Homework 3

Due: May 13, 2013 at 11:55pm **Points:** 100

Questions

1. (*20 points*) Consider the Bell-LaPadula model. 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, or both) 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}).

   (*text* §5.8, exercise 2).

2. (*20 points*) For the Biba model, suppose a system uses the same labels for integrity levels and categories as for subject levels and categories. Under what conditions could one subject read an object? Write to an object? (*text* §6.8, exercise 3).

3. (*15 points*) A cryptographer once stated that cryptography could provide complete security, and that any other computer security controls were unnecessary. Why is he wrong? (*Hint:* Think of an implementation of a cryptosystem, and ask what aspect(s) of the implementation can cryptography not protect.)
   (*text* §9.8, exercise 1)

4. (*15 points*) Let k be the encipherment key for a Caesar cipher. The decipherment key differs; it is $26 - k$. One of the characteristics of a public key system is that the encipherment and decipherment keys are different. Why then is the Caesar cipher a classical cryptosystem, not a public key cryptosystem? Be specific.
   (*text* §9.8, exercise 6)

5. (*30 points*) The following message was enciphered with a Vigenère cipher. Find the key and decipher it.

   ```
   TSMVM MPPCW CZUGX HPECP RFAUE IOBQW PPIMS FXIPC TSQPK SZNUL
   OPACR DDPKT SLVFW ELTKR GHIZS FNIDF ARMUE NOSKR GDIPH WSGVL
   EDMCM SMWKP IYOJS TLVFA HPBJI RAQIW HLDGA IYOUX
   ```

   (*text* §9.8, exercise 8)

Extra Credit

1. (*20 points*) Consider the RSA cryptosystem. Show that the ciphertexts corresponding to the messages 0, 1 and $n - 1$ are the messages themselves. Are there other messages that produce the same ciphertext as plaintext?
   (*text* §9.8, exercise 13).