HW 4

Question 1:

**Read Rights:** A subject of type \( st_i \) can only give the read rights that it has over an object of type \( ot_i \) to another subject \( st_j \) if and only if \( st_i = st_j \).

For \( i, j = 1, 2, 3 \) and \( i = j \) define

\[
\text{link}_{ij}(st_i, st_j) = \text{true} \\
\text{filter}_{ij}(st_i, st_j) = \{ ot_i/r \}
\]

**Write Rights:** A subject of type \( st_i \) can only give the write rights that it has over an object of type \( ot_i \) to another subject \( st_j \) such that \( st_j = st_i \).

For \( i, j = 1, 2, 3 \) and \( j = i \) define

\[
\text{link}_{ij}(st_i, st_j) = \text{true} \\
\text{filter}_{ij}(st_i, st_j) = \{ ot_i/w \}
\]

**Create:** A subject of type \( st_i \) can only create an object of type \( ot_i \).

\[
RI = \{ r:c, w:c \}, \quad RC = \emptyset.
\]

For \( i = 1, 2, 3 \)

\[
\text{cc}(st_i) = \{ ot_i \} \\
\text{cr}(st_i, ot_i) = \{ ot_i/r:c, ot_i/w:c \}
\]

Question 2 (4.11.5)

a. discretionary  

b. originator  

c. mandatory  

d. discretionary + mandatory

Question 3: Read pages 96-97

HW5

Question 1

(4.11.3) Everyone seemed to agree!

(4.11.6)

\[
\text{deny ( \{ ? Messages.deposit(pi, msg) \} when (Message.willaccept(pi) == 0) )}
\]
Question 2

5.8.1 (Sample: Christi Novak)
Compartmenta are added to security classifications to describe a kind of information. They arise from the “need to know” principle, which states that no subject should be able to read objects unless reading them is necessary for the subject to perform its functions. Individuals only “need to know” certain topics of information. As a result, they are cleared to read only the compartments that they “need to know”. It would be meaningless to have these compartments at the unclassified level because information at the unclassified level is not confidential data (or is supposed to be publicly available). It is not restricted at all. Therefore, setting up compartments would be completely unnecessary.

5.8.2
a. cannot read or write
b. cannot read or write
c. can read only
d. can read only
e. can write only

5.8.4 (Sample from: ??)
The DG/UX system prevents any write downs but allows read downs. So subjects in the user region cannot write and modify, but can read/execute the Virus Prevention region. The VP region contains system programs or trusted executables. This setup ensures that users’ activities do not result in the propagation of the viruses to the system programs as it would involve altering the programs. However, as users can read objects of this region, they can still execute the trusted system programs.

5.8.5 (Sample from: ??)
The DG/UX contains auditing and management files in the Admin region. Since these files should not be read or written by subjects apart from those belonging (or having clearance) to this region, and no read up or write up is allowed in this system, the User region is placed below the Admin region to ensure that the confidentiality and integrity of the data such as logs, MAC label definitions, etc. are not violated by access by general users.