Homework 4
Introduction to Information Security (266-642)
Due Date: April 25, 2005 (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 [Sta03] and "the Handbook" refers to [MOV97] (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 15 points)):
Part A: Problem 8.11 from the Stalling's book.
Part B: Problem 8.12 from the Stalling's book.

Question 3 (RSA 55 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 (10 points): Explain *low exponent attack* on RSA? This question is based on the following paper [KR95], which was handed out in class.
Part C (15 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.

Question 5 (Networking Basics [10 points]):
Part A: How do SYN-cookies protect a server from flooding attacks?
Part B: In a distributed-reflected denial-of-service attack, whose address is sent as the Source-IP of the SYN? Whose address is sent as the Source-IP of the SYN/ACK? Explain your answer. Use the following terminology:
M (Malicious Flood Generator)
R (Reflection Server (Innocent Bystander))
V (Victim of the Attack)

Question 6 (Hash Algorithms [70 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.
Part C [20 points]: Choose two random sets A and B of k persons. Let $P(k)$ be the probability that there is atleast one person in set A who shares a birthday with a person in set B. Give a formula for $P(k)$. Justify your answer. Plot $P(k)$ for $0 \leq k \leq 150$.

Question 7 (Specific hash algorithms [20 points]) :
Part A [15 points] : Problem 12.2 from the Stallings book.
Part B [5 points] : Problem 12.3 from the Stallings book.

References

[KR95] B. Kaliski and M. Robshaw. The secure use of rsa. *The Technical Newsletter of RSA Laboratories (Cryptobytes)*, 1(3):7–13, 1995.

[MOV97] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC press, 1997.

[Sta03] William Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2003.