Name: _____ **USC ID:** _____

CSci 530 Final Exam

Fall 2010

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**.

In particular, **each numbered questions must appear on separate pieces of paper so that the exam can be split for grading**. If part of the answer to one of the questions (Q1, Q2, or Q3) is on a sheet of paper also used for one of the other questions, then that part of your answer might not be graded and you will NOT receive credit for that part of your answer.

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**	**Letter**
Score					

Name: _____ **USC ID:** _____

1. (30 points) Wikileaks and the Doomsday File

If you have been following the news around Wikileaks, you are probably aware that they have distributed a "Doomsday file" containing the yet unreleased data provided to Wikileaks, most likely in unedited and unfiltered form as an attempted defense against action being taken against them. This file has been encrypted with a 256 bit AES key, and only the Wikileak leader and a few close trusted associates know the key, but can easily release the key, making all of this data available. The encrypted file has been widely distributed, such that it would be practically impossible to destroy all copies of the file.

From interviews with "computer security experts" the media reports that this file would be extremely difficult to crack, taking many years, and that as a result governments are unlikely to be able to crack the file and prevent the disclosure of the data if the key were to be released.

We have discussed cryptography and the strength of various cryptosystems in class. Given you understanding of the purpose of cryptography, please explain what is completely wrong about the statement in much of the media (in the second paragraph). Discuss what the real implications are of 1) the distribution of the encrypted file, and 2) of a successful cracking of the encryption. Further, explain 3) why governments might be trying to break the encryption on this file, and 4) if they were to be successful in decrypting the file within the next 10 years, list the some of the most likely techniques or reasons that they might succeed.

Name: _____ **USC ID:** _____

2. (30 points) Matching attacks and defenses

For each of the following systems or mechanisms, match the numbered system or mechanism with the lettered attack against which it is effective, or with a property or assurance that it provides. This is **not** a one-to-one mapping. So more than one system may match an attack, and a single method or mechanism may also match more than one attack or property. We are looking for specific matches for which you will receive credit. If you list a match that we are not looking for, but which is still correct, while you will not lose credit, you will not get credit either. You will lose a point if you associated a defense with an attack against which it is not effective. There are more blanks in the page below than actual correct answers, so you do not need to fill in all the blanks.

1. File or Object Encryption
2. Hash Functions
3. Network Based Intrusion Detection
4. Host Based Intrusion Detection
5. Virus Scanners
6. Anomaly Based Intrusion Detection
7. Host Based Firewall
8. Embedded Firewall
9. Network Firewall
10. Trusted Computing
11. Network Encryption (including SSL/TLS and IPSec)
12. Digital Signatures

a) Confidentiality: _____ _____ _____ _____ _____ _____ _____

b) Integrity: _____ _____ _____ _____ _____ _____ _____

c) Virus Defense: _____ _____ _____ _____ _____ _____ _____

d) Worm Defense: _____ _____ _____ _____ _____ _____ _____

e) Denial of Service Defense: _____ _____ _____ _____ _____ _____

f) Malware Defense: _____ _____ _____ _____ _____ _____ _____

g) Insider Threat: _____ _____ _____ _____ _____ _____ _____

Name: _____ **USC ID:** _____

3. (40 points) Design Problem

Because of the massive leaks of sensitive data on Wikileaks, you have been hired to improve the security of the systems used to disseminate such information within the federal government. Having paid attention during discussions in your advanced operating, you understand that the leaks were the result of an "insider threat", i.e. a trusted employee who betrayed that trust and sent the information to Wikileaks. You have been told that the purpose of the system that was compromised was to support the dissemination of the kind of information that was released, widely within the US government so that intelligence gathered by one agency is not kept out of the hands of those that legitimately need it to defend against criminal of terrorist threats. Unfortunately, the more widely disseminated information is within the government, the more likely it will be compromised through insider threats, and you just cannot get around that problem. So, you have been hired for an impossible task. When faced with such an impossible task, the only way to succeed is to redefine the problem.

a. Given that it is still necessary to disseminate this information widely within the government, and thus that we cannot eliminate the insider threat, discuss an achievable task goal (define what you can accomplish) that will minimize the impact of such future leaks. (10 points).

b. What defense mechanisms discussed in class are likely to be useful in limiting the extent of the release of such data via insider threats? Note that this is not as simple as it seems, as it requires significant thought. In particular, things about the achievable task goal identified in (a) to drive your solution.
(b and c together 30 points) - answer on back of this page.

Name: _____ **USC ID:** _____

c. For each of the mechanisms listed by you in (b) explain how you would implement or deploy the measure to prevent future significant leaks of sensitive information. (b and c together 30 points)