Homework 2

Due: October 23, 2019 at 11:59pm **Points:** 130

Questions

Remember to justify your answers.

1. (*20 points*) Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.
   (a) Paul, cleared for (TOP SECRET, { A, C }), wants to access a document classified (SECRET, { B, C }).
   (b) Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, { B }).
   (c) Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }).
   (d) Sammi, cleared for (TOP SECRET, { A, C }), wants to access a document classified (CONFIDENTIAL, { A }).
   (e) Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, { B }).

2. (*20 points*) Prove the following theorem: If there is an information transfer path from object $o_1 \in O$ to object $o_{n+1} \in O$, then enforcement of the strict integrity policy requires that $i(o_{n+1}) \leq i(o_1)$ for all $n > 1$.

3. (*20 points*) Using the statistical method in Section 10.2.2, decipher the following ciphertext, which was enciphered using the Caesar cipher:

   `TEBKFKQEBZLROPBLCERJXKBSBKQP`

4. (*20 points*) Consider the public keys (e_1, n_1) and (e_2, n_2) of two RSA cryptosystems.
   (a) You have discovered that n_1 and n_2 have a common factor but do not know what it is. How would you find it?
   (b) You have intercepted a message c enciphered using the first public key. You also know the common factor of n_1 and n_2. Show how to decrypt c.

5. (*20 points*) A cryptographic checksumn that computes 64 bit hashes has a probability of 0.5 that at least one collision will occur given 2^{32} messages. Alice wants to take advantage of this to swindle Bob. She and Bob agree to use such a cryptographic checksum. She draws up two contracts, one that Bob has agreed to sign and the other that Bob would not sign. She needs to generate a version of each that has the same checksum. Suggest how she might do this.
   Hint: Adding blank spaces, or inserting a character followed by a backspace, will not affect the meaning of either contract.

6. (*30 points*) The story "Computers Don't Argue" by Gordon R. Dickson is set in a society that relies on computerized records. It asks what happens when a record is incorrect.
   (a) The story starts with the book club mailing Mr. Childs a defective copy of Rudyard Kipling's "Kim", which he returned, and then sent him a copy of Robert Louis Stevenson's "Kidnapped", which he also returned. Identify 3 other places where human errors exacerbated the events that occurred to Mr. Childs.
   (b) What is the central flaw of the computerized system described in the story?

Extra Credit

E1. (*30 points*) Prove that the two properties of the hierarchy function (see Section 5.2.3) allow only trees and single nodes as organizations of objects.