

CS 361 Midterm: Spring, 2006
Sample Questions
Instructor: Dr. Bill Young

March, 2006

Name: _____

Answer all questions in the space provided. You may use scratch paper to do your work but only answers recorded on the test paper will be graded. Be as concise as possible.
Note: the questions on this sample are all questions asked on past midterms.

Page 1:	_____	(20)
Page 2:	_____	(10)
Page 3:	_____	(20)
Page 4:	_____	(10)
Page 5:	_____	(20)
Page 6:	_____	(10)
Total :	_____	(90)

1. (10 points) Suppose you have a secure system with three subjects and three objects, with levels as listed below.

Type	Name	Level
Object	Obj1	$(H, \{A, B\})$
Object	Obj2	$(L, \{B\})$
Object	Obj3	$(L, \{A, B\})$
Subject	Subj1	$(L, \{A, B\})$
Subject	Subj2	(H, \emptyset)
Subject	Subj3	$(L, \{A, B, C\})$

Here H dominates L . You wish to implement a Bell and LaPadula model of security for this system. Fill in the access rights (**R** and/or **W**) permitted by the model for each subject/object pair in the access matrix below:

	Obj1	Obj2	Obj3
Subj1			
Subj2			
Subj3			

2. (10 points) Assume you have a six sided die that is lopsided in such a way that it rolls each of 1, 2, or 3 twice as often as each of 4, 5, or 6. You wish to send the results of a series of rolls over a transmission channel. Compute the entropy of this language. (Please write down the appropriate sum; you don't have to compute a numeric answer.)

3. (10 points) Imagine a Bell and LaPadula-like secure system with the following five operations.
- (**READ s o**): if the subject and object exist and have the right relationship, the subject obtains the current value of the object; otherwise, do nothing.
 - (**WRITE s o v**): if the subject and object exist and have the right relationship, the object gets value v ; otherwise, do nothing.
 - (**CREATE s o**): add a new object with the given name, a level equal to the subject's level, and an initial value of 0. If an object of that name exists, do nothing.
 - (**DESTROY s o**): eliminate the designated object from the state, assuming that the object exists and the subject has **WRITE** access to it. Otherwise, do nothing.
 - (**RUN s**): the named subject runs some arbitrary private code that cannot access or modify any of the objects on the system.

A covert channel exists because a high level subject can modulate the existence of objects in such a way that a low level subject can “view” the result. Display a shared resource matrix appropriate for this system that exhibits the channel.

4. (Short answer – 20 points) Fill in the word or phrase that *best* matches the description provided. In most cases, what is needed is a general term, not a specific instance of the concept.
- (a) _____ Security concern involving whether resources are on hand when needed.
 - (b) _____ Describes an information transmission medium over which a message is transmitted without distortion or loss of information.
 - (c) _____ An encryption algorithm that replaces each symbol uniformly by another symbol.
 - (d) _____ The common name for the partial order among security levels in a hierarchical access control system such as Bell and LaPadula.
 - (e) _____ An information transmission medium that utilizes system resources that were not designed to transmit information.
 - (f) _____ The aspect of security concerning who can alter or modify stored information.
 - (g) _____ Security policy that says that an agent cannot access information for a client if he has previously served a client in the same general class.
 - (h) _____ The property that says that the levels of subjects and/or objects cannot vary in ways that violate the system security property.
 - (i) _____ Unit used to measure the entropy of a language.
 - (j) _____ Describes any cryptographic system that uses the same key for encryption and decryption.

5. (10 points) Declassification (lowering the security level of an object) effectively violates the *-property of Bell and LaPadula because the information in that object flows from high to low.
 - (a) Would *raising* the level violate either of the BLP properties? Why or why not?
 - (b) Would raising the integrity level of an object violate any principles of Biba's Strict Integrity model? Explain your answer.

6. (10 points) Suppose you work for a company with a Chinese Wall security policy with clients in the following conflict classes:
- { Cadbury, Nestle }
 - { Ford, Chrysler, GM }
 - { Citicorp, Credit Lyonnais, Deutsche Bank }
 - { Microsoft }

You have previously worked on cases for Nestle and Citicorp, and you are ready for a new assignment.

List any of your company's clients for whom you *are* able to work as your next assignment. Assume you can work for a client for whom you have previously worked.

7. (10 points) Assume you have a distributed system with n hosts and you wish to implement secure pairwise encrypted communication, i.e., from any host to any other. How many keys are needed if you have symmetric (secret-key) encryption? How many if you have asymmetric (public-key) encryption?

8. (10 points) Discuss the following question: If **Unclassified** is the lowest hierarchical security level in a Bell and LaPadula system, is it meaningful to have need-to-know compartments at this level? For example, would it make sense to have a confidentiality label of (**Unclassified**, { **Crypto** })? Why or why not?