CSC116
DISCUSSION 18

Gina Bai

LOGISTICS

- Project 4
  - Due Monday, July 12
- Extra Credit Opportunities
  - Growth Mindset #4
    - Due tonight, July 8th, at 11:45pm
  - Unit Testing Study
    - 2-hr lab session
    - Sign up by Tuesday via: https://ncsu.qualtrics.com/jfe/form/SV_cYiVI3CvGzloZIF

LAB 18

- Posted
- Postponed
  - Wednesday, July 14

- Catch up with the course materials!!!

Read the Software Requirements

A cipher is a way of encrypting a message to disguise it and keep it secret. The substitution cipher used in this project is a very simple means of encrypting a message in which each letter in the message is substituted with a different letter. The case of the letters as well as the white-space is preserved and nonalphabetic characters are unchanged. The encrypted message can then be decrypted by substituting the original letters for the substituted letters, thereby recovering the original message.

For example, using the following substitution letters for the original letters

Letter	Substitution
a	j
b	i
c	d
d	o
e	t
f	h
g	u
h	q
i	a
j	b
k	r

Original → aBc 0

Encrypted
→ a – j, B – I, c – d, 0 → jId 0

Decrypted
→ j – a, I – B, d – c, 0 → aBc 0

User Interface

Hint:
-e for encrypt
-d for decrypt
equals() for String comparison

For this project, you will write a program named **Cipher**.

The program will accept 4 arguments on the command line:

- the "flag" (option), `-e` or `-d`, which indicates whether to encrypt the file or decrypt the file
- the name of the input file
- the name of the output file, which will hold the encrypted/decrypted version of the input file
- the name of the cipher file, which will contain substitution letters for each letter of the alphabet in order from a to z

Examples

Here are some examples that use the file, RoadNotTaken.txt, which contains the poem, The Road Not Taken by Robert Frost, and the cipher file, cipher1.txt. The output file, EncryptedRoadNotTaken.txt, is created in the first example. The output file, DecryptedRoadNotTaken.txt, which is created in the second example, has exactly the same contents as the original file.

```
➤TERMINAL
$ java -cp bin Cipher -e test-files/RoadNotTaken.txt test-files/EncryptedRoadNotTaken.txt test-files/cipher1.txt
$ java -cp bin Cipher -d test-files/EncryptedRoadNotTaken.txt test-files/DecryptedRoadNotTaken.txt test-files/cipher1.txt
```

This can be verified by using the Unix diff command, as shown below. The lack of output after the command indicates that there are no differences between the files, i.e., the files have the same content.

```
➤TERMINAL
$ diff test-files/RoadNotTaken.txt test-files/DecryptedRoadNotTaken.txt
```

PROJECT 4

Read the Software Requirements

A cipher is a way of encrypting a message to disguise it and keep it secret. The substitution cipher used in this project is a very simple means of encrypting a message in which each letter in the message is substituted with a different letter. The case of the letters as well as the white-space is preserved and nonalphabetic characters are unchanged. The encrypted message can then be decrypted by substituting the original letters for the substituted letters, thereby recovering the original message.

For example, using the following substitution letters for the original letters

Letter	Substitution
a	j
b	i
c	d
d	o
e	t
f	h
g	u
h	q
i	a
j	b
k	r

Original → aBc 0

Encrypted
→ a – j, B – I, c – d, 0 → jId 0

Decrypted
→ j – a, I – B, d – c, 0 → aBc 0

Hints:
char array for substitution list (cipher file)
charAt() – Lecture 5: Strings
isLetter() – Lecture 5: Character Operations