Name: _____ **USC ID:** _____

CSci 530 Midterm Exam

Fall 2014

Instructions:

Show all work. No electronic devices are allowed. This exam is open book, open notes. You have **120 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 -** For each of the following encryption algorithms or modes of operation 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 mode or algorithm may match a characteristic or term, and a single characteristic or term may also match more than one mode or algorithm. 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. DES
    2. RSA
    3. AES
    4. One Time Pad
    5. Cipher Block Chaining (CBC)
    6. Output Feedback Mode (OFB)

    a) Asymmetric

    _____ _____ _____ _____ _____

    b) Symmetric

    _____ _____ _____ _____ _____

    c) Poor Integrity Protection

    _____ _____ _____ _____ _____

    d) Dense Key Space

    _____ _____ _____ _____ _____

    e) Non-repudiation

    _____ _____ _____ _____ _____

Name: _____ **USC ID:** _____

2. (40 points) Short Answer

a. List in approximate order all of the encryption and decryption steps required to send, receive, and verify the authenticity of an email message using PGP (when the senders and recipient's certificates are available to one another - but not yet verified). By list, I mean tell me what is encrypted or decrypted, and using what key. (20 points)

b. Using examples of each, explain the difference between a mandatory access control policy and a discretionary one (you need to say more than just list the examples)? (10 points)

c. Why is Diffie Hellman key exchange useful only for agreeing on a shared key, and not useful for authentication? (10 points) [answer on back of page]

Name: _____ **USC ID:** _____

3. (40 points) Design problem - Smartphone Payments

You have been hired by a smartphone maker to create an electronic wallet capability which will allow users of the device to register credit cards and use the phone instead of the cards to securely make payments, either online, or at point of sale. The cell phone has communications capabilities for near field communications and for wifi. Within the next year, most credit cards will be issued as "chip" cards, which are essentially smart cards. You will be asked questions about your design.

a. Please list the most important design considerations about your approach that will ensure that information needed by the phone to prove that it is a particular phone, or that it has access to a card, is not disclosed to merchants, criminals, or other entities in the system. (10 points)

b. Describe any specific features of the phone hardware that you believe will be necessary to provide the level of security you are required to implement. (10 points - answer on back of page)

c. How will you register a new account with a phone? By this I am asking how you will associate an account with a phone so that the phone can be used to initiate a payment from a particular credit card account. What information will be exchanged between the phone and other computers (e.g. the credit card has its own computer chip, and the card issuer also has computers). How will this approach prevent an adversary from associating a card with a phone that should not be authorized (e.g. how do you prevent someone that gets temporary access to your card or phone from associating the card with their own phone)? (15 points)

d. What kinds of vulnerabilities remain in your design? E.g. for a system implemented according to your design, what kinds of incorrect actions might an attacker still be able to accomplish and how will they be accomplished? (5 points - answer on back)