Final Exam: 24.370

Name: ________________________________

Student Number:___________________________

Instructions: 3 Hours, Closed Book, No Cheating, programmable calculators allowed, neatness counts (if I Can't read it, I can't mark it). Answer in the space provided. State any necessary assumptions made.
You may tear off the last page (p.10) to use it. Good Luck.

Given:

$c = 3 \text{ X } 10^8$ m/s (signals travel 2/3 c)
$\tau = 51.2$ usec (maximum round trip delay in ethernet)

1) Short Answers (be brief)

a) Briefly explain and give an example of an implementation for each type of switching;

i) Circuit switching:

ii) Message switching:

iii) Packet switching:

b) List three advantages of TDM over FDM as used in telephone switching.

c) Explain how TDM can be used for both circuit and packet switching networks.

d) ATM is a form of TDM switching. Briefly explain how ATM differs from traditional TDM, and specifically describe how ATM can be used to increase throughput.

e) An alternative available in wireless communication is CDMA. Briefly explain CDMA, focus on how it differs from alternative forms of multiple access

f) List three advantages that CDMA offers to cellular communication.

g) What four values uniquely identify an internet connection ?

h) Which provides a higher bandwidth - throwing a CDROM (~650 Mbytes) across a room (<30 m) or using a 10Mbps ethernet ? How about 100 Mbps ? Explain.

i) Is Federal Expressing (overnight delivery) of a 5 Gigabyte hard disk faster than a T1 connection (1.544 Mbps) ? Explain.

j) MTS is offering ADSL and Videon and Shaw are offering cable modems, to increase the speed of connections for home users to ~1.5 Mbps. Is this guaranteed to decrease the time for downloading web pages ? Explain.

k) Why would we want to make a web server multithreaded ?

l) How does RSA performance scale with key size ?

m) What is an advantage of RMI/CORBA over client/server programming with sockets?

2) IP Networks:

Given the network illustrated on the back page (you may remove this illustration from the exam, it will be used again for question 3), and assuming all ARP tables are initially empty and the routing tables are already stable, and the DNS server can resolve any request:

Show the sequence of packets that will occur when the following command is entered on **A**:

ping f.deptz.company.com

Before starting you will need to make an assumption. State the assumption first, and explain why you made the decision that you did.

Assumption:

Sequence of packets:

3) Transport Protocols (TCP/UDP):

Using the network illustrated on the back page, and assuming that each router has a minimum delay of 100 usec and all of the computers have buffer sizes of 6,000 bytes, and there is no other traffic on the networks, with maximum packet size of 1,500 bytes.

a) What would be the maximum data rate of TCP traffic from:

i) **A** to **B** ?

ii) **A** to **C** ?

iii) **A** to **F** ?

b) What is the Maximum UDP data rate between:

i) **A** and **B** ?

ii) **A** and **F** ?

c) To increase throughput between hosts, is it better to increase the bandwidth of the network connection(s), or to increase the host buffer memory, for:

i) **A** and **B**? Explain.

ii) **A** and **C**? Explain.

iii) **A** and **F**? Explain.

d) Assume that a corporate application encrypts all traffic using RSA. If the application can encrypt data at a rate of 100 Kbytes/sec, how will this affect the throughput of the data across the network (between **A** and **F**) ?

4) Security (Short Answers):

Alice and Bob want to exchange sensitive information using RSA. Alice generates a public and private key (100 digits long). Alice encoded her messages with her private key, Bob encodes his messages with Alice's public key.

a) Can an eavesdropper decode Alice's messages to Bob? Explain.

b) Can an eavesdropper decode Bob's messages to Alice? Explain.

c) How can Bob verify he is talking to Alice (assuming he obtained Alice's public key from a trusted authority) ?

d) Why can't Alice verify she is talking to Bob? How can this be modified so she can?

e) Can Mallot (man in the middle) forge messages to Alice? Explain.

f) Can Mallot forge messages to Bob? Explain.

g) Can Mallot replay messages from Bob to Alice? Explain.

h) Can Mallot replay messages from Alice to Bob? Explain.

i) How could these transactions be made more secure?

5) Security

A bank decides to implement a more secure Automated Teller Machine (ATM) system than the current ATM card system. This new system will utilize smart cards in place of the simple magnetic strip cards currently used. A smart card is a credit card with an embedded processor and memory in a tamper proof case. The card is designed so that the information stored on the card can not be directly read or written to by users/criminals, and all interactions are done through commands to the processor. The biggest advantage of this card is that it is not possible for a criminal to copy the card (since the internal state may not be read). The card also has an associated Personal Identification Number (PIN) which must be entered at the start of a transaction. Each PIN is at least 4 digits long, and maximum 6 digits longs

Each card uses RSA security (each card has a public and private key, as would each ATM and each Bank), and also contains a digital certificate identifying the card (signed by the bank), as well as any additional information that would normally be stored on a magnetic strip card.

a) Would it be secure to store the user's PIN on the smart card? Explain.

b) Show the sequence of transactions required to exchange keys between smart card and ATM machine.

c) What information should be contained on the digital certificate (including who would sign any signed data) to actually perform authentication? Describe how this authentication would then occur using your banks ATM.

d) Describe how the authentication mechanism would differ if you were using another banks ATM? (Hint: What infrastructure would be required?)

