Homework 4
Introduction to Information Security (266-642)
Due Date: March 25, 2003 (Tuesday)

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 (Networking Basics [10 points]):
Part A: How do SYN-cookies protect a server from spoofed IP addresses?
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 2 (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 3 (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

[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.