Homework 3
Introduction to Information Security (266-642)
Due Date: March 10, 2003 (Monday)

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 (Fermat's Little Theorem (FLT 10 points)): Problem 8.3 from the Stalling's book.

Question 2 (Chinese Remainder Theorem (CRT 20 points)):
Part A: Problem 8.11 from the Stalling's book.
Part B: Problem 8.12 from the Stalling's book.

Question 3 (RSA 50 points) :
Part A (15 points): Problem 9.4 from the Stallings book.
Part B (15 points): Problem 9.10 from the Stallings book.
Part C (20 points): Prove that RSA is insecure against a chosen plaintext attack. Specifically, given a ciphertext y, describe how to choose $\hat{y} \neq y$, such that knowledge of the plaintext $\hat{x} = D_K(\hat{y})$ allows $x = D_K(y)$ to be computed.
Hint: Use the multiplicative property of RSA, i.e., that

$$E_K(x_1)E_K(x_2) \mod n \ = \ E_K(x_1x_2 \mod n) \ .$$

Question 4 (El-Gamal and Diffie-Hellman 20 points):
Part A: Problem 10.1 from the Stallings book.
Part B: Assume that Alice sends a message m to Bob using El-Gamal. Remember that Oscar knows the public key and the ciphertext. Reason that if Oscar has an algorithm for finding out the plaintext m, then he can solve the Diffie-Hellman Problem (DHP).
Note: The converse of this statement was proved in class.

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, 2003.