



Computer Science and Engineering

Applied Cryptography Project 1
(Cryptanalysis: decryption of substitution ciphers)

Team Members:

Names	Net ID	Email ID
Archana Purushothama	ap4095	ap4095@nyu.edu
Prashanth Tekal Venkateshprasanna	ptv207	prashanth.venkatesh@nyu.edu

Table of Contents

	Topic	Page Number
1.	Introduction	3
2.	Implementation	4-5
2.1	Cryptanalysis using Dictionary1	5
2.2	Cryptanalysis using Dictionary2	5
3.	Sample Execution Output	6-8

1. Introduction

Cryptanalysis (from the Greek *kryptós*, "hidden", and *analýein*, "to loosen" or "to untie") is the study of analyzing information systems in order to study the hidden aspects of the systems. It is also the art of deciphering encrypted communications without knowing the proper keys. There are many cryptanalytic techniques.

The project focuses on cracking a *Symmetric-Key Ciphers* by exploring its weakness. If the length of the key is known then we can design a deterministic algorithm to find the corresponding plaintext by guessing. As there is a time constraint to break the given ciphertext the project challenges us to design a logic which provides results in least possible time. Though these encryption methods are now outdated, but still they are used to crack the cryptographic challenges.

The name *substitution cipher* comes from the fact that each letter that you want to encipher is substituted by another letter or symbol, but the order in which these appear is kept the same. Another way to say this is that the message you want to keep secret (called the *plaintext*) is transformed into the enciphered message (called the *ciphertext*) by using a different alphabet.

The substitution systems can be classified as Monoalphabetic Ciphers and Polyalphabetic Ciphers.

1. *Cracking of Monoalphabetic Ciphers*

We have the knowledge of all possible *plaintext* and the *Key length*. In this case if the key length =1 then shifting the ciphertext by 1 in either direction and comparing the calculated plaintext to the given Dictionaries will easily help us guess the encoded plaintext.

2. *Cracking of Polyalphabetic Ciphers*

A typical polyalphabetic system will use from 2 to 26 different alphabets. Polyalphabetic systems which repeat the same set of alphabets over and over again in the same sequence are known as periodic systems. Polyalphabetic systems which do not keep repeating the same alphabets in the same order are known as aperiodic systems.

2. Implementation

- **Language – C++**

- **Known facts –**

- The plaintext space and ciphertext space are the set $\{\text{<space>,a,...,z}\}^L$. where $L(\text{length})$ is given as 100.
- The key space is the set $\{0,...,26\}^t$. In other words the key k can be written as $k[1],...,k[t]$, where each $k[j]$ is in $\{0,...,26\}$, for $j=1,...,t$.
- The encryption algorithm computes each $c[i]$ as equal to the (lexicographic) shift of $m[i]$ by $k[j(i)]$ positions, where the computation of each $j(i)$ is left unspecified and may depend on i,t,L . In other words, each ciphertext symbol $c[i]$ is the shift of the plaintext symbol $m[i]$ by a number of position equal to one of the key symbols, which symbol being chosen according to an undisclosed, deterministic, and not key-based, scheduling algorithm that is a function of i, t and L .

- **Input to the program**

- The number t of key symbols
- An L -symbol challenge ciphertext

- **Output of the program**

- Possible set of key symbols
- Plaintext if found in the Dictionary
- Time taken for the execution

- **Assumption** – ‘ t ’ key symbols are distinct but is applied on plaintext in any possible combination.

- Exception cases are handled. For instance, incorrect `keyLength`.

2.1 Cryptanalysis using Dictionary 1 :

- a) Parse the Dictionary1 and given cipher text to find the difference in Ascii values of each character [0-26 for the alphabets and 33-91 for the space]
- b) Key symbols are recorded, where key symbol is the Ascii difference.
- c) KeyLength is the prime parameter, which is checked to determine if a particular text is a part of cipher or not.
- d) A flag variable is set if the plaintext is found in the dictionary.
- e) Parsing is stopped if entire Dictionary is parsed or if matching plaintext is found for the cipher.

2.2 Cryptanalysis using Dictionary 2 :

Assumption – Ciphertext contains any of the words but retain the order in which they appear in Dictionary

An approach similar to the Dictionary1 is used,

- a) Parse the Dictionary2 starting from a random word in the dictionary to avoid the incorrect calculation when the keyLength is larger than the word.
- b) The Ascii difference between the characters is calculated and recorded as the key symbols.
- c) KeyLength is the prime parameter, which is used to determine if a particular word is the part of given cipher.
- d) A flag variable is set when a possible plaintext is found.
- e) Parsing is halted when the entire dictionary is parsed or a matching plaintext is found.
- f) In case plaintext is not found in the Dictionary, partial match is output if present.

