## Calvin Hew 2078855H

**Assessed Exercise 2: Monoalphabetic and Vigenere Cipher Program**

The final state of the program can be described as complete upon reflection of the task specification. The program is able to carry out the operations of encoding and decoding utilising both Monoalphabetic and Vigenere cipher methods.

A number of assumptions were made upon the implantation of the program. It was stated that the initial message in the plain text file (prior to encoding) was supposed to be in capital letters. Thus, it was assumed that any other characters in the file: lowercase letters, punctuation, whitespace etc. would not be encoded, but written to the output file as they originally appeared on the initial plain text file. Though checks for lower case characters and repeated letters were considered for the keyword input used to create the cipher, users could still type in non-letter symbols (such as !,@,£ etc.). However, this would cause the cipher to not function as intended to, so it was assumed that the user would only input letters when creating the keyword. It was assumed that a keyword had to contain at least one character and held an upper limit of 26 letters.

Tests were conducted using the sample text file (text1P.txt) provided in the setup folder to highlight the program’s main functionality as shown in *Appendix 1* for the Vigenere cipher, whilst the coder’s own tests were used for the Monocipher as shown in *Appendix 2*.

The Vigenere test (*Appendix 1*) uses the keyword **LEOPARD** to generate the cipher alphabet successfully as shown. The initial plaintext file (text1P), provided in the AE2 setup file was encoded. This produced a cipher text file (text1C), which was then further decoded to a deciphered file (text1D).

The encryption and decryption functions of the program appeared to work as the contents of the input P and output D files were identical. The letter frequencies report corresponded with expected values calculated on paper with letters ‘H’ and ‘E’ being the most frequent letters for encoded and decoded files respectively.

The Monocipher test *(Appendix 2)* was conducted in a similar manner to the Vigener test, where the keyword of **PIRATE** was used in this instance. Moreover, the message used for the input P file contained other special cases such as lower-case letters and punctuation that were not addressed when testing the Vigenere cipher.

As before upon encoding, an encrypted file- messageC and a letter frequency report was produced from the plain text file message. The contents within the decoded messageD file matched the text in the original plain text file, thus justifying the Monocipher’s functioning state. Both frequency reports produced showed that ‘O’ was the most frequently used character. This was also identified when calculating expected results as the cipher used left the letter ‘O’ unchanged due to the character having the same index in both the monoalphabet and regular alphabet.

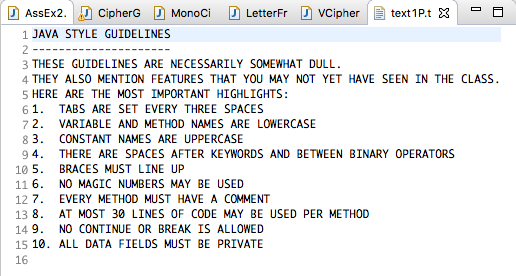
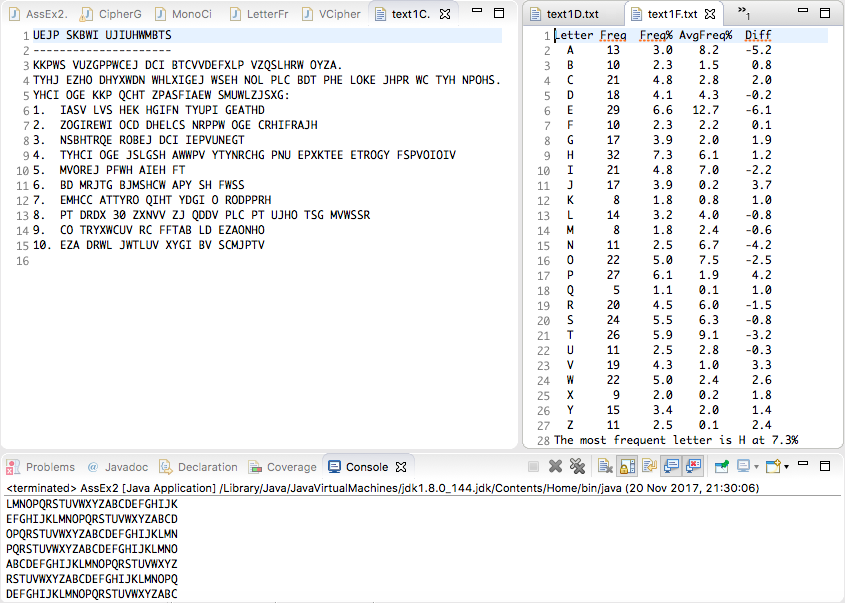
*Appendix 3* shows all the input exceptions that can be thrown if:

