Name: ______________________ **USC ID:** ______________________

CSci 530 Midterm Exam

Fall 2016

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. **(20 points) Identity Management –** For each of the following methods of identity 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. Code sent as SMS Text Message
   2. Smart Card
   3. Password
   4. Kerberos
   5. Shibboleth
   6. Secure-ID
   7. Fingerprint

   a) Something you know

   _____ _____ _____ _____ _____

   b) Something you Have

   _____ _____ _____ _____ _____

   c) Something about you

   _____ _____ _____ _____ _____

   d) Relies on possession of encryption key

   _____ _____ _____ _____ _____

   e) Vulnerable to replay attack (in any form)

   _____ _____ _____ _____ _____

   f) Vulnerable to man in the middle attack

   _____ _____ _____ _____ _____

Note that your answer to e and f will require that you think about what is meant by a replay attack of man in the middle attack, and consider how the approach operates. We have probably not pointed to these vulnerabilities in exactly these words in the readings or lectures.

Name: ________________________ USC ID: ________________________

2. (40 points) Short Answer

a. What are the strengths and weaknesses of mandatory access policies as compared with discretionary policies? Why are both kinds of policies important? List at least two examples each of mandatory access control policy models and representations or implementations of discretionary policies. (10 points)

b. Provide an example of how existing network, mobile, cloud, or commercial services today could benefit from technologies supporting mandatory access controls. What would such policies mean for the users of today’s computer systems (what might be different from what they expect of their computers today). (10 points)

c. Explain the steps used by a web browser to exchange an encryption key for use in encrypting the channel of an SSL (or TLS) protected session and to ascertain that it is communicating with the server to which it is trying to connect. (15 points)

d. List as many ways as you can think of for an attacker to obtain access to the information that has been communicated through the SSL (or TLS) connection described in part c. (5 points)

Name: ______________________ **USC ID:** ______________________

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

There has been a lot of recent talk about how state sponsored cyber-criminals are trying to influence our upcoming election through attacks on voter registration systems, possibly voting tabulation systems, and the campaign and personal systems of various candidates for office. You have been hired as an intern at the federal election commission to present proposed measures that can be taken to protect the integrity of our voting systems. Because you have not yet completed CSci530 there are many things that you haven’t been taught yet about security, but your report is to focus on recommendations based on topics from the first half of the course, in particular on the application of cryptography, key management, identity management, and policy and access control.

In the discussion that you provide you may think long term and consider technologies that require deployment of infrastructure not yet universally available so long as you state your assumption and why you believe that infrastructure will be deployed (separate from the voting systems you are discussing). You should not assume that we are looking for a completely on-line voting system. Instead, it will still be the case that the majority of voters will go to a polling place to cast their votes which will then be tallied locally, with results communicated to higher level centers (e.g. local polls to county registrars to the state level who will communicate results nationally and publish the results). Vote by mail (which can possibly include email) can be supported for absentee voters and others.

There will be tradeoffs to consider, balancing the ability to ascertain the integrity of the results (that all votes were cast by authorized voters and correctly counted), secrecy of ballots (that the votes of an individual cannot be determined by others), and convenience and functionality (e.g. ease with which absentee votes can be cast, early voting, etc). No solution is perfect. I am more interested in your reasoning and the effectiveness of your solutions for specific situations.

a. Authentication of voters – How do we know who is voting? (10 points)
   Discuss possible approaches for authenticating voters, either when they show up at a polling place, when they cast their votes in a polling booth, or when they submit an absentee ballot through the mail (including possibly e-mail)? What are the strengths and limitations of the approaches? How might an adversary try to defeat each of the approaches you listed? (please answer on back of page)

Name: ______________________ **USC ID:** ______________________

b. Authorization and Policy (10 points)
What are the actions to be protected by the voting systems (including actions performed only by administrators, and actions performed by voters, and the public in general). Who should have the authority to perform each of these actions? In answering, it is appropriate to consider a role based access control model. Are these policies mandatory policies or discretionary policies?

c. Integrity of Voted Ballots (10 points)
One important concern with an all-electronic voting system is that it does not maintain a "paper trail" of the votes cast. This makes it difficult to audit the election results if a candidate claims that the election was rigged and that someone (or a piece of malware) manipulated the vote tallies. Discuss approaches that will create an audit trail that can be reviewed after the election if fraud is suspected. How might your approach work together with some of the authentication technologies you described in part (a).

d. Secrecy of votes (10 points)
At least for the casting of votes at a polling place, what measures can be taken to assure the privacy of votes (protect information about who voted for whom)? Certainly one way would be to record only the vote totals, and not individual ballots, but I am more concerned with how to protect the privacy of votes while also providing an auditable record of how votes were cast as described in c.
(answer on back of page)