Homework #4

Due: May 24, 2021 **Points:** 100

Questions

1. (*16 points*) Consider the RSA cipher with $p = 5$ and $q = 7$. Show that $d = e$ for all choices of public key $(e, 35)$ and private key d.

2. (*20 points*) Reconsider the case of Alice and her stockbroker, Bob, in the example in section 10.1. Suppose they decide not to use a session key. Instead, Alice pads the message (BUY or SELL) with random data. Explain under what conditions this approach would be effective. Discuss how the length of the block affects your answer.

3. (*20 points*) Why should a time-based authentication system invalidate the current password on a successful authentication?

4. (*20 points*) Suppose a user wishes to edit the file *xyzzy* in a capability-based system. How can he be sure that the editor cannot access any other file? Could this be done in an ACL-based system? If so, how? If not, why not?

5. (*24 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 2 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?