YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467a: Cryptography and Computer Security — *Handout #3*
Professor M. J. Fischer — *September 27, 2005*

Problem Set 2

Due in class on Tuesday, October 4, 2005.

In the problems below, "textbook" refers to *Introduction to Cryptography with Coding Theory: Second Edition* by Trappe and Washington..

Problem 7: Simplified CFB Mode

Textbook, problem 4.9.9.

Problem 8: DES Brute Force Speedup

Textbook, problem 4.9.11.

Problem 9: Birthday Paradox Calculation

Write a computer program to compute p_n, the probability that at least two people in a random collection of n people have the same birthday. Ignore leap years and assume the probability of a person's birthday falling on any given day is exactly $1/365$, independent of everyone else in the set. Your program should work for n in the range $[1, 365]$. Using your program, find the smallest value of n for which $p_n \geq 1/2$ and for which $p_n \geq 3/4$.

Problem 10: Simplified DES Implementation

Textbook, problem 4.10.1.