CS 361 Sample Final
Instructor: Dr. Bill Young

Name: ____

All of the questions on this sample test came from finals in previous semesters. Some of the questions on this sample may cover matters we didn't cover this semester. Also, your final likely will have few to none "essay" type questions; expect more multiple choice and short answer questions.

Finally, to save space, I didn't leave room on this test to answer the questions. Your actual final will have room to answer on the test paper.

1. (Short answer) 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) ______________________ *Haven't covered.* Names a program that, in addition to a useful effect, has a second, nonobvious malicious effect.

   (b) ______________________ Transmitted with a document, this "cryptographically seals" the document to ensure that it has not been altered.

   (c) ______________________ Artifact generated by one party to "vouch for" the identity or trustworthiness of another.

   (d) ______________________ *Haven't covered.* Describes a malicious program that attaches itself to another program, runs when that program executes, and terminates when that program terminates.

   (e) ______________________ Describes the attempt to extract the meaning of encrypted messages without knowledge of the key.

   (f) ______________________ Term for any cryptographic system that encodes by reordering of symbols in the plaintext.

   (g) ______________________ The major problem greatly reduced by the invention of public-key cryptosystems.

   (h) ______________________ Names a random number included within a message to show that the message is "fresh," i.e., is not being replayed from an earlier exchange.

   (i) ______________________ An encryption algorithm that uses a long series of numbers as a key, usually a pseudorandom sequence. Used on computers as a good approximation to a one-time pad.

   (j) ______________________ Security attack that attempts to limit the availability of resources.

(k) ________________________ *Haven't covered.* According to the IEEE, the name for an incorrect step or command in a program that may lead to a failure.

(l) ________________________ Methodology due to Richard Kemmerer for finding covert channels in a system.

(m) ________________________ General concern in commercial security that often outweighs confidentiality.

(n) ________________________ Policy due to Biba that is the dual of Bell and LaPadula security.

(o) ________________________ List that stores with an object the names and permissions of any subjects currently permitted access to that object.

(p) ________________________ General name for interference in a communication channel that may cause a message to be corrupted or distorted.

(q) ________________________ Theoretically unbreakable cryptographic algorithm that uses a key as long as the plaintext.

(r) ________________________ General name for any encryption algorithm that encodes a text in large "chunks" rather than on a symbol-by-symbol basis.

(s) ________________________ Commercial symmetric encryption algorithm designed as a successor to DES.

(t) ________________________ International standard for the evaluation of secure computer systems.

2. Assume you have a public key cryptosystem in which K_x is X's public key, and K_x^{-1} is the corresponding private key. Consider the following simple protocol:

   1. $A \rightarrow B : \{\{M\}_{K_a^{-1}}\}_{K_b}$
   2. $B \rightarrow A : \{\{M\}_{K_b^{-1}}\}_{K_a}$

   The goal is for A to share with B a secret message M, such that each party is authenticated to the other.

   (a) List what B is supposed to believe at the end of step 1. Justify each point.

   (b) List what A is supposed to believe at the end of step 2. Justify each point.

   (c) This protocol is not secure. An attacker H might learn the secret M as follows. Assume that H listens in and obtains from step 1 the message $\{\{M\}_{K_a^{-1}}\}_{K_b}$ that A sent to B. By initiating a new run of the protocol with B and using this message as if it were a new secret M, it is possible for H to discover the original secret. Provide a rigorous argument for this claim.

   (d) Can you suggest a change to the protocol that would defeat this attack.

3. Suppose you have a secure system with exactly the four subjects given below, with security levels as listed:

Type	**Name**	**Level**
Subject	S_1	$(H, \{A, B\})$
Subject	S_2	$(L, \emptyset)$
Subject	S_3	$(H, \{A, B, C\})$
Subject	S_4	$(L, \{B, C\})$

   Here H dominates L. The goal is to enforce Bell and LaPadula-style security for this system, and prohibit information from flowing "down" in the system. You decide to use a noninterference model.

   Using the notation $S_i \mapsto S_j$ to indicate that S_i *may interfere with* S_j, list all interferences allowed in the system (except the reflexive interferences of the form $S_k \mapsto S_k$). That is, what is the noninterference policy of the system?

