CS4600 Homework 1

1. Security mechanisms other than cryptography is not unnecessary. It can't provide any desired level of confidentiality because, even though data and resources can be hidden, the case of information leakage via an insider can cause massive damage if cryptography was the only security mechanism.
As it is the same case for integrity, cryptography alone is riskier than having more layers of security because no perfect security exist. We can get close but perfect security is unlikely. Redundancy and layering must exist so that when one mechanism fail, the remaining mechanisms will still provide some degree of protection versus having no protection at all if cryptography alone is implemented as a security mechanism. Therefore, I refute the cryptographer's claim.

2. For this Access Control Matrix, ownership comes with the capability to read, write, and execute (rwx).

|  |  | Objects | | | | | |
|---|---|---|---|---|---|---|---|
|  |  | Alice | Bob | Cyndy | alicerc | bobrc | cyndyrc |
|  | Alice | Cntrl | --- | --- | rwx | r-- | --- |
| Subjects | Bob | --- | Cntrl | --- | r-- | rwx | --- |
|  | Cyndy | --- | --- | Cntrl | r-- | rw- | rwx |

   a. The original ACM is defined as shown above

|  |  | Objects | | | | | |
|---|---|---|---|---|---|---|---|
|  |  | Alice | Bob | Cyndy | alicerc | bobrc | cyndyrc |
|  | Alice | Cntrl | --- | --- | rwx | r-- | r-- |
| Subjects | Bob | --- | Cntrl | --- | --- | rwx | --- |
|  | Cyndy | --- | --- | Cntrl | r-- | rw- | rwx |

   b. The modified ACM is defined as shown above

3. The analysis is presented below
   a. Paul can't read or write the document because it would violate no write-down rule and Paul isn't cleared for category B
   b. Anna can't read or write the document because Alice isn't cleared for category B
   c. Jesse can read but can't write the document because no write-down rule since Jesse's clearance level dominate object's permission level
   d. Sammi can read but can't write the document because no write-down rule since Sammi's clearance level dominate object's permission level
   e. Robin can't read but can write the document because the object's permission level dominates Robin's clearance level, and it would violate no read-up rule