Homework 1

Due: October 9, 2024 **Points:** 100

1. (*15 points*) Argue for or against the following proposition. Ciphers that the government cannot cryptanalyze should be outlawed. How would your argument change if such ciphers could be used provided that the users registered the keys with the government?

2. (*20 points*) A computer security expert has said that without integrity, no system can provide confidentiality.

   (a) Assume the system provides no integrity controls. Do you agree with the noted computer security expert? Justify your answer.

   (b) Now suppose the system has no confidentiality controls. Can this system provide integrity without confidentiality? Again, justify your answer.

3. (*15 points*) A system has two processes, p_1 and p_2. The system has two files, f_1 (owned by p_1) and f_2 (owned by p_2). The rights on the system are r (read), w (write), x (execute), and o (own). The distinguished right o allows the owner to change the owned object's column in the access matrix. Without an o right, a subject may not make those changes. Initially, each process can read and write the file that it owns.

   (a) Please show the access control matrix for this system.

   (b) p_1 wants to give permission to p_2 to write f_2. Can p_1 do this? If so, please explain why and draw the access control matrix that results from p_1 doing so. If not, please explain why not.

   (c) p_1 wants to give p_2 permission to execute f_1. Can p_1 do this? If so, please explain why and draw the access control matrix that results from p_1 doing so. If not, please explain why not. (If the previous part made any changes to the access control matrix, ignore them; use the access control matrix in the first part of the problem as representing the current protection state of the system.)

4. (*30 points*) A system has 2 subjects, s_1, s_2, and 4 objects o_1, o_2, o_3, and o_4. Assume that discretionary access controls allow anyone access.

   (a) Using the *minimum* number of security levels, assign security levels to both subjects and objects according to the Bell-LaPadula model, such that the following conditions hold:
   s_1 can write only into o_3 and o_4.
   s_2 can write only into o_3.
   Hint: Don't forget to include o_1 and o_2 in your answer.

   (b) Determine which objects can be read by which subjects under the assignment of part a.

   (c) Modify the assignment of part a so that s_1 cannot read o_4. (That is, all the conditions of part a hold, and in addition s_1 cannot read o_4.)

5. (*20 points*) Given the integrity levels HIGHEST, HIGH, MEDIUM, LOW, and LOWEST (ordered from highest to lowest) and the categories X, Y, and Z, specify what type of access (read, write, both, or neither) is allowed by the Biba model in each of the following situations. Assume that discretionary access controls allow anyone access.

   (a) A process cleared for (HIGHEST, { X, Y }) wants to access a document classified (LOW, { Y }).

   (b) A process cleared for (LOWEST, { X }) wants to access a document classified (LOWEST, { Y }).

   (c) A process cleared for (MEDIUM, { Y, Z }) wants to access a document classified (MEDIUM, { X, Y, Z }).

   (d) A process cleared for (LOW, { Z }) wants to access a document classified (LOW, { Z }).

   (e) A process cleared for (HIGH, { X, Z }) wants to access a document classified (HIGHEST, { Y, Z }).