CYENG 351 – SP 23: Embedded Secure Networking
Instructor: Dr. Shayan (Sean) Taheri
Gannon University (GU)

Assignment 4: Chapter 4 - The Secure Sockets Layer

Total Points: 100**; and Deadline:** March/22/2023, 11:59 PM.

Note – Cheating and Plagiarism: Cheating and plagiarism are not permitted in any form and they cause certain penalties. The instructor reserves the right to fail culprits.

Deliverable: All of your responses to the questions of assignment should be included in a single compressed file to be uploaded to the Gannon University (GU) – Blackboard Learn environment.

Question 1. Provide short answers (i.e., no more than five lines on average with the font size of 12) for the following items. The grade for each item is **10 points**.

1. Explain the usage of **Media Access Control** in a session of the **SSL Protocol**. State how the session can be attacked.
2. Mention the phases in the **SSL Handshake Process**, discuss each phase, and provide a figure for each phase that represents its computational steps.
3. Specify why the **SSL Protocol** is practically suitable for embedded networks.

Question 2. Complete the laboratory part, titled "**Wireshark Lab: DNS v8.1**". The grade for this question is **40 points**. Provide the screenshots for all of the major steps/processes in your experiments as well as the answers to the laboratory questions.

Question 3. Complete the laboratory part, titled "**EXPERIMENT #1: Introduction to Xilinx's FPGA Vivado HLx Software**" in the "**UCF-EEE3342LabManual.pdf**" file using your "**Nexys A7 FPGA Board**" to be received from the **GU – ECE Department**. The grade for this question is **30 points**. Provide a report that includes: (**A**) your overall understanding of the experiments; (**B**) the interesting points and the challenges that you faced in this laboratory; and (**C**) the screenshots for all of the major steps/processes in your experiments.