Name: ________________________ **USC ID:** ________________________

CSci 530 Midterm Exam

Fall 2015

Instructions:

Show all work. No electronic devices are allowed. This exam is open book, open notes. You have **120 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. **(20 points) Cryptography –** For each of the following methods of identification, authentication, or key management match the method with the **major** characteristics or relevant terms discussed in class. This is **not** a one-to-one mapping. So more than one method may match a characteristic or term, and a single characteristic or term may also match more than one method. We are looking for specific characteristics and terms, for which you will receive credit. If you list what is a minor characteristic, while you will not lose credit, you will not get credit either. You will lose a point if you associated a term with a characteristic that does not apply to the method. There are more blanks in the page below than actual correct answers, so you do not need to fill in all the blanks.

   1. Diffie-Hellman Key Exchange
   2. Biometrics
   3. Kerberos
   4. SSL or TLS (as used on typical website)
   5. Passwords
   6. Smartcards

   a) Authenticates Client (or initiating party)

   _____ _____ _____ _____ _____

   b) Authenticates Server (or responding party)

   _____ _____ _____ _____ _____

   c) Enables key exchange between parties

   _____ _____ _____ _____ _____

   d) Strong protection of credentials

   _____ _____ _____ _____ _____

Name: ______________________ **USC ID:** ______________________

2. (40 points) Short Answer

a. Why is it important that strong cryptographic key storage devices perform encryption locally on the device itself, rather than utilize the computer to which they are connected for that function? Give several examples of such devices. (15 points)

b. Briefly mention on the access control mechanisms for files opened within the Unix (or windows or Linux) operating systems is based on both access control lists and on capabilities (15 points).

c. Briefly explain why encryption using a 128 bit long AES key is actually much stronger than encryption with a 512 bit RSA key. (10 points) [answer on back of page]

Name: ______________________ **USC ID:** ______________________

3. (40 points) Design problem – Cryptographic File Access Control

In class discussions, and in the readings, we learned how confidentiality and integrity can be provided in an electronic message system through encryption, key management, and cryptographic has functions. In this question you will apply similar techniques to manage access to files stored in distributed file system. For the purpose of this question, you are to assume that you start with a base storage system that allows individuals to add files, and that the content of the files (data) can be read by anyone, i.e. the underlying data storage system is not providing access control. You should also assume that the users of the system have generated certificates for use with PHP, and that the public keys of these users can be retrieved from a directory.

a. Explain how to protect the confidentiality of the information stored in the filesystem. How would you implement an access control list associated with a stored file, so that only identified and authorized users would be able to retrieve the information stored in the file. (15 points)

b. From a security perspective, how would you manage certain pieces of meta-information about the file, specifically how would you determine the last writer of the file. The same method you use to preserve the last writer will also prevent unauthorized individuals from changing the contents of the file. Describe the mechanism you would use. (15 points – answer on back of page)

c. What you have designed so far is not a complete file system (we have not asked you how to maintain the directory structure, etc). There are certain actions that are traditionally performed on files which are not protected. Briefly list some of the functions that are not subject to the access controls you have described, and comment on the implications that result (in particular, for some purposes might this limitation not make a difference). Feel free to discuss simple changes (at a high level, or in how the system is used) that would make the limitations no matter. (10 points)