Name: _____ **USC ID:** _____

CSci 530 Midterm Exam

Fall 2017

Instructions:

Show all work. This exam is open book, open notes. You may use electronic devices if your references materials are stored on the device, and as long as communication is disabled (e.g. Airplane mode). You may not use your device for communications and you may not use it to retrieve information from the web or from files stored elsewhere. 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) Cryptography and Key Management -** For each of the following methods of encryption 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. AES in Cipher Block Chaining Mode
    2. One Time Pad
    3. RSA
    4. AES in Output Feedback Mode
    5. Diffie-Hellman Key Exchange
    6. Public Key Infrastructure (use of a Certification Authority)
    7. Key Management in Kerberos

    a) Involves a Trusted Third Party

    _____ _____ _____ _____ _____

    b) Involves public keys or public key cryptography (asymmetric)

    _____ _____ _____ _____ _____

    c) Involves conventional keys or conventional cryptography (symmetric)

    _____ _____ _____ _____ _____

    d) Strong protection of confidentiality

    _____ _____ _____ _____ _____

    e) Strong protection of Integrity

    _____ _____ _____ _____ _____

    f) Requires Initialization Vector

    _____ _____ _____ _____ _____

Name: _____ **USC ID:** _____

2. (40 points) Short Answer

a. What are the main differences between the Bell-LaPadula model for authorization as compared with the Biba Model. (10 points)

b. Provide two examples for each and discuss two advantages or disadvantages each, for each of authentication based on i) something you know; ii) something you have; and iii) something about you. (for each of these I, ii, and iii, your answer should include the two examples, and then two sentences - those sentences describing and advantage or disadvantage of the approach). (20 points, answer on back of page)

Name: _____ **USC ID:** _____

c. Provide two examples of information flow policies and explain how they are useful to prevent information disclosure and system compromise. (note that you may need to rely on the discussion in lecture, rather than simply searching for the term in the lecture notes) (10 points)

Name: _____ **USC ID:** _____

3. (40 points) Design problem - The Equifax Data Breach - and Solutions

You have been hired as a consultant to advice on the response to the Equifax data breach. Your new employer understands that you have not taken the section of this class on malicious code, so you are only being asked to advise on technology solutions related to cryptography, identity management, and or policy. You will be asked how changes to the way these services are used in the credit reporting industry can help to mitigate the impact of the Equifax breach, or how these technologies might prevent similar breaches from occurring in the future.

A) Authentication Technologies – Problems with our current approach

What is wrong with the existing form of authentication of individuals applying for credit, and why is this a significant problem following the recent Equifax data beach. In answering this question focus on the initial authentication that is performed during "enrollment" (i.e. opening a new account), rather than the authentication performed after an account has been opened. (10 points)

B) Authentication Technologies – Improving the Situation

Thinking along the lines of federated identity (this is a hint of one possible approach), or along other lines if you choose to do so, suggest alternative ways to "enroll" users for new accounts (e.g. when applying for a new card). Discuss the advantage of your approach as compared with existing techniques. Discuss the limitation of your approach: what does it depend upon for security? Are there cases that it cannot be applied for certain users? How might a criminal attempt to get around the protections provided? What else might you do to mitigate some of these failures? (15 points – answer on back of page)

Name: _____ **USC ID:** _____

C) Preventing these kinds of breaches in the future - Improving data access policy

It is believed that the attack exploited a known vulnerability in a software package that was used on a web server managed by Equifax. This specific attack could have been prevented if the appropriate patches had been applied, but there are many vulnerabilities that do exist for which the attacks are unknown (sometimes called a zero-day attack) and for which patches are not yet available. To address security comprehensively, we must design our system so that a vulnerable software module does not have significant access to all of the information in an enterprise such as Equifax. Part of that design involves applying policies for access to data (confidentiality and Integrity) that will limit the impact of these inevitable vulnerabilities.

Discuss some of the kinds of policies that might be applied in the Equifax system that could reduce the impact of the breach that affected the vulnerable web server. (15 points)