YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

CPSC 467b: Cryptography and Computer Security *Handout #2*
Professor M. J. Fischer *February 3, 2005*

Problem Set 1

Due in class on Thursday, February 10, 2005.

Problem 1: Cracking the Hill cipher

Suppose we are told that the plaintext

```
breathtaking
```

yields the ciphertext

```
RUPOTENTOIFV
```

where the Hill cipher is used, but the dimension m is not specified. Determine the encryption matrix. (See lecture notes, week 2, for details on the Hill cipher. Note that letters of the alphabet are encoded by the integers 0...25, and all arithmetic is performed modulo 26.)

Problem 2: Decrypting a substitution cipher

The file "ciphertext" in the `http://zoo.cs.yale.edu/classes/cs467/2005s/course/assignments/ps1/` subdirectory contains encrypted text using a substitution cipher. The set of valid characters is ASCII characters $32 \ldots 126$. Characters outside of this range (e.g., newline) are left unchanged. Decipher the message. Briefly describe the method that you used. (You will probably want to write some code to help you [1].)

Problem 3: Entropy, redundancy, and its use in enabling cryptanalysis

Textbook, exercise 3.11.
[Use the definition of redundancy given in the textbook rather than the slightly different version given in the notes.]

Problem 4: DES

Consider a DES-like scheme where

- block length is 8;
- $f_i(x)$ is $(i \cdot x)^K \bmod 16 \quad (i = 1, \ldots, 4)$;[2]
- number of rounds is 4;

Decrypt 10100101 using $K = 1101$.

[1] For your reference, the key generation program and the enciphering program are in perm_gen.cc and subciph.cc, resp.

[2] For the computation of $f_i(x)$ you should interpret the bit strings x and K as integers written in binary. The output of $f_i(x)$ is expressed in binary as well.