Milwaukee School of Engineering
Electrical Engineering and Computer Science Department
Dr. Durant

CS-4920 – Information Security
Midterm Exam

Name: _____

Read all questions carefully – some have multiple parts.

Closed notes, book, calculator, laptop, etc.

Please ask if any questions are not clear.

Good luck!

Page 2:	_____	of 20
Page 3:	_____	of 30
Page 4:	_____	of 15
Page 5:	_____	of 20
Page 6:	_____	of 15
Total:	_____	of 100

1. (20 points) Based on the framework of Schneier's "Liars and Outliers," consider a workplace society in which the group interest is giving the right people credit for their good ideas and the competing interest is for each individual to get credit for good ideas regardless of who came up with them. Give an example of a societal pressure enforcing the group norm that falls into each of the following categories:
    a. Moral
    b. Reputational
    c. Institutional
    d. Security

2. (10 points) Define “confidentiality” and “integrity”.
3. (5 points) Why is “security through obscurity” (e.g., keeping algorithms secret) not considered a sound security practice?
4. (5 points) Why do faster computers generate a greater relative benefits for the users of cryptography than the attackers of it?
5. (10 points) We discussed 3 classes of cryptographic functions (secret key, public key, and hash function). Which of them, in their most basic use, requires that some information not be available to the entire world? For each algorithm class you’ve identified, define the information that is not public.

6. (15 points) 3-hat problem

    a. (5 points) State the solution to the 3-hat problem presented in class (3 players each wearing a hat that may be any of 3 colors; each player can only see the other 2 hats; exactly one player will correctly guess his color of hat).
    b. (10 points) Explain why the 3-hat solution works.

7. (10 points) A hash function takes an arbitrary length message and generates a 64-bit hash value. It begins with a hash register of 0xA5A5A5A5_A5A5A5A5 then successively grabs 2, 6-bit values from the message and uses them as positions of bits to exchange in the hash register. The hash value is the final value of the register. Assume that the padding method (what to do if the message length is not a multiple of 12 bits) and endianness are defined for the algorithm (the details are unimportant). There are numerous reasons that this hash is not cryptographically secure – list 3-5 reasons (2-4 points each depending on quality/clarity, maximum of 10 points).
8. (10 points total, 2 points each) True or false
    a. True or false: Secret key algorithms are asymmetric.
    b. True or false: Public key algorithms can be used for signatures.
    c. True or false: ECB (electronic codebook) requires knowing the previous ciphertext and the current plaintext to calculate the current ciphertext.
    d. True or false: In a secret key algorithm, there must be enough keys to generate any possible plaintext to ciphertext mapping.
    e. True or false: Triple DES uses up to 3 times the number of key bits as DES, but is only twice as hard to break.

9. (5 points) What property should a mode of operation for large storage (e.g., an encrypted hard drive) have that would not be important for a non-recorded, secure video stream?
10. (5 points) Given a well designed 20-bit cryptographic hash function, about how many distinct objects would you expect to see before encountering a hash collision?
11. (5 points) What is a preimage attack (against a hash)?