Homework #3 Revision 1

Revision 1 has the new due date, changed from May 7.

Due: May 10, 2021 **Points:** 100

Questions

1. (*16 points*) Classify each of the following as an example of a mandatory, discretionary, or originator controlled policy, or a combination thereof. Justify your answers.
   (a) The file access control mechanisms of the UNIX operating system
   (b) A system in which no memorandum can be distributed without the creator's consent
   (c) A military facility in which only generals can enter a particular room
   (d) A university registrar's office, in which a faculty member can see the grades of a particular student provided that the student has given written permission for the faculty member to see them.

2. (*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}).

3. (*20 points*) In the Clark-Wilson model, must the TPs be executed serially, or can they be executed in parallel? If the former, why; if the latter, what constraints must be placed on their execution?

4. (*24 points*) An affine cipher has the form $c = (am + b) \bmod n$. Suppose m is an integer between 0 and 25, each integer representing a letter.
   (a) Let $n = 26$, $a = 3$, and $b = 123$. What is the ciphertext corresponding to the phrase `THIS IS A CIPHER MESSAGE`.
   (b) A requirement for a cipher is that every plaintext letter correspond to a different ciphertext letter. If a and b are not relatively prime to n, does the affine cipher meet this property? Either prove it does or present a counterexample.

5. (*20 points*) In the story " 'Repent, Harlequin!' said the Ticktockman" by Harlan Ellison, the Harlequin repeatedly disrupts schedules.
   (a) An "insider threat" is usually defined as someone who is trusted with access or information betraying that trust. It may be deliberate, the attacker knowing they are attacking; it may be unintentional, the attacker unaware of the effect of their actions. This story has a classic example of an unintentional insider attack. What is it? What might the consequences be? How does this relate to computer security?
   (b) Ellison uses an unusual style of writing in this story, in which he begins in the middle, then goes to the beginning, and then to the end. Further, the story has a manic quality due to the choice of words and its structure. How is this similar to handling a computer intrusion incident?