6) Encryption (RSA)

Alice is running a business on the Internet, and wants people to send her credit card numbers encrypted with RSA.

She selects **p** = 11, **q** = 17 as her two large prime numbers.

a) Which of the following values would be a suitable value for the public encryption key **e**? State the reasons for your selection. (Hint: Only one value is suitable).

5 7 10 15 24 32

b) Which of the following values would be a suitable value for the secret decryption key **d**? State the reasons for your selection. (Hint: Only one value is suitable).

0 1 9 11 15 23 24

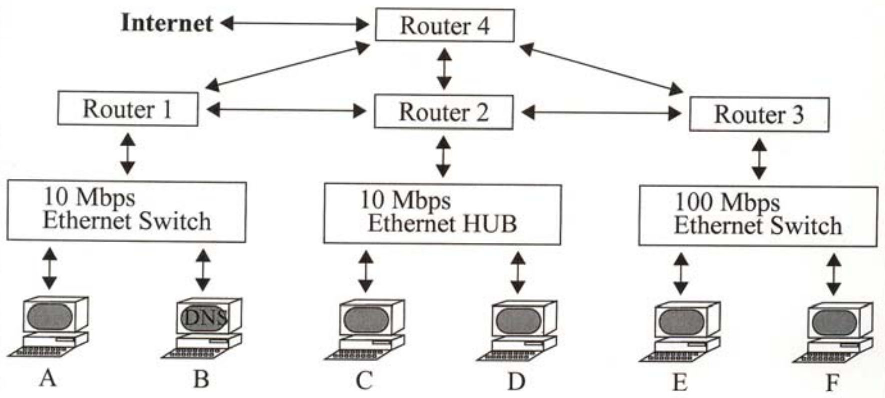
c) Bob wants to encrypt the number 9. What is the encrypted value of 9?

d) Alice receives the encrypted message: **0,1,70,0,1,70,0,1,70,0** which represents Bob's credit card number (each digit encrypted separately), What is Bob's credit card number?

e) Could characters (1 byte / character) be encrypted/decrypted one character at a time with these keys? Explain.

Have a good Summer ....Good luck in your future careers.......

This network is to be used with questions 2 and 3 in the exam.You may remove this illustration from the exam booklet (it does not need to be turned in).



A	(a.deptx.company.com)	129.1.10.1	(MAC: 00:11:22:33:44:01)
B	(b.deptx.company.com)	129.1.10.2	(MAC:00:11:22:33:44:02)
	- DNS server for *.company.com)		
C	(c.depty.company.com)	129.1.20.1	(MAC: 00:11:22:33:44:08)
D	(d.depty.company.com)	129.1.20.2	(MAC: 00:11:22:33:44:09)
E	(e.deptz.company.com)	129.1.30.1	(MAC: 00:11:22:33:44:0A)
F	(f.deptz.company.com)	129.1.30.2	(MAC: 00:11:22:33:44:0B)
R1 (router 1)			
	r1.deptx.compnay.com :	129.1.10.3	(MAC: 00:11:22:33:44:03)
	r1.net1-2.company.com :	129.1.40.3	
	r1.net1-4.company.com :	129.1.50.3	
R2 (router 2)			
	r2.depty.compnay.com :	129.1.20.4	(MAC: 00:11:22:33:44:06)
	r2.net1-2.company.com :	129.1.40.4	
	r2.net2-4.company.com :	129.1.60.4	
	r2.net2-3.company.com :	129.1.70.4	
R3 (router 3)			
	r3.deptz.compnay.com :	129.1.30.5	(MAC: 00:11:22:33:44:07)
	r3.net3-4.company.com :	129.1.80.5	
	r3.net2-3.company.com :	129.1.70.5	
R4 (router 4)			
	r4.net1-4.company.com :	129.1.50.6	
	r4.net3-4.company.com :	129.1.60.6	
	r4.net2-4.company.com :	129.1.80.6	
	r4.net-ext.company.com :	129.1.90.0	

Routers 1 and 4 are located in Winnipeg (< 1 km), Router 2 is located in Sydney Australia (20,000 km from Wpg), and Router 3 is in Brandon (200 km from Wpg). All routers are interconnected with T1 lines (1.544 Mbps), and they are connected to the LANs with the bandwidth of the individual LAN.