YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467a: Cryptography and Computer Security *Handout #3*
Professor M. J. Fischer *September 28, 2006*

Problem Set 2

Due on Thursday, October 5, 2006.

Work each of the following problems from the textbook, *Introduction to Cryptography with Coding Theory: Second Edition* by Trappe and Washington.. For each problem, show your work and justify your answer, whether or not the question specifically requests this.

Problem 2: Affine Cipher

Textbook, problem 2.13.4.

Problem 3: Vigenère Cipher

Textbook, problem 2.13.10.

Problem 4: Hill Cipher

Textbook, problem 2.13.15.

Problem 5: LFSR Machine

Textbook, problem 2.13.21.

Problem 6: Chaining Modes

For each of the standard chaining modes ECB, CBC, CFB, OFB, and PCBC, describe how to recover from the loss of a ciphertext block, and state explicitly how many message blocks become unrecoverable as a result of the loss.

Problem 7: Birthday Paradox Calculation

Write a computer program to compute p_m, the probability that two random subsets of size m drawn from a universe of size 100 have a non-empty intersection. Use your program to find the smallest values of m for which $p_m \geq 1/2$ and for which $p_m \geq 3/4$.

Problem 8: Meet-in-the-Middle Attack

Let E, D be the encryption and decryption functions for a symmetric cryptosystem with key space $\mathcal{K}$. Assume the plaintext and ciphertext spaces are the same. Let EE, DD be the encryption and decryption functions for the doubled verion as described in Lecture 5.

Eve is carrying out a known plaintex attack on the doubled system. Suppose she knows a pair (m, c) where $c = EE_{(k_1,k_2)}(m)$, but she does not know k_1 or k_2. She computes two sets:

$$X_m = \{E_k(m) \mid k \in \mathcal{K}\};$$

$$X_c = \{D_k(c) \mid k \in \mathcal{K}\}.$$

(a) Explain why $X_m \cap X_c \neq \emptyset$.

(b) How might these sets help her break the doubled system?

(c) Construct a symmetric cryptosystem and find a pair (m, c) for which $|X_m \cap X_c| \geq 2$, or show why that is not possible.