Name: _____ **USC ID:** _____

CSci 530 Midterm Exam

Fall 2007

Instructions:

Show all work. No electronic devices are allowed. This exam is open book, open notes. You have **100 minutes** to complete the exam.

Please prepare your answers on separate sheets of paper. You may write your answers on the sheet of paper with the question (front and back). If you need more space, please attach a separate sheet of paper to the page with the particular question. **Do NOT extend your answer on the back of the sheet for a different question, and do NOT use the same extra sheet of paper to answer more than one question**.

In particular, **each numbered questions must appear on separate pieces of paper so that the exam can be split for grading**.

Be sure to include your **name** and **USC ID** number **on each page**.

There are **100 points** in all and **4 questions.**

	Q1	Q2	Q3	Q4	Total Score
Score					

Name: _____ **USC ID:** _____

1. (20 points) Cryptography

a. Explain why we use the chaining modes of operation to convert block ciphers to stream ciphers? Specifically, what benefit is obtained by using a stream cipher and why is it important? Give an example of a form of analysis that is possible using a block cipher that is prevented when we use cipher-block-chaining. (8 points)

b. For the following modes of operation, indicate (yes or no) whether during encryption, the value of a ciphertext block is dependent on the position of corresponding plaintext block in the stream (position), the plaintext of all preceding plaintext (preceding) blocks in the stream, and whether the modification of a bit in a block in the ciphertext of the stream will result in a predictable change in the corresponding decrypted plaintext block (predictable). Be careful in considering this last case – note that I emphasized "corresponding" block. I am not asking about the next block or the preceding block. (12 points).

	ECB	CBC	CFB	OFB
Position				
Preceding				
Predictable				

Name: _____ **USC ID:** _____

2. (20 points) Key Management for Public Keys

Discuss the approaches used to determine or validate the binding of public keys to principals for authentication of end users in PGP and SSH, and of servers (i.e. no user cert) using SSL (or TLS), and for the exchange of keys in Diffie-Helman Key Exchange. Who is responsible for establishing (or certifying) the binding in each case, and once authentication (or an encrypted channel) is established, what is the information known by each party about the other.

Name: _____ **USC ID:** _____

3. (30 points) Mandatory Access Controls

Discuss the relative ease with which a virus can spread through a system that implements mandatory access controls. Consider both the Bell-Lapadula model and the Biba model. Which model will have the greatest impact on the spread of a virus. How is the spread of a virus or worm on more common systems affected by the privileges with which the users run? What about the privileges with which servers run?

Name: _____ **USC ID:** _____

4. (30 points) Design problem

You have been hired by a consortium of banks to design the next generation of phish-free authentication tokens for distribution to customers. The banks plan to distribute USB devices to customers for use in authentication. The banks want to be sure that customers have the USB device in their possession for certain sensitive operations like adding payees for home banking. The approach to be employed by the bank is supposed to provide protection from as many forms of malicious code as possible, not just phishing attacks.

a. What should be stored on the USB device? Describe the interface that should be available for an application to use the device.

b. Suggest an approach to make this “two factor” authentication – i.e. not just that the user has the USB device, but also another factor to prevent a lost device from being used by anyone that finds it. Consider alternative approaches and explain why yours is better than the others.

c. Consider several forms of malicious software that might be circulating on the network. Discuss how such software might still be able to breach the security of your proposed system. Is the new attack more difficult than the attacks that were effective before deploying the USB device? How have you managed to make it harder for an attack to be successful?