YALE UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

Problem Set 1

Due on Wednesday, January 18, 2012.

In the problems below, "textbook" refers to Wade Trapp and Lawrence C. Washington, *Introduction to Cryptography with Coding Theory, Second Edition*, Pearson, 2006.

Problems 5 and 6 are intended to be solved using the computer. The others should be doable with pencil and paper. However, you are free to make any use of computers that you wish for this problem set using any programming language that you are comfortable with. As with any problem set, show your work. That means if you wrote a program to help you solve the problem, then submit the code as well as your answers. The code will not be graded, but in case your answer differs from the correct one, it will help with the grading.

Please submit your solutions in electronic form, preferably as PDF files. They can be prepared using `pdflatex`, `MS Word`, or even scanned from *legible* handwritten notes. Be sure to include your name, date, and problem set number inside the file. It is also helpful if the file name contains your name in the same form as your course home directory on the Zoo.

You should submit your homework and any accompanying files using the `submit` script on the Zoo. If you don't have a Zoo account and a CPSC 467 course account, you will need to get them in order to submit your homework. The submit script will take multiple files but not directories, so if you want to submit a directory tree, then archive it first as a `.zip` or `.tar.gz` file and submit that file instead. For those of you who have not used the script before, the following Zoo command should do the trick:

```
/c/cs467/bin/submit 1 my.name_ps1_solutions.pdf
```

Please ask me or a TA if you have any questions. Also, I encourage you to make a trial submission in advance of the deadline just to make sure the submit script works for you.

Problem 1: Caesar Cipher [Textbook, p.55, problem 2.13-1]

Caesar wants to arrange a secret meeting with Marc Antony, either at the Tiber (the river) or at the Coliseum (the arena). He sends the ciphertext *EVIRE*. However, Antony does not know the key, so he tries all possibilities. Where will he meet Caesar? (*Hint:* This is a trick question.)

Problem 2: Affine Cipher [Textbook, p.55, problem 2.13-2]

The ciphertext *UCR* was encrypted using the affine function $9x + 2 \bmod 26$. Find the plaintext.

Problem 3: Hill Cipher [Textbook, p.57, problem 2.13-15]

Eve captures Bob's Hill cipher machine, which uses a 2-by-2 matrix $M \bmod 26$. She tries a chosen plaintext attack. She finds that the plaintext *ba* encrypts to *HC* and the plaintext *zz* encrypts to *GT*. What is the matrix M?

Problem 4: Multiple Ciphers [Textbook, p.58, problem 2.13-24]

Alice is sending a message to Bob using one of the following cryptosystems. In fact, Alice is bored and her plaintext consists of the letter *a* repeated a few hundred times. Eve knows what system is being used, but not the key, and intercepts the ciphertext. For systems (a), (b), and (c), state how Eve will recognize that the plaintext is one repeated letter and decide whether or not Eve can deduce the letter and the key. (*Note:* For system (c), the solution very much depends on the fact that the repeated letter is *a*, rather than *b, c,*....)

(a) Shift cipher
(b) Affine cipher
(c) Hill cipher (with a 2×2 matrix)

Problem 5: Shift Cipher [Textbook, p.59, problem 2.14-1]

The following ciphertext was encrypted by a shift cipher:

```
ycvejqwvhqtdtwvwu
```

Decrypt. (The ciphertext can be found in the file /c/cs467/assignments/ps1/ciphertexts.m on the Zoo under the name *ycve*.)

Problem 6: Vigenère Cipher [Extra credit] [Textbook, p.60, problem 2.14-60]

The following was encrypted by the Vigenère method using a key of length at most 6. Decrypt it and decide what is unusual about the plaintext. How did this affect the results?

```
hdsfgvmkoowafweetcmfthskucaqbilgjofmaqlgspvatvxqbiryscpcfrmvsw
rvnqlszdmgaoqsakmlupsqforvtwvdfcjzvgsoaoqsacjkbrsevbelvbksarls
cdcaarmnvrysywxqgvellcyluwwveoafgclazowafojdlhssfiksepsoywxafo
wlbfcsocylngqsyzxgjbmlvgrggokgfgmhlmejabsjvgmlnrvqzcrggcrghgeu
pcyfgtydycjkhqluhgxgzovqswpdvbwsffsenbxapasgazmyuhgsfhmftayjxm
wznrsofrsoaopgauaaarmftqsmahvqecev
```

(The ciphertext can be found in the file /c/cs467/assignments/ps1/ciphertexts.m on the Zoo under the name *hdsf*. The plaintext is from *Gadsby* by Ernest Vincent Wright.))