* Keyword is left blank, contains lowercase letters or has repeated letters.
* File does not exist, file name does not end in P/C/D or file name is left blank.

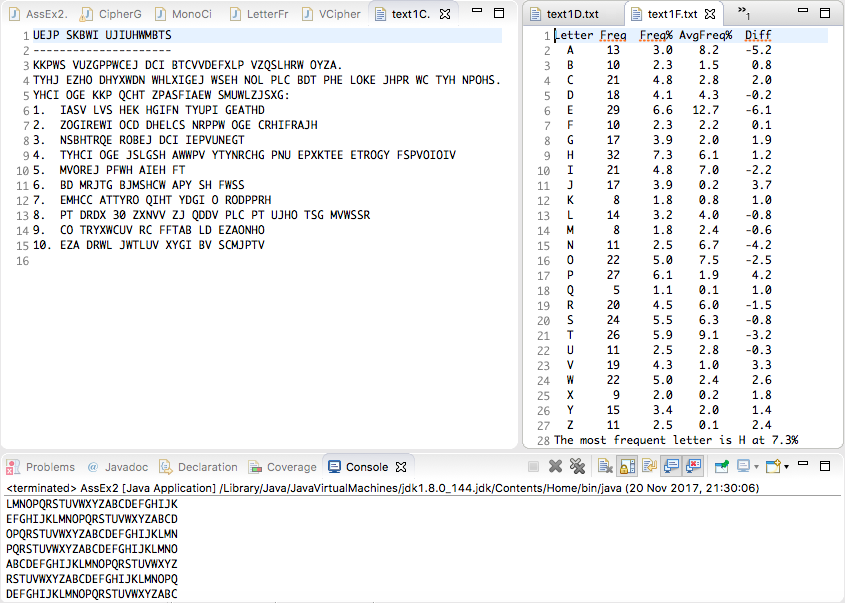
**Appendices (Screendumps)**

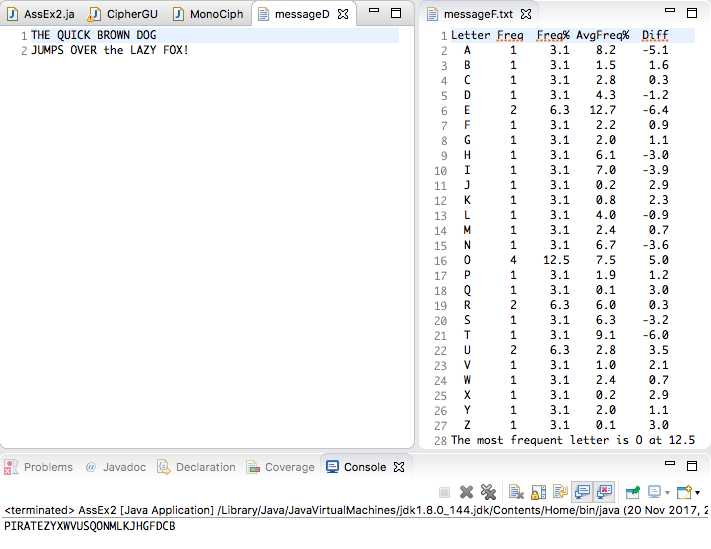
