Name: _____ **USC ID:** _____

CSci 530 Midterm Exam

Fall 2019

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 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) Policy Management** - For each of the following methods of representing policy, 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 approach may match a characteristic or term, and a single characteristic or term may also match more than one approach. 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. Access Control List
    2. Capability List
    3. Access Matrix
    4. Bell LaPadula
    5. Biba
    6. Clark-Wilson Model
    7. Role-Based Access Control

    a) Associated with object

    _____ _____ _____ _____ _____

    b) Separation of roles

    _____ _____ _____ _____ _____

    c) Objects have Labels, Subjects have Clearances

    _____ _____ _____ _____ _____

    d) Star Property

    _____ _____ _____ _____ _____

    e) Can be used to specify Confidentiality Policy

    _____ _____ _____ _____ _____

    f) Discretionary Access Control Model

    _____ _____ _____ _____ _____

    g) Associated with subject

    _____ _____ _____ _____ _____

Name: _____ **USC ID:** _____

2. (40 points) Short and medium length answers

a. Give several examples of authentication based on *something you know*. Be sure to include approaches based on something you know that require providing that information to prove your identity, and also approaches where you prove that you know something without actually sending the information at the time of authentication. Explain some of the problems/limitations of authentication based on *something you know.* (15 points)

b. What is special about devices used for authentication based on *something you have* that provides stronger protection from impersonation. Be specific in answering this question. (5 points) (answer on back of page)

c. Explain the importance of using good (strong) random number generation in cryptographic protocols. How does using poor random number generation create a similar problem as one of the limitations you should have mentioned in part (a) regarding weaknesses of authentication based on something you know. (10 points)

d. Explain some of the consequences of using a weak hash function in a cryptographic protocol (i.e. one for which it is easy to find collisions). Provide a specific example of an attack that would work against such a system.
(10 points) (answer on back of page)

Name: _____ **USC ID:** _____

3. (40 points) Evaluate design of End-To-End Security Protocols

a. Explain the role of a trusted third party when performing key management (as well as authentication) in systems that utilize conventional cryptography, and also in systems that use public key cryptography (I would suggest using Kerberos, and the combination of TLS/SSL with Public Key Infrastructure). How is it that we trust the third party in these systems (by this I mean what is at risk if the third party is compromised). More specifically, for each of the key management systems you are discussing, tell me whether compromise of the third party will allow an adversary to impersonate users or systems, whether it will allow an adversary to fraudulently sign documents, whether an adversary can intercept and read communication between the legitimate parties, and if so, whether this ability extends to past communications, current communications, and or future communications. (15 points)

b. Explain the benefits of end to end encryption in systems like PGP. Why do we have stronger assurance of the confidentiality of our communication in such systems than we would have based on a hop-by-hop encryption as is supported through transport layer security systems such as SSL and TLS? (5 points) (answer on back of page)

c. When end-to-end encryption was added to Whats App, key management was facilitated through servers managed by Facebook who owns Whats App (these servers fill the role of a certificate authority). How might this affect the ability of an intermediary to intercept and read end-to-end messages sent in the future? (10 points)

d. Explain how one can modify the design of a security protocol like SSL or TLS, to utilize Diffie-Hellman Key exchange to limit the ability of an adversary who compromised one of the end points (learned their long term private or secret key) from being able to decrypt messages that were sent in the past between the parties (the property you are adding is known as perfect forward secrecy).
(10 points) (answer on back of page)