Georgia Tech *College of Computing*

Georgia Institute of Technology

CS 4235: Computer Security: Fall 2011

Quiz II

There are 13 questions and 8 pages in this quiz booklet (including this page). Answer each question according to the instructions given. You have **85 minutes** to answer the questions.

If you find a question ambiguous, write down any assumptions you make. **Be neat and legible.** If I can't understand your answer, I can't give you credit!

Use the empty sides of this booklet if you need scratch space. You may also use them for answers, although you shouldn't need to. *If you do use the blank sides for answers, make sure to clearly say so!*

Note well: Write your name in the space below AND your initials at the bottom of each page of this booklet.

THIS IS AN "CLOSED BOOK, CLOSED NOTES" QUIZ.
NO BOOKS, NO NOTES, NO OTHER MATERIALS, NO PHONES, NO COMPUTERS, NO LAPTOPS, NO PDAS.
MAKE SURE YOU'VE READ ALL THE INSTRUCTIONS ABOVE!

Initial here to indicate that (1) you've read the instructions and (2) you agree to abide by the Georgia Tech Honor Code:

Do not write in the boxes below

1-5 (xx/20)	6-10 (xx/30)	11-13 (xx/10)	Total (xx/60)

Name:

I Warmup

1. [4 points]: Which of the following are true of different types of ciphers?

(Circle ALL that apply)

A. The security of the one-time pad depends on the hardness of factoring.

B. The security of Diffie-Hellman Key Exchange depends on the hardness of the discrete log problem.

C. The security of the RSA cryptosystem depends on the hardness of factoring.

D. In the RSA cryptosystem, signing is mathematically equivalent to decryption.

E. All of the above.

2. [4 points]: Which of the following are true about port scans, such as the one you ran on Problem Set 4? Assume that the port scanning tool only sends TCP "SYN" packets, as the `nmap` tool you used does.

(Circle ALL that apply)

A. A port scanning tool can be used to discover the version of a Web server that a host is running.

B. A port scanning tool can be used to discover the version of an operating system that a host is running.

C. A host can protect itself against port scanning by simply not responding to any of the port scanning tool's TCP SYN probes on any port.

D. Port scanning can be used to determine what services are running on a particular host.

E. All of the above.

3. [4 points]: Which of the following is true about cryptographic hashes?

(Circle ALL that apply)

A. Cryptographic hash functions are designed to be collision-resistant to prevent message forgery.

B. If two parties have previously agreed on a secret key, a cryptographic hash function can be used to generate message signatures.

C. If two parties have previously agreed on a secret key, cryptographic hash functions can be used to encrypt messages.

D. Cryptographic hashes are sometimes used to generate "digests" of public keys that are easier to recognize than the public key itself.

E. All of the above.

4. [4 points]: Which of the following are true about various cryptanalysis attacks?
(Circle ALL that apply)

A. An attacker who knows that a given application protocol (e.g., HTTP) starts with the same protocol messages could perform a known plaintext attack on the ciphertext.

B. A successful known plaintext attack can result in recovery of both the full plaintext of the message and they key that was used to encrypt the message.

C. A brute force attack on an encryption algorithm becomes exponentially more difficult as the size of the key increases.

D. Generating a collision becomes exponentially more difficult as the number of bits in the hash increases.

E. All of the above.

5. [4 points]: Which if the following are true about cross-site scripting (XSS) attacks?
(Circle ALL that apply)

A. An attacker can use an XSS attack to steal a victim's Web cookies for another Web site.

B. A user can defend against XSS attacks by preventing the browser from executing any scripts.

C. A Web site can defend against an XSS attack by ensuring that the input to a script does not itself contain any code.

D. An attacker could launch an XSS attack by posting a comment on a message board.

E. All of the above.

II Potpourri

6. [6 points]: Suppose that you have a hash function that takes input and randomly generates a 16-bit value. What is the probability of collision if the hash value takes 10 inputs? *Show your work.*

(Answer legibly in the space below.)

7. [6 points]: Explain the purpose of Diffie-Hellman key exchange. Show a diagram of exchanges that demonstrates that Diffie-Hellman is vulnerable to a man-in-the-middle attack. Use A for Alice's secret, B for Bob's secret, and M for Mallory's secret. Also use g as the base for exponentiation, and p as the modulus. (So, Alice starts by sending Bob $g^A \mod p$, but this is intercepted by Mallory.) What does the attacker know after mounting this attack?

(Answer legibly in the space below.)

Alice **Mallory** **Bob**

Initials:

8. [6 points]: Define *perfect security*, and explain why a one-time pad generates perfect security. Explain why re-using a one-time pad can introduce weaknesses in the security of the one-time pad.

9. [6 points]: Given the password "security" for the PlayFair cipher, fill in the matrix below to generate the PlayFair matrix. What is the resulting cipher for the word "quiz"? Explain why the PlayFair cipher is more secure against statistical attacks than a standard substitution cipher, like the Caesar cipher.

(Answer legibly in the space below.)

(Answer legibly in the space below.)

10. [6 points]: Suppose an attacker is running a Web server that runs a script that takes user and password input from a form and retrieves the information for that user, as follows:

```
set ok = execute( "SELECT * FROM Users
   WHERE user=' "  &  form(user)  & " '
           AND   pwd=' " & form(pwd) &  ' );
if not ok.EOF
           login success
else  fail;
```

A. Write down input to the “user” part of the form that would cause the database to reveal every row of the table (i.e., information for all users).

B. Write down input to the “user” part of the form to cause the entire user table to be deleted.

(Answer legibly in the space below.)

Initials:

III Onion Routing

George Burdell learned about Onion Routing in class and has installed Tor on his laptop, to try to prevent the Georgia Tech network administrators from eavesdropping on his Web surfing activity. George is surprised to find out that Web surfing with Tor is incredibly slow, and asks you whether you know why.

11. [3 points]: Explain how onion routing works in the space below. Suppose you have a message, M, that you wish to send to a user Alice. Write down the onion encryption for M to send the message to Alice, first via node A, then via node B, and finally via an "exit node" C. Use the notation $\{M, Y\}_X$ to indicate that a message M that should be sent next to node Y is encrypted with the public key for node X. *Your answer should have multiple nested encryptions.*

(Answer legibly in the space below.)

George is disappointed that Tor requires so many nested encryptions and suggests instead that the message only be encrypted for user Alice, rather than for each hop. "Reducing the number of encryptions would make the system much faster, since each node would not need to decrypt a layer of the message."

12. [3 points]: Explain to George what properties of Tor would be lost if each hop of the Tor path were not encrypted.

(Answer legibly in the space below.)

Initials:

13. [4 points]: George observes that if the entry and exit nodes of a Tor path are located within the same Internet service provider, there is some likelihood that that Internet service provider could mount an attack to link the sender and receiver of a message: “If an ISP can see both the traffic entering and exiting Tor, it might be able to determine which traffic was destined to which receiver.” Is he right? If he is right, how would you fix the vulnerability? If he is wrong, why is he wrong?

(Answer legibly in the space below.)