4. (2 parts) Suppose you have an unbalanced coin that is twice as likely to yield a head as to yield a tail.

   (a) What is the entropy of this language? Give the appropriate instance of the formula rather than a numeric answer.

   (b) The entropy of this language is less than 1, suggesting that you can actually represent the outcome of a series of n flips of this coin in less than n bits. One way to accomplish this is to encode *pairs* of flips rather than single flips. The following is one such encoding: encode HH as 0; encode HT as 10; encode TH as 110; encode TT as 111. Argue rigorously that this encoding is better on average than using one bit per flip. (Hint: consider on average how many bits it takes to encode 18 flips of this coin.)

5. Imagine that you are designing a policy for *multi-level survivability*. Each subject relies on services or information from other subjects, possibly provided via the objects of the system. But you don't want to be disabled by the failure of a less reliable/survivable subject. Assume you can attach "survivability" labels to the subjects (and possibly objects) in the network. Describe briefly an abstract survivability policy (modeled on one of the security policies we've described this semester).

6. A system provides protection using the Bell and LaPadula policy. A virus writer finds a way to introduce a virus into the system at an arbitrary level. The goal is to propagate as widely as possible by infecting other objects on the system. Should the virus be introduced into an object at system-low (the level that all other levels dominate) or at system-high (the level that dominates all other levels)? Explain.

7. The notation we introduced for cryptographic protocols is very expressive. We used

   $$A \to B : M$$

   to mean that A sends message M to B. Along with our notation for describing encryption of message M with key K, $\{M\}_K$, we can succinctly describe almost any cryptographic protocol. Using this notation, what is the message exchange that occurs when PGP is used by A to send to B a message M in a confidential manner (encrypted). Assume any keys you need, but explain what they are. Don't worry about authentication, compression or segmentation.

8. Describe an algorithm that generates an access control matrix for any given history H of the Chinese Wall model. That is, you have a collection of companies $C_1, C_2, \ldots, C_j$, the conflict classes to which they belong, and a history of accesses by subjects $S_1, S_2, \ldots, S_k$ to those companies' files. Describe how you would generate an access control matrix for the current state of the system.

9. A public key system can be used to ensure *nonrepudiation of origin*; that is, the sender cannot claim that she did not send the message because it is encrypted with a key that only she knows. Assume instead that we have a *symmetric* cryptosystem in which Alice and Bob share key K_{ab} which they use for secure communication. Bob claims that message M must have come from Alice and to prove it, displays both the message and its encryption $\{M\}_{K_{ab}}$. It must have come from Alice, he claims, since only Alice could have encrypted it with their shared key. Is his argument convincing? Explain.

10. How well does the DES encryption algorithm perform as far as introducing confusion and diffusion into the ciphertext? Explain.

    That semester they had coded DES. I'd ask you about AES, if I asked this question again.

11. A one-time pad is a random bit string K of the same length as the plaintext that is Xor'd with the plaintext to yield the ciphertext, as follows: $M_i \oplus K = C_i$. If used cautiously, this is theoretically unbreakable. However, suppose you carelessly use the same key K to encrypt two plaintexts M_1 and M_2. An attacker with access to the ciphertexts C_1 and C_2 can establish a (possibly useful) relationship between the plaintexts that does not involve K. Explain.

12. (2 parts: 10 points total) If E_K is a symmetric block encryption algorithm with key K, then the Cipher Block Chaining encryption mode can be characterized by the following equations:

$$C_0 = IV$$

$$C_i = E_K(P_i \oplus C_{i-1}),$$

    where C_i is the ith ciphertext block, IV is an *initialization vector* to get the process started, and $\oplus$ is exclusive or. The IV is just a random string transmitted as the zeroth block C_0 of the ciphertext. There is no P_0.

    (a) (5 points) Exhibit the corresponding decryption algorithm D_K. To encrypt plaintext block P_i requires encrypting all earlier blocks. Explain why *decrypting* a ciphertext block does not depend on decrypting any other blocks.

    (b) (5 points) One website claims that: "CBC might seem to provide message integrity, but one can snip the first few blocks from a message encrypted in that mode without any garbled text being visible in the plaintext." Is this true or false? Explain.