Name: ______________________ **USC ID:** ______________________

CSci 530 Midterm Exam

Fall 2005

Instructions:

Show all work. **If a question asks for a numerical or algebraical result, indicate your answer clearly (for example, by drawing a box around it)**. 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. Place the following cryptosystems in order according to the size of their keyspace. (10 points)

1) RSA with a 512 bit key

2) Triple DES

3) AES 192-Bit

4) DES

5) RSA with a 1024 bit key

6) ROT 13 (A Caesar cipher rotating letters in the alphabet by 13)

b. For DES (3 points), Triple DES (3 points), AES (3 points), and ROT 13 (1 point), what is the size of the keyspace (the space from which keys are drawn, I am not asking about the effective keyspace, but the actual keyspace).

Name: ______________________ **USC ID:** ______________________

2. (25 points) Digital Signatures and Hash Functions

A digital signature is usually implemented by taking a hash of a message and encrypting the hash value with the private key of the signer.

a. What could happen if a collision were found in the hash function used for the signature? (5 points)

b. What might be the possible impact of such a collision on the security of the digital signature mechanisms? (10 points)

c. What factors will affect the impact, and what things might be done to mitigate the effect of such collisions. (10 points)

Name: _______________________ USC ID: _______________________

3. (25 points) Authentication

Which parties are authenticated in each of the following protocols? Are the client, initiator, server, verifier, sender, recipient, etc. authenticated?

For each of the protocols, explain your answer and also explain what precisely is known about the other party at the conclusion of the protocol exchanges.

- Unix password authentication
- Kerberos basic and mutual authentication
- Diffie Hellman
- SSL (both cases)
- S/MIME or PGP, or other secure electronic mail system

4. (30 points) Design problem

You have been hired by FEMA (The Federal Emergency Management Agency) to develop a remote repository of records (prescriptions, driver's licenses, passports, etc) that will enable residents displaced by a disaster such as a hurricane to access images records and important documents that they have registered with the repository.

The same system will be used to allow residents who have left their homes without appropriate identification to prove their identities to emergency workers who might be distributing aid, or to allow them to access their assets on deposit with banks, without their ATM cards or other identification.

Privacy if of critical importance in such a system as citizens will be unwilling to register their documents if they know that it allows others to access the documents without authorization. The ability to access the records in a crisis is also critical, as that is the purpose of the repository.

You have taken this position knowing that there is no perfect solution to these problems, and that all you expect to do at this is highlight important considerations in a couple of areas, those which are listed below.

Be sure to consider human factors in the answers to the questions below. How hard is it to remember something you haven't used for three years, while you are under the stress of an evacuation? Think about how these kinds of limitations might be addressed.

a. Authentication (15 points)

Discuss the benefits and drawbacks for basing authentication on each of something you know, something you have, or something about you, or combinations of the above. Be sure to consider the environment within which authentication will occur when discussing these issues.

b. Privacy (5 points)

What are the privacy implications of providing such a repository, and are there steps that can be taken to preserve the privacy of those who have registered documents with the repository. How might these privacy measures conflict with the requirement for legitimate access to the data in the repository.

c. System design (10 points)

Sketch the design of a system you have in mind to address these concerns. The design can be procedural, i.e. here is how people will access the data, but you should explain where the data might be stored from a preservation and access perspective. Your answer should focus on the confidentiality, integrity, privacy, and availability aspects of the design.