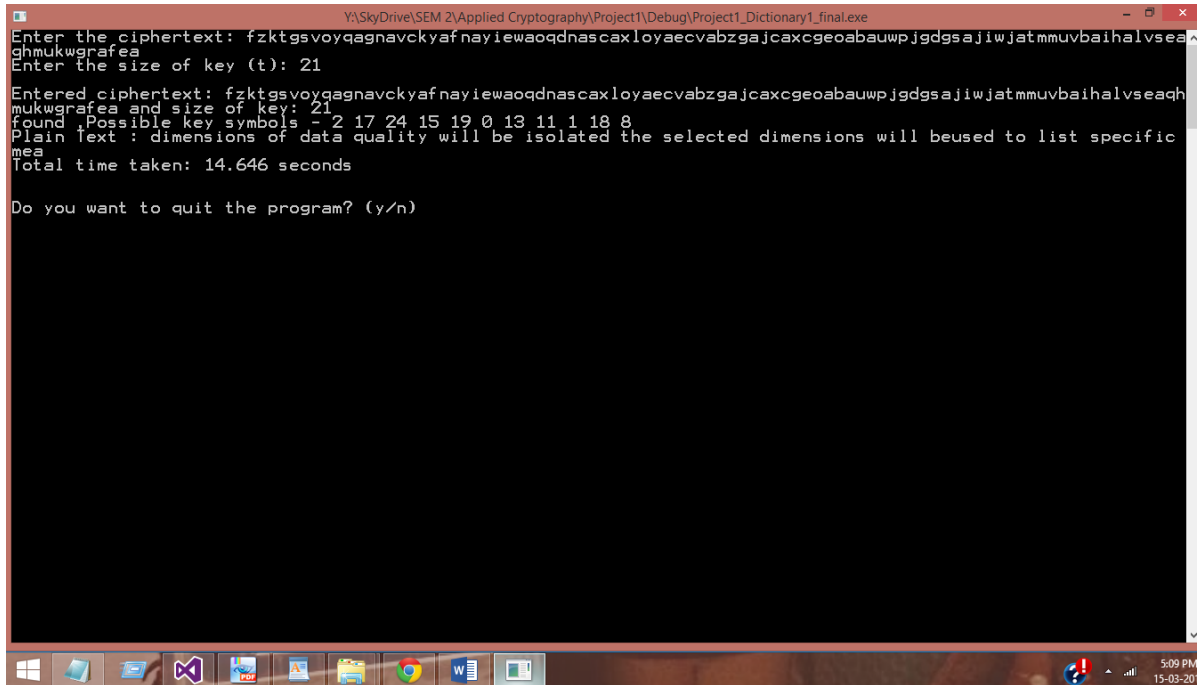
Scope of improvement:

- g) On failure to find a plaintext match in the first iteration in Dictionary, we can reiterate.
For instance,
Round 1: Parsing started from random position 14 in dictionary, and the previous first word match was at 20,
Round 2 is started from position 21.

