MS&E 130/231: Information Systems, Autumn 2005-06
Instructor: Ashish Goel
Handout 4: Practice problems for the midterm

Problems 1-4 are from last year's midterm. Another problem from last year's midterm concerned material we did not cover last year. We will post solutions on Saturday evening.

You may bring a calculator to the exam if you wish.

1. Are there any conditions under which an application designer would choose to use UDP rather than TCP? Describe those conditions, or explain why not.

2. Suppose TCP is being used to send a very large file cross-country. Assume that the RTT is 100ms, the packet sizes are 1KB, and the link capacity is 1Gbit/s. If the window size is restricted to 64KB (i.e. 64 packets in this case), what is the maximum data rate that can be achieved? What would the maximum window size have to be to completely utilize the entire link capacity? Please remember that 1 Byte = 8 bits.

3. Ms. Granger wants to submit her homework assignment over the Internet. Knowing that the Internet is not safe, she encrypts her assignment using her private key before she emails it, so that the Professor knows the assignment came from her. What kind of an attack is Ms. Granger vulnerable to, and what should she do to avoid this attack?

4. What is the IP invariant? Explain how the success of IP routing depends, to a large part, on the fashion in which ICANN assigns IP addresses.

5. Consider p = 13 and q=5. You are also told that e = 29. Follow steps 4 and 5 of the RSA algorithm described in class to obtain d. What are the public and private keys? Encode the message m=20 using the public key, and then encrypt the result using the private key. You may use a calculator. *This problem is hard, and you might be tempted to skip it. But RSA is important and beautiful, and I would like you to understand it well. So here is a small incentive: There will be a version (with slightly smaller numbers) of this problem in the midterm. So if you solve this practice problem and understand it well, you will be guaranteed to ace one problem on the midterm.*

6. Why doesn't IP maintain a checksum for the entire packet in its header?

7. Why is DNS an application layer protocol as opposed to a being a part of the core Internet functionality?

8. Suppose n = pq, where p and q are prime. Prove that if you are given n and $\phi(n)$, you can factorize n efficiently.

9. In shared key (or symmetric key, or private key) cryptography, there is a shared key that is known to Alice and Bob, but not to anyone else. This shared key is then used to encrypt/decrypt any communication between the two. Assume that Alice generates the shared key, and that there is some secure method (which we are not concerned with in this problem) of sending this shared key to Bob.
    1. First, prove that public key cryptography is at least as powerful as shared key cryptography. Hint: Show how you can simulate a shared key cryptosystem using a public key cryptosystem.
    2. Which is likely to be harder – public key cryptography, or shared key cryptography?
    3. Which of the following can be achieved given a shared key – authentication, encryption, and non-repudiation? How or why not?

10. Explain how Moore's law favors cryptography, assuming that factoring k bit integers takes time which is exponential in k but encrypting and decrypting a message using RSA with k-bit keys takes time proportional to k^2.

11. What can go wrong with the following communication protocol? How would you fix it?

Alice:	Hello, I am Alice.
Bob:	Prove it. Here is a nonce, R.
Alice:	Here is $K_A^-(R)$.
Bob:	Let me apply K_A^+ to this value. The answer is R. No one else could have generated $K_A^-(R)$. You must be Alice!
Alice:	Ok, here is an important secret: K_B^+("Gossip, gossip,…").
Bob:	Oh, thanks!