Name: _____ **USC ID:** _____

CSci 530 Midterm Exam

Fall 2009

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**. The exam will be split apart for grading by different people, and if part of your answer for one question appears on a page given to a different grade because the sheet contains parts of the answer to more than one question, then you will NOT receive credit for that part of the answer not seen by the grader. 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. **(30 points) Cryptography -** For each of the following pairs of cryptosystems and modes of operation, 1) indicate which provides stronger confidentiality protection and why, and 2) which provides stronger integrity protection, and why.
    a. RSA with a 512 bit key (used as a block cipher) vs. AES in Output feedback mode. (10 points)

    b. DES in Electronic Code Book mode vs. DES in Cipher Block Chaining mode (10 points) [Your explanation will be extremely important in answering this, as I am willing to accept more than one answer if properly justified.]

    c. Triple DES with a 112 bit key vs. RSA with a 512 bit Key (both as block ciphers) (10 points).

Name: _____ **USC ID:** _____

2. (30 points) Authentication and Key Management

In each of the following authentication or key distribution methods: 1) list the pieces of secret or private information known or shared by each of the parties; 2) how one party proves knowledge of such information to the other party; and 3) what such proof allows the other party to conclude.

a. Authentication of a client to a server using Kerberos. (10 points)

b. Password based authentication to an SSL protected web server (10 points)

c. Certificate based authentication of the client to an SSL protected web server (10 points).

Name: _____ **USC ID:** _____

3. (40 points) Design problem

You have been hired by the department of health and human services to assist in the design of a patient medical record and billing system that will be used to reduce the cost of health care under whatever health care reform plan is finally adopted.

a. Discuss in general terms the confidentiality and integrity policies that should be associated with the health care records (i.e. what kinds of data exist in the system and for each class of data, who should have what kinds of access). (10 points)

b. In more specific terms, are the policies you suggest mandatory access controls, discretionary access controls, or a combination? Justify your answer. (10 points)

c. How do you suggest authenticating users in the system? Consider whether you will use different methods for different classes of users, and suggest an approach for each. On what basis will each class be authenticated? (10 points)

d. What are some of the requirements for data integrity in the system? Suggest an approach to ensure the integrity/authenticity of patient records and prescriptions in the system. Explain how your approach is related to your answer in part c. (10 points)