Date: Wednesday, November 20, 2002
Prof.: Dr Jean-Yves Chouinard

Design of Secure Computer Systems CSI4138/CEG4394

Assignment 4 (due Friday, November 29, before noon)

Problem 1: *(Authentication Protocols)*

Problem 10.2 from the textbook (Cryptography and Network Security: Principles and Practice, **second edition**, by William Stallings).

Problem 2: *(Digital Signature Standard (DSS))*

Problem 10.9 from the textbook.

Problem 3: *(Propagating Cipher Block Chaining (PCBC))*

Problem 11.2 from the textbook.

Problem 4: *(End-to-end Encryption and Authentication (IPSec))*

Problem 13.3 from the textbook.