

Problem Set 1

Due on Wednesday, September 11, 2013

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

Problems 7 and 8 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 as described in Problem Set 0 (handout 3). Give “1” as the first argument to `submit` so that your submission goes into the right folder, e.g.,

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

Please ask me or the TA if you have any questions.

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 2.13-3]

Encrypt *howareyou* using the affine function $5x + 7 \bmod 26$. What is the decryption function? Check that it works.

Problem 3: Hill Cipher [Textbook, p.57, problem 2.13-16]

- (a) The ciphertext *ELNI* was encrypted by a Hill cipher with a 2-by-2 matrix. The plaintext is *dont*. Find the encryption matrix.
- (b) Suppose the ciphertext is *ELNK* and the plaintext is still *dont*. Find the encryption matrix. Note that the second column of the matrix changed. This shows that the entire second column of the encryption matrix is involved in obtaining the last character of the ciphertext. (See the end of Section 2.7).

Problem 4: Vigenère Cipher [Textbook, p.58, problem 2.13-25]

The operator of the Vigenère machine is bored and encrypts a plaintext consisting of the same letter of the alphabet repeated several hundred times. The key is a six-letter English word. Eve knows that the key is a word but does not yet know its length.

- (a) What property of the ciphertext will make Eve suspect that the plaintext is one repeated letter and will allow her to guess that the key length is six?
- (b) Once Eve recognizes that the plaintext is one repeated letter, how can she determine the key? (*Hint: You need the fact that no English word of length six is a shift of another English word.*)
- (c) Suppose Eve does not notice the property needed in part a, and therefore uses the method of displacing then counting matches for finding the length of the key. What will the number of matches be for various displacements? In other words, why will the length of the key become very obvious by this method?

Problem 5: Multiple Affine Ciphers [Textbook, p.55, problem 2.13-6]

Suppose you encrypt using an affine cipher, then encrypt the encryption using another affine cipher (both are working mod 26). Is there any advantage to doing this, rather than using a single affine cipher? Why or why not?

Problem 6: Types of Classical Ciphers

There are two main types of classical ciphers: *substitution* ciphers and *transposition* ciphers. For each type:

- (a) explain how in principle these ciphers work,
- (b) give two examples,
- (c) explain how, when given access to a ciphertext, you would recognize which type of cipher was used to encrypt it.

Problem 7: Shift Cipher

The following ciphertext was encrypted by a shift cipher:

hufvulmyvtaoltvzajsblslzzhthalbyavaolilzajyfwavnyhwolyjhujyl
halhuhsnvypaotaohaoloptzlsmjhuuvaaiylhriybjlzjouply

By performing a frequency count, guess the key used in the cipher. What is the decrypted plaintext? (The ciphertext can be found in the file /c/cs467/assignments/ps1/ciphertexts.m on the Zoo under the name *hufv*.)

Problem 8: Vigenère Cipher [Textbook, p.60, problem 2.14-8]

The following was encrypted by the Vigenère method. Find the plaintext.

ocwyikoooniwugpmxwktzdwgtssayjzwyemdlbnqaaavsuwdvbrflauplooubfgg
hgscmgzlatocdsdeidpbhtmuovpiekifpimfnoamvlpqfxejsmxmpgkccaykwf
zpyuavtelwhrmwkbvgtguftefjlodfefkvpxsgrsorgvtajbsauhzzalkwuow
hgedefnswmrciwcpaavogpdnfpktdbalsisurlnpsjyeatcuceesohdarkhwot
ikbroqrdfmzghgucebvgwcdqxpbgqwlpbdaylooqdmuhbdqgmyweuik

(The ciphertext can be found in the file /c/cs467/assignments/ps1/ciphertexts.m on the Zoo under the name *ocwy*. The plaintext is from *The Adventures of the Dancing Men* by Sir Arthur Conan Doyle.)