3. Sample Execution Output

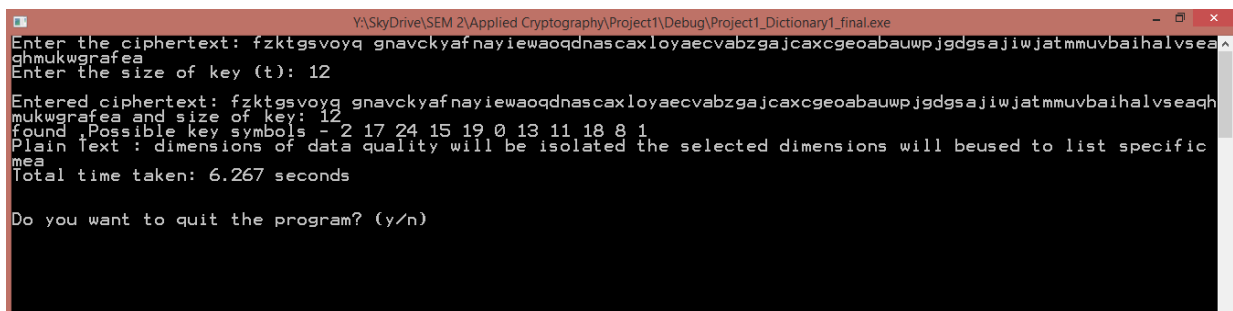
3.1 Sample run for Dictionary1

Figure 1: Execution with KeyLength 21



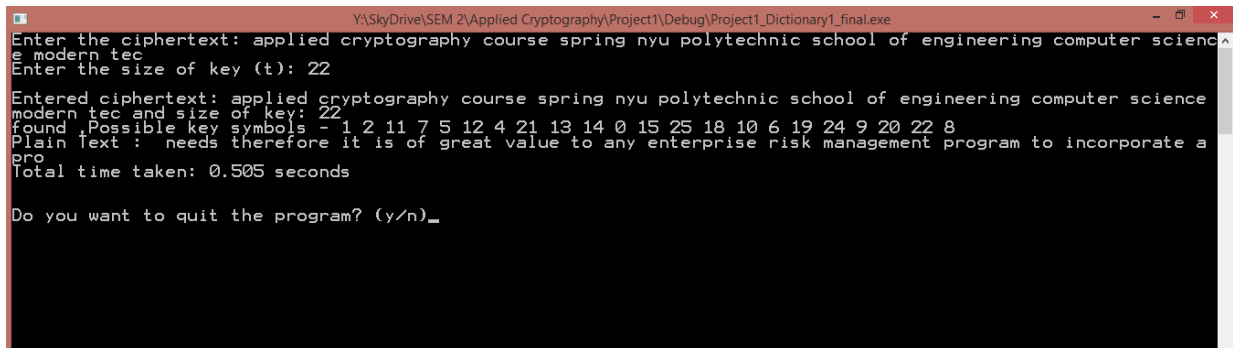
```
Y:\SkyDrive\SEM 2\Applied Cryptography\Project1\Debug\Project1_Dictionary1_final.exe
Enter the ciphertext: fzktgsvoyqagnavckyafnayiewaoqdnascaxloyaecvabzgajcaxcgeoabauwpjgdgsajiwjatmmuvbaihalvseah
ghmukwgrafea
Enter the size of key (t): 21
Entered ciphertext: fzktgsvoyqagnavckyafnayiewaoqdnascaxloyaecvabzgajcaxcgeoabauwpjgdgsajiwjatmmuvbaihalvseah
mukwgrafea and size of key: 21
found Possible key symbols - 2 17 24 15 19 0 13 11 1 18 8
Plain text : dimensions of data quality will be isolated the selected dimensions will be used to list specific
mea
Total time taken: 14.646 seconds
Do you want to quit the program? (y/n)
```

Figure 2: Example Run 2



```
Y:\SkyDrive\SEM 2\Applied Cryptography\Project1\Debug\Project1_Dictionary1_final.exe
Enter the ciphertext: fzktgsvoyq gnavckyafnayiewaoqdnascaxloyaecvabzgajcaxcgeoabauwpjgdgsajiwjatmmuvbaihalvseah
ghmukwgrafea
Enter the size of key (t): 12
Entered ciphertext: fzktgsvoyq gnavckyafnayiewaoqdnascaxloyaecvabzgajcaxcgeoabauwpjgdgsajiwjatmmuvbaihalvseah
mukwgrafea and size of key: 12
found Possible key symbols - 2 17 24 15 19 0 13 11 18 8 1
Plain text : dimensions of data quality will be isolated the selected dimensions will be used to list specific
mea
Total time taken: 6.267 seconds
Do you want to quit the program? (y/n)
```

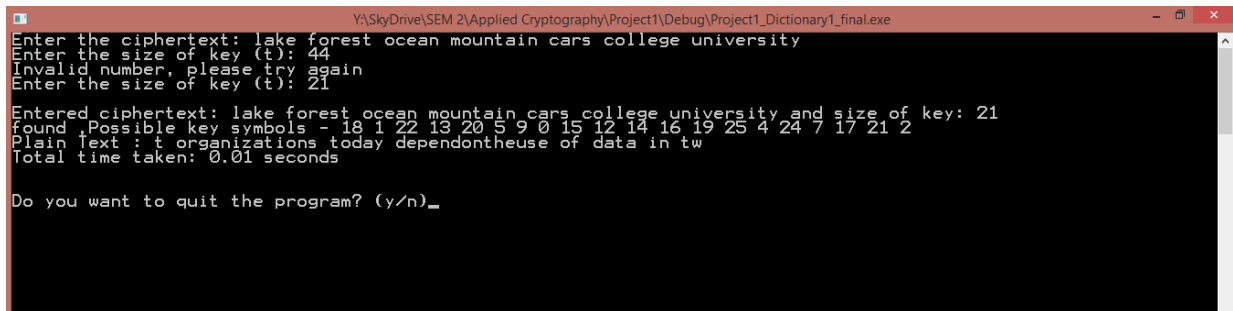
Figure 3: Example Run 3



```
Y:\SkyDrive\SEM 2\Applied Cryptography\Project1\Debug\Project1_Dictionary1_final.exe
Enter the ciphertext: applied cryptography course spring nyu polytechnic school of engineering computer scienc
e modern tec
Enter the size of key (t): 22
Entered ciphertext: applied cryptography course spring nyu polytechnic school of engineering computer science
modern tec and size of key: 22
found Possible key symbols - 1 2 11 7 5 12 4 21 13 14 0 15 25 18 10 6 19 24 9 20 22 8
Plain text : needs therefore it is of great value to any enterprise risk management program to incorporate a
pro
Total time taken: 0.505 seconds

Do you want to quit the program? (y/n)_
```

