Date: Wednesday, September 18, 2002
Prof.: Dr Jean-Yves Chouinard

Design of Secure Computer Systems CSI4138/CEG4394

Assignment 1 (due Friday, September 27, before noon)

Question 1: *(one-time pad)*

Problem 2.2 from the textbook (Cryptography and Network Security: Principles and Practice, **second edition**, by William Stallings).

Question 2: *(cryptanalysis of a simple substitution cipher)*

Problem 2.4 from the textbook.

Question 3: *(Simplified DES)*

Problem 3.3 from the textbook.

Problème 4: *(Data Enryption Standard)*

Problem 3.7 from the textbook.