Name: _____ **USC ID:** _____

CSci 530 Midterm Exam

Fall 2010

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. **(30 points) Cryptography** - For each of the following methods for encryption or key management methods, match the method with the **major** characteristics discussed in class. This is **not** a one-to-one mapping. Some more than one method may match a characteristics, and a single method may also match more than one characteristic. We are looking for specific characteristics, for which you will receive credit. If you list what is a minor characteristic (for example, that DES by itself does not provide authentication), while you will not lose credit, you will not get credit either. You will lose a point if you associated a method 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. One time pad
    2. AES in Cipherblock Chaining Mode
    3. Diffie-Hellman-Key exchange
    4. RSA with a 1024 bit key
    5. DES in output feedback mode (OFB)
    6. DES in Electronic Code Book (ECB) mode

    a) Key exchange without authentication

    _____ _____ _____ _____ _____

    b) Does not provide integrity protection

    _____ _____ _____ _____ _____

    c) Sparse key space

    _____ _____ _____ _____ _____

    d) Provable / perfect confidentiality protection

    _____ _____ _____ _____ _____

    e) Uses an initialization vector

    _____ _____ _____ _____ _____

    f) Block cipher

    _____ _____ _____ _____ _____

    g) Uses asymmetric keys

    _____ _____ _____ _____ _____

Name: _____ **USC ID:** _____

2. (30 points) Authentication and Key Management

Discuss the authentication methods used during the lifecycle of an electronic mail message. Enumerate the authentication methods that may be used at different stages in the composition, submission, delivery, retrieval, and reading cycle. Note that for communication by email in the real world, more than one of these methods are likely to be used - it is not an either/or implementation. For each, discuss:

a. For each method, what entities are authenticated (e.g. the sender, the recipient, an intermediate server), what is the basis for the authentication (e.g. what credentials are used), and what is the purpose of the authentication (e.g. what are we trying to protect against) (10 points)

b. For each method, what is the period over which the authentication persists? In particular, does the authentication last only during the life of a session, or can someone viewing a message one month later still validate the authentication? (10 points)

Name: _____ **USC ID:** _____

c. Discuss the limitations of each method. What are the difficulties in deployment? If a method only works (meets the goal of the "purpose" you listed in part "a") under certain assumption, discuss these assumptions. (10 points)

Name: _____ **USC ID:** _____

3. (40 points) Design problem

You have been hired by the Southern California Power Department to design their next generation home energy power management system. This system will support the dissemination of current power pricing information to devices in the customer's home. It will also support the transmission of power usage data from the customers power meter to the utility. For those users that subscribe to third party (web sites run by organizations other than the SCPD) power portals, selected usage data will be provided in real time to such third party sites, where it may be processed and presented to the user, or accessed by appliances at the customers' home for display or to make power management decisions.

a. Discuss in general terms the confidentiality and integrity policies that should be associated with the data and messages in such a system (i.e. what kinds of principals access data in such a system, what kinds of data and messages exist in the system and for each class of data, which principals should have what kinds of access). (15 points)

b. For each of the policies that you mentioned in (a), tell me whether the policy is a mandatory access controls, discretionary access controls, or a combination? Justify your answer. (5 points)

Name: _____ **USC ID:** _____

c. When (or for what activities) is authentication required in the system you are designing? For each instance where such authentication is required indicated the basis for authentication, and suggest an approach for implementing the authentication mechanism. (20 points).