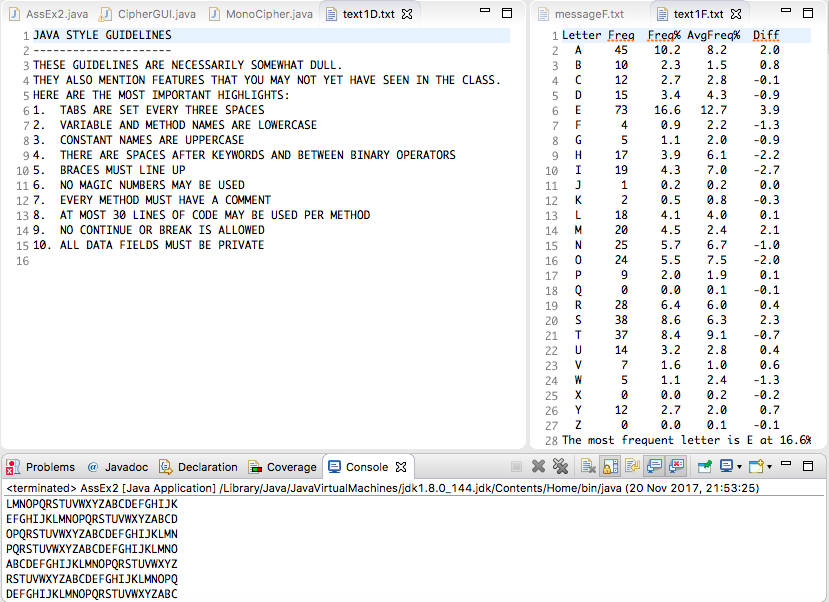
*Appendix 1: Vigener Cipher*

Printed VCipher Alphabet



Original Plain Text (P) File



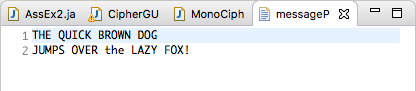
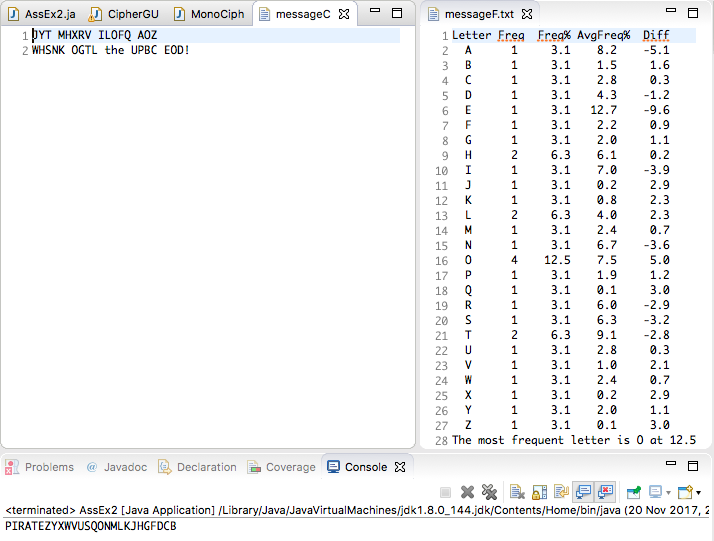
*Appendix 2: Monoalphabetic Cipher*

