

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 characteristic, 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)