Homework 3
Introduction to Information Security (266-642)
Due Date: Nov 1, 2007 (Thursday)

Note: You can talk to your classmates, instructor, and TA about the problems. However, unless stated otherwise, problems should be written up individually. University of Wisconsin rules for academic misconduct apply.
In the homework, "the Stallings book" refers to [2] and "the Handbook" refers to [1] (I have linked the Handbook to the class homepage. You can download it for free.) Unless otherwise stated each part of a question has equal weight.

Question 1 (RSA) [20 points]: Suppose that there are two users on a network. Let their RSA moduli be n_1 and n_2, with n_1 not equal to n_2. If you are told that n_1 and n_2 are not relatively prime, how would you break their systems?

Question 1 (Hash Algorithms [50 points]):
Part A [25 points] : Problem 11.4 from the Stalling's book.
Part B [25 points]: Problem 11.6 from the Stalling's book.

Question 2 (Specific hash algorithms [30 points]) :
Part A [15 points] : Problem 12.2 from the Stallings book.
Part B [15 points] : Problem 12.3 from the Stallings book.

References

[1] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC press, 1997.

[2] William Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2006.