Design of Secure Computer Systems CSI4138/CEG4394

Assignment 3 (due Friday, November 15, before noon)

Problem 1: *(Hash functions)*

Problem 8.5 from the textbook (Cryptography and Network Security: Principles and Practice, **second edition**, by William Stallings).

Problem 2: *(Comparison between MD4 and MD5)*

Problem 9.2 from the textbook.

Problem 3: *(SHA-1)*

Problem 9.3 from the textbook.