**1. Digital Authentication**

In our textbook, ***Access Control, Security, and Trust, A Logical Approach***, Example 6.1 is on page 118. Using this example derive the rule associated with this example and complete a proof of this rule using the methods you have learned in CIS634, e.g. ML, HOL, etc. Report your work, the rule and its proof, as usual in a complete folder of required files…

(HINT: Asymmetric-Key Cryptography, or public-key cryptography, begins with Section 15.5, page 233, in our pdf textbook, ***Certified Security by Design Using Higher Order Logic***.)

**2. Delegation**

In our textbook, ***Access Control, Security, and Trust, A Logical Approach***, an extended example is included as Section 7.3 that begins on page 141 and ends with the associated derived rule on page 144. Generate the proof of this rule and report your work as usual in a complete folder of required files…

(HINT: Delegation is included as part of the discussion of conops in our pdf textbook, ***Certified Security by Design Using Higher Order Logic***, e.g. beginning at the bottom of page 184.)

**3. Access Control**

There are many types of access control; e.g. role-based access control, rule-based access control, discretionary access control, etc., which are described by a number of entities. For example, Techotopia at https://www.techotopia.com/index.php/Mandatory,_Discretionary,_Role_and_Rule_Based_Access_Control discusses different types of access control. Other entities use different types of access control and/or eliminate some types. The point is that there is no standard with regard to "types" of access control.

This question asks you to consider what you know about access control, particularly discretionary access control as we've discussed, and delegation. As you consider this you need to briefly state your opinion about whether or not delegation adds to the "decidability" of access control, and most importantly if delegation adds to the security of access control.

As usual, your report should include a complete folder and subfolders with all sections included in a LaTex final report. You should have the following:

1. Title page
2. Abstract
3. Acknowledgements
4. Table of Contents
5. Executive Summary
6. Chapter 1: Your submission to answer Question 1 of this exam
7. Chapter 2: Your submission to answer Question 2 of this exam
8. Chapter 3: Your submission to answer Question 3 of this exam
9. Appendices of source code – as required

Good luck!