assignment"
b) No one but your TA can decrypt the message.
c) Your TA can be sure that the message came from you, and not from someone else in the class. You will need to use key certification and the Web of Trust, because someone else could send your TA a public key, claiming it was yours.
d) The text of the message explains how conditions b) and c) are met.

ATTENTION: Your message must be sent to the entire class not to the TAs. We ask you to do this deliberately to give the opportunity to students to try decrypting other people's messages. In fact, as we explain below, we are offering extra credit to anyone who successfully manages to do so!!!

Logistical Details: To do this assignment, you will have to create your own pair of public/private keys and email your public key to your TA. He needs to have received your email by **noon on Thursday, April 24, 2003**, if you plan to have him certify your key (see the class notes or the PGP documentation to learn about what "key certification" means).

Your TA will certify keys in person during his TA hours that week (he will send email with the exact hours and location). When you come to see your TA, please bring a

printout of the "fingerprint" of your key with you. He needs the "fingerprint" to certify your key (again, please refer to the PGP documentation to find out what "key fingerprints" are, and how to generate them).

If you don't certify your keys during these times, you'll have to find a student in the class whose key has been certified to certify your key. Then you need to email your certified public key to the TA. **If you don't certify your key, you can still do this assignment**. However, some other student might then be able to impersonate you and send the TA a public key, claiming it is yours. **In any event, you will have to email your TA your public key before you submit the requested message to the class list. Both are due by the midnight of Tuesday, April 29, 2003.**

In Summary: learn PGP, generate a set of public and private keys, e-mail your public key to *your TA* by noon on April 24, have him certify your key during his office hours (or have a fellow student certify your key, or risk impersonation), and send your encrypted message to the *entire class* by midnight on April 29, 2003.

We suggest that you experiment with using PGP among yourselves before you send your email messages to the TA. For example, form pairs and try exchanging your public keys and then sending encrypted and signed messages to each other.

You will receive 50% extra credit if you can decrypt someone else's message (send a copy of it in plain text to **the TA**) or if you successfully impersonate someone else (i.e., convince the TA that your message really came from someone else.)

You will be penalized by 50% if someone else impersonates you or if someone decrypts your message, **and by 70% if you certify a key that turns out to be a fake**. The penalty for certifying a fake key will be higher than the extra credit for impersonating someone else! **Good luck!**