Homework Assignment 2

Due by 11:59 pm on Wednesday, September 13, 2017

Please submit your solutions in electronic form as you did for Homework Assignment 1. (See handout 2.)

Problem 1: Affine Cipher

Happy Hacker read about the affine cipher. He liked that it had a bigger key space than the Caesar cipher, but he thought it should be bigger still, so he invented the double affine cipher. Here's how it works.

- Pick two affine cipher key pairs $k_1 = (\alpha_1, \beta_1)$ and $k_2 = (\alpha_2, \beta_2)$. The Happy key is the pair (k_1, k_2).
- Encrypt a plaintext letter m as $E_{k_2}(E_{k_1}(m))$, where E_{k_i} is the affine encryption function with key pair k_i, for $i = 1, 2$.

(a) How large is Happy's key space?

(b) Suppose $k_1 = (5, 11)$ and $k_2 = (9, 4)$. What is Happy's encryption of the letter "`F`"? Show your work.

(c) Let c be a ciphertext letter. Describe how to decrypt c, and show why one recovers the original plaintext letter. Work through the decryption for the ciphertext you found in part (b).

(d) Smarty Sam told Happy that his scheme was no better than the original affine cipher because the substitution specified by Happy's double key $((\alpha_1, \beta_1), (\alpha_2, \beta_2))$ was the same as the affine substitution $E_{(\alpha,\beta)}$ specified by a single key pair (α, β). Happy couldn't understand how that can be. Help Happy by finding an affine key pair (α, β) that defines the same substitution as the one specified by Happy's double key $((5, 11), (9, 4))$. Show your work.

Problem 2: Playfair

Consider the Playfair cipher with passphrase

```
WE MUST STATE RELATIONSHIPS, NOT PROCEDURES - GRACE
HOPPER
```

(a) Construct the Playfair matrix.

(b) Decrypt the following letter pairs using the matrix from part (a):

```
RZ TI RY TP EA IC TR GV
```

(c) Do your best to recover the plaintext message described by the cyphertext pairs of part b.

Problem 3: Cryptanalysis

Read chapter 1 of the Paar and Pelzl textbook, *Understanding Cryptography*. Then solve problem 1.2 on book page 24. (The PDF page number may differ.) Be sure to explain your answers.

You are free to make any use of computers that you wish for this problem, using any programming language or tools 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. If you make use of somebody else's code, then be sure to properly acknowledge the source of that code.