Be sure to read the entire exam before you start. If you have any questions I'm available at mphamner@gmail.com

1. Suppose you are tasked with establishing an access-control system within which employees must use a secure relay to send communications. Basically an employee says to encrypt and send a message, i.e. "go". The secure relay actually encrypts and sends the message, i.e. "launch". Further suppose that our old friends Alice and Bob are in the roles of employee and secure relay respectively.
    a. First, generate a derived inference rule for this situation. Assume that Bob received a cryptographically signed message from Alice that he verifies from her key K_A. Having verified the cryptographically signed message, Bob performs the required encryption and sends the message.
    b. Second, complete a proof based on the derived inference rule.

2. Symmetric encryption

Megalomania is a multi-national corporation that designs, develops and sells online video games. Being a multi-national corporation means that Megalomania has offices in a number of countries including the United States, the United Kingdom, Japan, Australia, and Hong Kong. Brian and Susan are employees of Megalomania working out of the UK and Australia offices respectively. They are software engineers who work on game development and frequently need to send information to each other. Because the game development world is extremely competitive it is crucial to Megalomania's success that Brian's and Susan's correspondence is not read by Megalomania's competitors. Therefore, Brian and Susan use encryption to send and receive all communication. Brian and Susan know that symmetric encryption is not necessarily as secure as asymmetric encryption. So, they have also devised a scheme that changes their shared key each time they send a message. The key stays the same until either Brian or Susan sends their next message. At least in theory, anyone who does get Brian and Susan's shared key would have the last key but not the current key.

In the textbook Example 6.4 describes how two people could set-up a communication channel through a secure relay. Because of the way that Brian and Susan continuously change the symmetric key they do not want to proceed with the secure relay exactly as described in Example 6.4. However, Megalomania requires the use of a secure relay for all encrypted messages. This question explores how Brian and Susan can implement their scheme to protect a symmetric key while also maintaining a corporate policy regarding secure communications.

To start the process Susan must work with the relay to establish a secure channel for communication between herself and Brian. First, describe the steps the relay must take to accomplish this. Then, assume that Brian also wants to authenticate Susan. Describe the steps that must also be taken to accomplish this.

3. I have mentioned several times that HOL is not the only theorem prover, e.g. Isabelle is another theorem prover as is Coq. A relatively recent research area uses theorem provers in conjunction with artificial intelligence. I am providing you with a paper by Nawaz, et al titled "A Survey on Theorem Provers in Formal Methods. Based on your knowledge from CIS634 and this paper, what do you believe needs to be done to facilitate the use of theorem provers such as HOL in artificial intelligence?

As usual, use all the tools and resources you have available. 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!