Milwaukee School of Engineering

Electrical Engineering and Computer Science Department

SE-4920 – Computer Security – Final Exam

Print Name: _____

- This is a take-home exam.
- The exam will be emailed to the class before 8:00 A.M. on Monday 21 May 2007.
- **Email your completed**, typed responses to the exam in Word, PDF, or other nicely styled format to the instructor by **8:00 A.M. on Wednesday**. You must be finished with the exam by this time. Any **handwritten items** (*e.g.*, figures for the final problem) may be submitted to the instructor's mailbox by **1:00 P.M. on Wednesday**.
- You may not consult with anyone except the instructor about the content of this exam.
- The instructor will be available at various times to answer questions, both in his office, and via email.
- You **are allowed to use** both textbooks, the PDF notes the instructor provided on the online course outline, any other materials **directly** linked from the course website, and any class notes that you had before this midterm was distributed. You **are not allowed to use** any other materials.
- You are allowed to work on this exam for a **maximum of 3 hours**. You must complete the time log below. Any time spent actively working on the exam (writing/typing ideas, reading it) must be included. (Thinking about the exam does not need to be logged as long as you are not referring to any references, the exam itself, or your written/typed responses.)
- You **must sign** a hardcopy of this page in ink below, signifying that you have followed these rules.

Sign Here: _____
*I have neither given nor received aid on this exam, and have followed all the above rules.*

Time Log
(Enter times as "hh:mm A.M./P.M." Use local time (CDT-0500).
Enter durations as "hh:mm".)

| Begin | End | Interruption | Total | Notes |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | **Total** | | |

## Problems

1. (5 points) **Explain** the **avalanche effect** in the context of hash functions.

2. (7 points) **Consider** the following **approaches** to creating a message with a signature using a public key algorithm:
   A. Encrypt the message using the private (decrypting) key so that anybody can receive it and verify that it came from the private key holder
   B. Transmit the plaintext message. Also transmit a version of a hash of the message encrypted using the private (decrypting) key.

B is the approach commonly used and has various advantages over A. **Discuss** at least **two** such distinct advantages.

Perform the following operations in **mod 7** arithmetic, giving all answers in reduced mod 7 form.

3. (3 points) **Add** 3 to 6.

4. (4 points) **Calculate**/find the **additive inverse** of 6 and justify your response.

5. (5 points) **Find**/calculate the **multiplicative inverse** of 5 and justify your response.

6. (20 points) The basic **Diffie-Hellman algorithm** is susceptible to an active, man-in-the-middle attack (hint: see last slide of 4/3 notes). When discussing chapter 16 on 4/27, we discussed a modification of Diffie-Hellman that has the perfect forward secrecy property (Figure 16-2 in the text). This modified exchange also defends against the man-in-the-middle (MIM) attack. **Illustrate** how an attacker can execute an MIM attack against basic Diffie-Hellman. **Then, illustrate** how an MIM attack would fail in the enhanced Diffie-Hellman exchange. **Discuss** the choice of messages that the MIM attacker sends to each side. (Note: there are at least 2 approaches to an MIM attack on the enhanced algorithm—you may illustrate any attack as long as proper supporting discussion is provided [justify the need/reason for the attacker to send each message].)

7. (4 points) What is a **difference** between a **passive RFID** tag and an **active RFID** tag?

8. (6 points) Briefly **describe** a type of consumer action or habit tracking that could be made possible by increased use of RFID in the retail environment that is **not possible** using "traditional" customer loyalty/discount cards (e.g., the type that Pick 'n Save requires the use of in order to receive a sale price).

9. (6 points) **Why** do many systems that store password hashes **salt** the passwords before hashing?

10. (6 points) **Contrast** the image acquisition technologies for **iris-** and **retina-based** biometric identification. **Which** is less invasive?

11. (4 points) **Describe** one of the methods discussed by the presenters by which a fingerprint reader could be fooled.

12. (4 points) What is "**live tissue verification**" as it applies to biometric ID techniques, such as retinal scans and fingerprint scans?

13. (5 points) **Describe** one way in which User Account Control in Windows Vista improves on Windows XP security.

14. (5 points) **Explain** the "digital hole" as it applies to securing digital video.

15. (4 points) Generally, cryptography algorithms are based on "hard problems". **Which hard problem** is the basis for elliptic curve cryptography?

16. (6 points) **What** are the **two key items** stored for each entry in a rainbow table and **why**?

17. (6 points) In NTFS security, we learned from a presenter that files are encrypted using file-specific keys, and then those keys are encrypted with users' public keys. This has many advantages over direct encryption with the users' public keys. **Discuss one.**