Date: Wednesday, October 16, 2002
Prof.: Dr Jean-Yves Chouinard

Design of Secure Computer Systems CSI4138/CEG4394

Assignment 2 (due Friday, October 25, before noon)

Question 1: *(Triple DES in CBC mode)*

Problem 4.1 from the textbook (Cryptography and Network Security: Principles and Practice, **second edition**, by William Stallings).

Question 2: *(Triple DES improvement)*

Problem 4.2 from the textbook.

Question 3: *(Centralized key distribution)*

Problem 5.3 from the textbook.

Problème 4: *(Pseudorandom sequence generator)*

Problem 5.5 from the textbook.