CMP1127M Programming & Data Structures Assessment 1 Report

Andrew Smith

1. Basic Features

Feature	Explanation
Caesar Cipher Encryption	Encrypts plain text into cipher text through the use of the Caesar Cipher method of encryption and key shifts corresponding to the standard English alphabet.
Caesar Cipher Decryption	Decrypts cipher text back into all possible plaintexts through the use of the Caesar cipher method of decryption, all possible decryptions are displayed on the screen to the user along with the keys along with the programs recommendations.
Exception Handling	Handles exceptions well, program does not advance when users put in the wrong data.
Classes	Program is built around 5 main classes in which instances are made of them and their methods are called upon at various points during the program.
Write to Text File	The program allows all possible decryptions to be written to a text file with a .txt extension.
Variety of Programming Techniques	A wide variety of C# programming techniques have been used, including switches, for loops, while loops, if statements, conversion between data types, classes, methods etc.

2. Data Structures Used

Data Structure	Explanation	Example of use in Program
Integer	Any whole number.	int countX = 0;
Boolean	Any value that is true or false.	switch1 = false;
String	Any consecutive series of characters.	string decryptedWord = “”;
Char	Any single character.	char x;
Array (list)	A collection of data types that are the same type.	char[] alphabetList = {'A','B','C','D'…}’
Array (collection)	A collection of data types.	List<int> possibilityListKeyA = new List<int>();
Dictionary (collection)	A collection of values that have a key and a value.	Dictionary<string, int> decryptedPossibilites = new Dictionary<string, int>();

3. Additional Features (Enhanced Submission)

Feature	Explanation
Option to pass the already once encrypted cipher text through a cipher alphabet.	The encrypted text can be encrypted once more if the user selects this option. If they select it then after the encrypted message has been shifted with the Caesar Cipher it is passed through a random cipher alphabet to encode it even more. This was a standard feature of the enigma machine and offers more security as the decrypter has to discover the cipher alphabet too.
Frequency Analysis Method 1	Frequency analysis is used in the Caesar cipher decryption part of this program. Firstly, the possible decryptions are displayed and then at the bottom there are a number of decryptions that the program "believes" to be correct based on the degree of accuracy. This works by counting the number of 'e' and 't' characters (the 2 most frequent characters in the English alphabet) in the plaintext and then sorting this in order via a bubble sort algorithm, then the top results are sectioned off and displayed to the user.
Bubble sort Algorithm	There is a bubble sort algorithm implemented into this program to order the frequency of letters from highest to lowest. This is used in the frequency analysis.
Frequency Analysis Method 2	In the Affine Cipher decryption part, another method of frequency analysis is implemented. This is done differently, with this new method counting the number of times the top 5 letters in the English Alphabets appear in the plaintext and then using this to calculate the decryption with the highest frequency of English letters.
Random Generation of Keys	When the user selects to encrypt a message, they can either input their own keys to use or they can request a random key to be generated for them.
Write to Text File Name of Choice	When the user is asked whether they want the message to be written to a text file they can choose the name of the text file with the .txt file extension.
Write to Webpage	The user can also request the decryptions to be written to a basic HTML webpage for viewing on the web.

4. Additional Tasks (Enhanced Submission)

Feature	Explanation
Affine Cipher Encryption	The enhanced additional tasks for the assessment have been completed. This mainly involved the Affine Cipher, which works by calculating modular values. This program includes a feature to select to encrypt using this method of encryption for a higher level of security.
Affine Cipher Decryption	The program also allows you to decrypt the Affine cipher as mentioned in the advanced section of the project. This allows all 312 possible Affine cipher keys to be listed, working through the possible A values (1,3, 5…) and B values (1,2,3,4…) and displaying them and the plaintext.
Frequency Analysis Method 2	Frequency analysis is used again here to display what the machine thinks to be the most probable decryption.
Random Generation of Keys	The Affine encryption can randomly generate a key for the user to use.
High Number of Keys	The Affine cipher allows for 312 different keys to be used so this has a higher security than the standard Caesar cipher.
Write to Text file	The Affine Cipher section of the program allows the user to write the decryption possibilities to a text file.
Write to Webpage	The Affine Cipher section of the program allows the user to write the decryption possibilities to a basic HTML webpage.

Video URL: https://youtu.be/PgeB0vfAd78

References:

Sphar, C. and Davis, S. R., (2008), *C# 2008 For Dummies,* Indianapolis, Indiana: Wiley Publishing, INC.

Singh, S. , (1999) *The Code Book, The Secret History of Codes and Codebreaking,* London: Fourth Estate.

Van der Lubbe, Jan C.A. , (1998) *Basic Methods of Cryptography,* Cambridge: Press Syndicate of The University of Cambridge.

MSDN Microsoft (2015) *String.length Property.* Available from https://msdn.microsoft.com/en-us/library/system.string.length%28v=vs.110%29.aspx?f=255&MSPPError=-2147217396 [Accessed 15th November 2015].

MSDN Microsoft (2015) *Collections (C# and Visual Basic).* Available from https://msdn.microsoft.com/en-us/library/ybcx56wz.aspx?f=255&MSPPError=-2147217396 [Accessed 18th November 2015].

Stack Overflow (2012) *% (mod) explanation).* Available from http://stackoverflow.com/questions/10065080/mod-explanation [Accessed 24th November 2015].

Stack Overflow (2011) *Efficient way to remove ALL whitespace from String).* Available from http://stackoverflow.com/questions/6219454/efficient-way-to-remove-all-whitespace-from-string [Accessed 21st November 2015].

Stack Overflow (2011) *Easiest way to read from and write to files).* Available from http://stackoverflow.com/questions/7569904/easiest-way-to-read-from-and-write-to-files [Accessed 18th November 2015].