CS 361 Midterm
Sample Questions
Instructor: Dr. Bill Young

Name: _____

Read all questions carefully. 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, but this sample is longer than an hour test. Also, some of these questions turned out to be not great, so I probably wouldn't ask them again. Treat this sample as an idea of the range of questions that might be asked. But please don't obsess about these specific questions.*

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			

Be able to do a similar problem for Biba's Strict Integrity model and for both parts of Lipner's Model.

Think what an analogous table might look like for Biba's Ring Policy or Low Water Mark Policy.

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.) *You might also be asked to show an encoding that is better than the naive encoding and prove that it is better.*

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 $L(s) \geq L(o)$, the subject obtains the current value of the object; otherwise, do nothing.

   (WRITE s o v): if the subject and object exist and $L(s) \leq L(o)$, 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.

   Describe a covert channel in this system *using only these operations.* That is, show a sequence of instructions that could be used to signal a 0 from H to L, and a separate sequence of instructions to signal a 1. Each element of the sequence should be of the form: `L: instruction` or `H: instruction`. If some initial set-up is required or you assume the prior existence or non-existence of some objects, say so. Your solution must be repeatable. *Finally, state clearly what difference L sees in the two cases.*

   Assumptions? _____

H sends 0	**H sends 1**
L sees what difference?	

You might also be asked to display the row in the shared resource matrix appropriate for this system that reflects 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 resouces 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 "conflict" class.

(h) _____ The property that says that the levels of subjects and/or objects can vary, but only in ways that don't violate the system security properties.

(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. (5 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 not* able to work as your next assignment. Assume you *can* work for a client for whom you have previously worked.

7. (5 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? *This question is about material from Week 8 (so not covered on the test).*

8. (10 points) Steve Lipner uses the access control rules of Bell and LaPadula and of Biba's Strict Integrity policy to model a commercial security environment. The following is a simplified version of Lipner's model.

   Confidentiality labels are generated in terms of the hierarchical levels (from high to low): **AM** and **SL**. In addition there are five need-to-know categories: **D**, **PC**, **PD**, **SD**, **T**.

   Integrity labels are defined in terms of the hierarchical levels (from high to low): **ISP**, **IO**, **ISL**. There are two integrity need-to-know categories: **ID**, **IP**.

   Finally, users/objects are given labels according to their role/type:

User Role	**Confidentiality**	**Integrity**
Ordinary users	$(SL, \{PC, PD\})$	$(ISL, \{IP\})$
System programmers	$(SL, \{SD, T\})$	$(ISL, \{ID\})$
System controllers	$(SL, \{D, PC, PD, SD, T\})$	$(ISL, \{IP, ID\})$

Object type	**Confidentiality**	**Integrity**
Production code	$(SL, \{PC\})$	$(IO, \{IP\})$
Software tools	$(SL, \{T\})$	$(IO, \{ID\})$
System programs	$(SL, \emptyset)$	$(ISP, \{IP, ID\})$

   Assuming the following users/objects have the associated roles/types, fill in the table below with the R and/or W permissions that the system would allow.

Name	**Role or Type**
User1	Ordinary user
User2	System programmer
User3	System controller
Obj1	Production code
Obj2	Software tool
Obj3	System program

	Obj1	**Obj2**	**Obj3**
User1			
User2			
User3			

9. (5 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?

10. (5 points) Labels in the Bell and Lapadula model are of the form (L, C), where L is from a totally ordered set and C is a set of need-to-know categories. You could map this onto a set of labels just containing categories where dominates becomes set membership, though you might have to add some new categories. First, illustrate how this would work in a system that has hierarchical levels $\{l, h\}$ and categories $\{A, B\}$ by showing how to map a label in the old system to a label in the new system that accomplishes "the same thing." Then explain *in general* how you could take an arbitrary BLP policy and implement the same policy replacing (L, C) by C'. I.e., $dom\,(x, y)$ in the old system iff $dom\,(x', y')$ in the new system.