Name: _____ **USC ID:** _____

CSci 530 Midterm Exam

Fall 2012

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 - 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. AES as a block cipher
    2. One time pad
    3. Diffie-Hellman-Key exchange
    4. RSA with a 256 bit key
    5. DES in cipher feedback mode (CFB)
    6. DES in Electronic Code Book (ECB) mode

    a) Suitable as the basis for providing authentication

    _____ _____ _____ _____ _____

    b) Provides strong integrity

    _____ _____ _____ _____ _____

    c) Dense key space

    _____ _____ _____ _____ _____

    d) Provable / perfect confidentiality protection

    _____ _____ _____ _____ _____

    e) Uses an initialization vector

    _____ _____ _____ _____ _____

    f) Stream cipher

    _____ _____ _____ _____ _____

    g) Uses a single key shared by sender and receiver

    _____ _____ _____ _____ _____

Name: _____ **USC ID:** _____

2. (30 points) Identity Management

Answer the following questions regarding identity management:

a. The three "factors" for authentication bay be describes as "something that is known", "something that one has", and "something about an individual". Explain how effective implementation of the second and third factors are each dependent on "something that is known". (10 points)

b. What is the goal of federated identity management (what advantages does it provide)? Be sure to consider both kinds of federated identity management systems: those that use a common implementation and are federated only administratively, as well as those that support federation across different implementations for authentication (such as web based federated identity management systems). (10 points)

c. What are the difficult of effectively implementing federated identity management system? For any difficulties you identify, indicate which kind of system (from the kinds in part b) the difficulty applies to. (10 points) [answer on back of page]

Name: _____ **USC ID:** _____

3. (40 points) Design problem

You have been asked to design the key management system for a smart meter system to be used by power companies (utilities) across the world. In this system, utility owned smart meters will be installed on customer's houses. These meters will communicate in a wireless mesh (meaning that one meter will send packets to another meter, which will forward the packets until they reach a "concentrator" on a power pole, which will then send the packets back to the utility over a fiber optic link or a long haul radio link). Important security goals for the communication are that the integrity and privacy of customer data be maintained, and that the system should be resistant to denial of service attacks. Certain functions of the meters may be controllable remotely by utilities, and there might be a capability to update the software on the meters by the utility over the network. The meters are also capable of communicating with certain devices in each customer's home.

My advice to you for answering the questions that follow is to read all parts of the question up front, then think about creating a table to represent some of the answers to the different parts, and refer to your table in the answer to the questions that follow (for example, create a table with column one representing the answer to part a, with column to containing the corresponding answer to part b, and possibly other columns as well to answer the other parts of the question, then in your answer to a, simply state that the answer is in the first column of the table, etc).

a. List the entities that need encryption keys in such a system. Entities may be specific devices, certain people, etc, but list the different kinds of devices and the different roles of people, etc)? (5 points)

b. For each of the entities your listed in part a, list the keys that need to be provided up front (the term is "provisioned") and the kind of each key (e.g. a secret key, a private key, a public key). (10 points)

c. For each of the KEYS listed in part b, indicate who else shares the key. If they key is a private key, then indicate that the key is PRIVATE, and tell me who knows the corresponding public key. (10 points)

d. Describe briefly the purpose of each key and indicate the reason that you chose a secret, private, or public key for that purpose, and the reason for sharing the key (or the corresponding key) or for not sharing the key (or the corresponding key) with other entities in the system). (15 points)