Name: _____ **USC ID:** _____

CSci 530 Midterm Exam

Fall 2008

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 **3 questions.**

	Q1	Q2	Q3		Total Score
Score					

Name: _____ **USC ID:** _____

1. (35 points) Cryptography

   a. Explain why the cipher feedback and the output feedback modes of operation for stream ciphers would be incompatible with the use of an underlying public key cryptosystem?
   (10 points)

   b. When PGP or S/MIME is used to send an encrypted and signed message to multiple recipients, describe in general terms the structure of the key and signature management fields in the message, i.e. (that means) what keys and hashes are generated for the purpose of sending the message, and what encryption keys are pre-existing and how are these keys used on both the sender side and the recipient side, and what fields of the message are they used to encrypt or decrypt. (20 points)

   c. For the hashes generated and messages or fields encrypted in part b, give an example of a suitable cryptosystem or has function that may be used. (5 points)

Name: _____ **USC ID:** _____

2. (25 points) Authentication

In the following systems or methods, list the primary disadvantage or weaknesses of the authentication that results when connections are established. What is known both parties once the connection has been established. (5 points each)

a. SSL or TLS authentication of web sites (both with and without client side certificate)

b. Diffie-Hellman Key exchange.

c. Public key based authentication in SSH.

d. Authentication of users with Kerberos.

e. Biometric authentication (e.g. fingerprint) from a remote workstation.

Name: _____ **USC ID:** _____

3. (40 points) Design problem

You have been hired by the department of the treasury to consult on the design of the security system that will be implemented for online access to the auction system used as part of the economic stabilization package. This will be an auction where those having securities they wish to sell will enter information about the securities and for similar securities, the treasury will purchase from the lowest bidder.

a. It is critically important that the treasury be able to hold the participants accountable for the descriptions provided during the auction when settling accounts after a successful transaction. Explain in detail how you will advise that the system be designed so that the treasury will be able to clearly demonstrate what the description of the securities entered by the participants were, without the ability of the participant to claim that the description was later modified in the system (either by the treasury itself, or by anyone else). (15 points)

b. Discuss the limitation of your approach, i.e. tell me what kinds of attack on the system you described in part a might still allow the descriptions to be modified, and thus allow a participant to attempt to get out of a transaction by claiming the documentation is not authentic. Which of these attacks result from carelessness on the part of the participant, and which ones on poor design and or carelessness by the treasury. [note: depending on your design in A, you might have already addressed the second issue, in which case you will receive credit for that part of question B, but you would still need to answer the first part of question B] (15 points)
(answer on back of page)

c. How would you change the procedures used in “enrolling” for the auction in order to further limit the ability of the treasury to change the descriptions, and thus to prevent participants from refuting their transactions. . [note: Again, depending on your design in A, you might have already addressed this issue, in which case you will receive credit for this part based on the design presented in part A] (10 points)