Decoded File (D) with Frequency Report

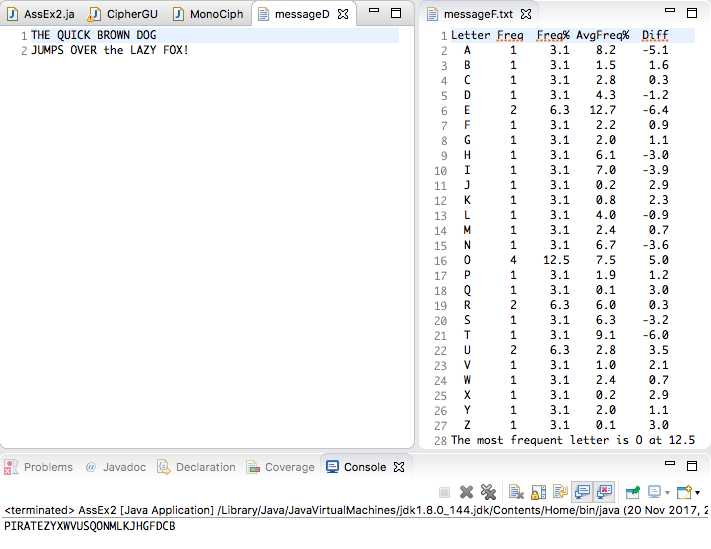
Encoded File (C) with Frequency Report

Original Plain Text (P) File

Printed Monocipher Alphabet

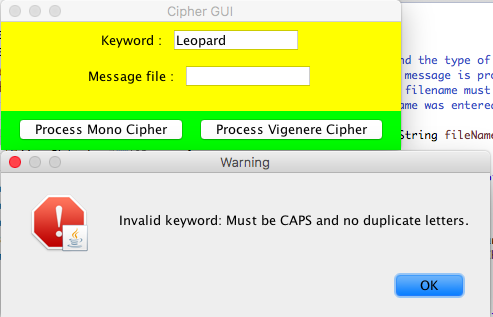


Encoded (C) File with Frequency Report

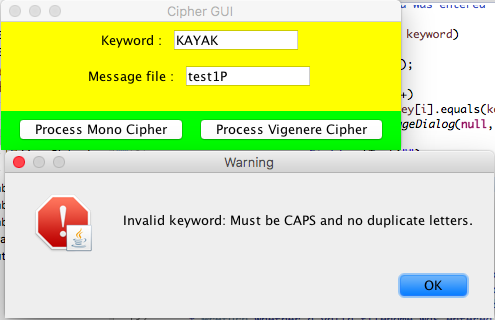
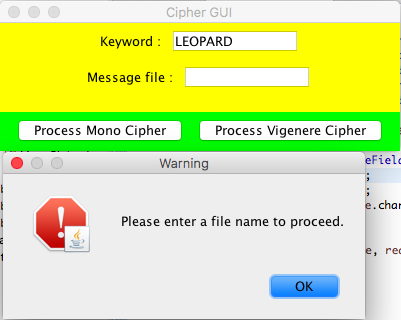
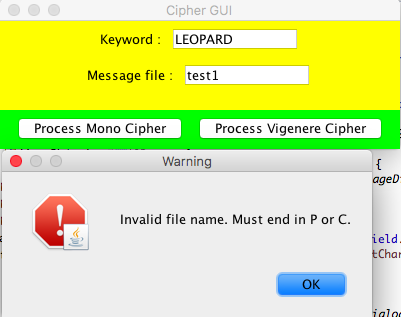
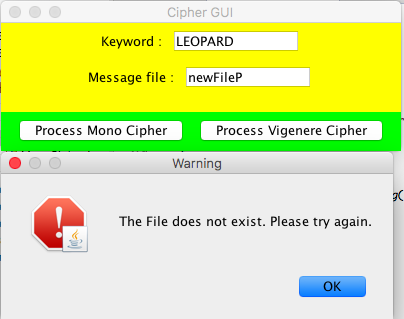
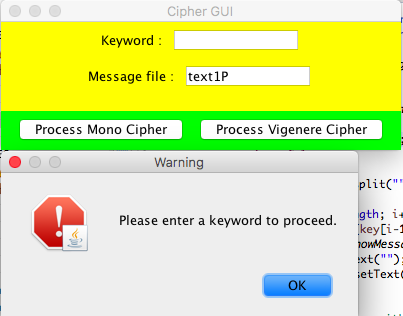


Decoded File (D) with Frequency Report

Appendix 3: Exception Testing



Lower case Letters Error



Empty Keyword Error

Non-Existent File Error

Invalid File Name Error

Empty File Name Error

Duplicate Letters Error