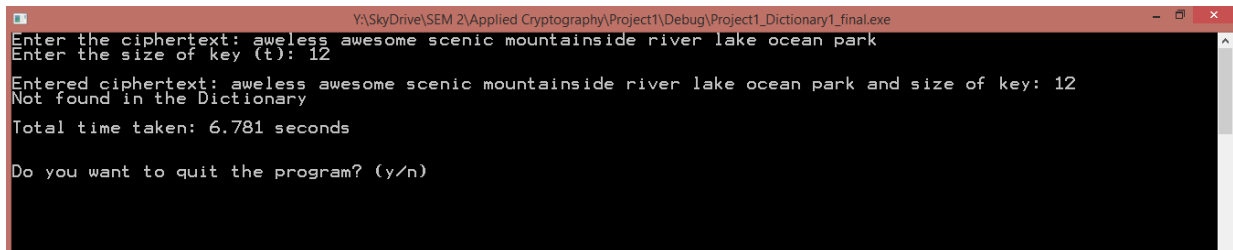
Figure 4: Example Run 4



```
Y:\SkyDrive\SEM 2\Applied Cryptography\Project1\Debug\Project1_Dictionary1_final.exe
Enter the ciphertext: lake forest ocean mountain cars college university
Enter the size of key (t): 44
Invalid number, please try again
Enter the size of key (t): 21
Entered ciphertext: lake forest ocean mountain cars college university and size of key: 21
found Possible key symbols - 18 1 22 13 20 5 9 0 15 12 14 16 19 25 4 24 7 17 21 2
Plain text : t organizations today dependontheuse of data in tw
Total time taken: 0.01 seconds

Do you want to quit the program? (y/n)_
```

Figure 5: Output of example Run 5

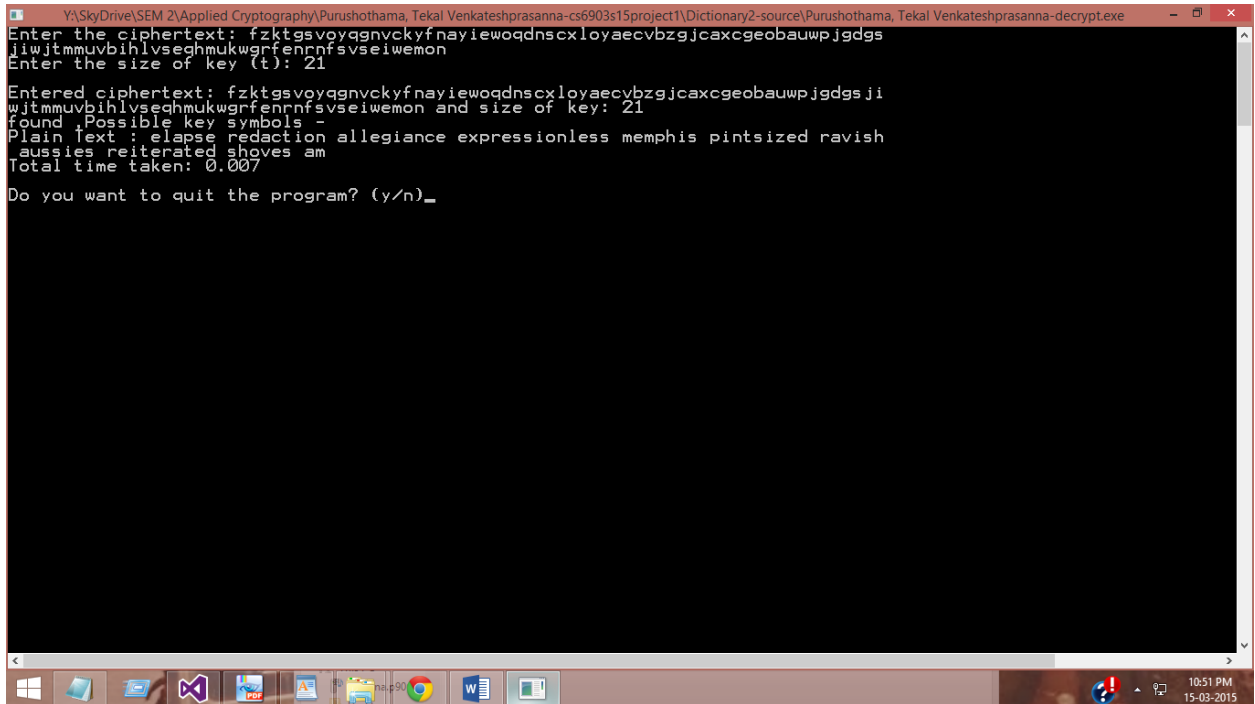


```
Y:\SkyDrive\SEM 2\Applied Cryptography\Project1\Debug\Project1_Dictionary1_final.exe
Enter the ciphertext: aweless awesome scenic mountainside river lake ocean park
Enter the size of key (t): 12
Entered ciphertext: aweless awesome scenic mountainside river lake ocean park and size of key: 12
Not found in the Dictionary
Total time taken: 6.781 seconds

Do you want to quit the program? (y/n)
```

