Assignment 1

Due: 11:59pm June 7 (Sunday)

This assignment is done individually.

You can use **either C, C++, Java, or Python** to implement this assignment.

In this assignment, you will implement the monoalphabetic cipher (cs558-02.pdf) to encrypt/decrypt files containing only lower-case letters a-z. **The file contains only 1 line and does not contain spaces, tabs, and newlines.** You can assume that the file contains less than 10000 characters. For each plaintext letter, your program should randomly generate a ciphertext letter based on a seed. **The seed will be hardcoded in your program. The seed should be the same in encryption and decryption so that the same mapping (i.e. the same key) will be used in encryption and decryption.** Different plaintext letters should be mapped to different ciphertext letters. Different mappings will be generated with different seeds.

The program has three arguments: inputfile, outputfile, and 1/0

    - inputfile: input file name
    - outputfile: output file name
    - 1: encryption, 0: decryption

E.g. in C, an example command for executing your program is (assume that the name of your executable is mono):
    ./mono in out 1: encrypt file in and store the result in file out:
    ./mono out in1 0: decrypt file out and store the result in file in1

After the above two commands, files in and in1 should contain the same content.

Your program (both encryption and decryption) will print the mappings generated between the plaintext letters and the ciphertext letters. The mappings will be printed using the format a-c1, b-c2, …, z-c26, where ci is the corresponding cyphertext letter, and c1\=c2\=…\=c26. E.g.

a-b, b-d, e-h, ……

Submission guideline:

Please hand in your **source code** electronically through mycourses.binghamton.edu (**please do not submit .o or executable code**). Your code should compile and run correctly on bingsuns.binghamton.edu or remote.cs.binghamton.edu. If you do not have access to remote.cs, please let me know.

- Write a **README** file (**text file, do not submit a .doc file**) which contains
    - Your name and the email address
    - The programming language used
    - Whether your code was tested on bingsuns or remote.cs.
    - How to compile and execute your program.
    - (Optional) Anything special about your submission that you would like take note of.
- Place all your files under one directory with a unique name (such as p1-[userid] for assignment 1, e.g. p1-pyang).
- Tar the contents of this directory using the following command.
    tar –cvf [directory_name].tar [directory_name]
    E.g. tar -cvf p1-pyang.tar p1-pyang/
- Use mycourses to upload the tared file you created above.