

Exercise Set 1.**Due in Class on Monday, February 12****Write as if this were part of your resume for a high-paying job you really want!**

1. Consider two wheels, one inside the other. On the outer wheel are placed the letters A, B, ..., Z in cyclical clockwise order. On the inner wheel are placed the letters A, B, ..., Z in cyclical counter-clockwise order on a rotatable disk. By proper alignment, with one letter under another, we get a substitution cipher. Identify this substitution cipher for an arbitrary placement of the inner wheel, giving both the encryption function and decryption function in terms of the alignment chosen.

2. Decrypt the affine cipher with ciphertext:

HWZO DGABU UNOTJZOD BAN HJGN.

You must show your work.

3. A character is called a *fixed point* of a cipher with encryption function E_k provided $E_k(x) = x$. Consider affine ciphers based on the alphabet $A, B, C, \dots, Z$ ($0, 1, 2, \dots, 25$). Classify the keys for the affine ciphers according to the number of fixed points they have. Use this to compute the average number of fixed points of a random affine cipher (a cipher chosen from all the affine ciphers with each having an equal probability of being chosen). [Remark: Just for comparison purposes it can be shown that the average number of fixed points for a permutation chosen at random from all the permutations of $\{0, 1, 2, \dots, N - 1\}$ (e.g. $N = 26$) equals 1.]

4. The purpose of this exercise is to show how choosing familiar words as keys or passwords impacts security. Do the following:

(1) Write down off the top of your head your guess for the number of English words you know.

(2) Take a standard size dictionary and open it to a random page and count the number of words you know on that page and the number of words on that page. Multiply these numbers by the number of pages in the dictionary. Do this a total of at least ten times and average your results to get an estimate for the size of your vocabulary [compare with (1)] and the number of words in the dictionary.

What's your conclusion?

5. Consider a message $x_1x_2\cdots x_n$ of length n using the ordinary English alphabet including a space which we denote by $*$ ($*$, $A, B, \dots, Z$, i.e. $0, 1, 2, \dots, 26$ with $*$ being 0, A being 1, and so forth). We encrypt the message using a variation of the one-time pad:

Choose $k_1k_2\cdots k_n$ not at random but to be some meaningful message itself and use the following encryption:

$$E_k(x_i) = ((x_i + k_i)/2)\%27 \quad (i = 1, 2, \dots, n).$$

Now think of $k_1k_2\cdots k_n$ as the message and $x_1x_2\cdots x_n$ as the key and encrypt the message $k_1k_2\cdots k_n$ as follows:

$$E_x(k_i) = ((x_i - k_i)/2)\%27 \quad (i = 1, 2, \dots, n).$$

(1) Determine the decryption keys for E_k and E_x as affine ciphers on each character.

(2) Show that $E_k(x_i) + E_x(k_i) = x_i$ for all i and thus that $E_x(k_i)$ can be used to decrypt the first cipher.

(3) Similarly show that $E_k(x_i) - E_x(k_i) = k_i$ for all i and thus $E_k(x_i)$ can be used to decrypt the second cipher.

(4) Think of a scam in which this can be used!