Homework #2

Due: February 7, 2023 **Points:** 100

Questions

1. (*15 points*) A cryptographer once claimed that security mechanisms other than cryptography were unnecessary because cryptography could provide any desired level of confidentiality and integrity. Ignoring availability, either justify or refute the cryptographer's claim.

2. (*30 points*) Paul needs to read and write some documents. In the following, assume the system security policy is described completely by the Bell-LaPadula model. Note that the situation described may be impossible, in which case say so and show why.

   (a) Please give the *least* clearance that Paul can have if he wishes to read a document with classification (SECRET, {NUC,EUR}) and a document with classification (CONFIDENTIAL, {ASI}).

   (b) Please give the *greatest* clearance that Paul can have if he wishes to write to a document with classification (TOP SECRET, {EUR}) and a document with classification (SECRET, {EUR,NUC}).

   (c) Please give the *greatest* clearance that Paul must have if he wishes to read a document with classification (SECRET, {EUR,NUC}), to write a document with classification (CONFIDENTIAL, {NUC,EUR}), and to read another document with classification (TOP SECRET, {ASIA, EUR}).

3. (*30 points*) In class I said that the two properties of the hierarchy function (see Section 5.2.3) allow only trees and single nodes as organizations of objects. Prove this formally.

4. (*15 points*) Suppose a system used 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? Remember to justify your answer.

5. (*10 points*) In the Brewer-Nash (Chinese Wall) model, why must sanitized objects be in a single company dataset in their own conflict of interest class, and not in the company dataset corresponding to the institution producing the sanitized object?