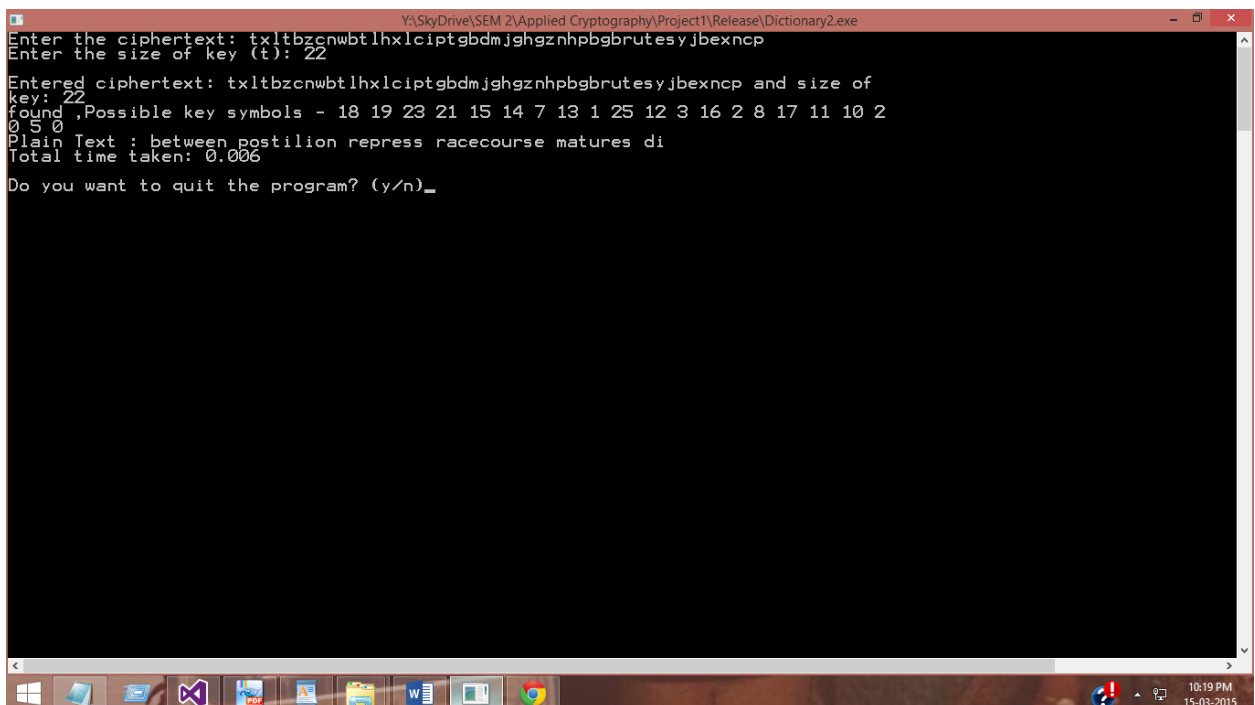
3.2 Sample run for Dictionary2

Figure 6: Output of Example run 1



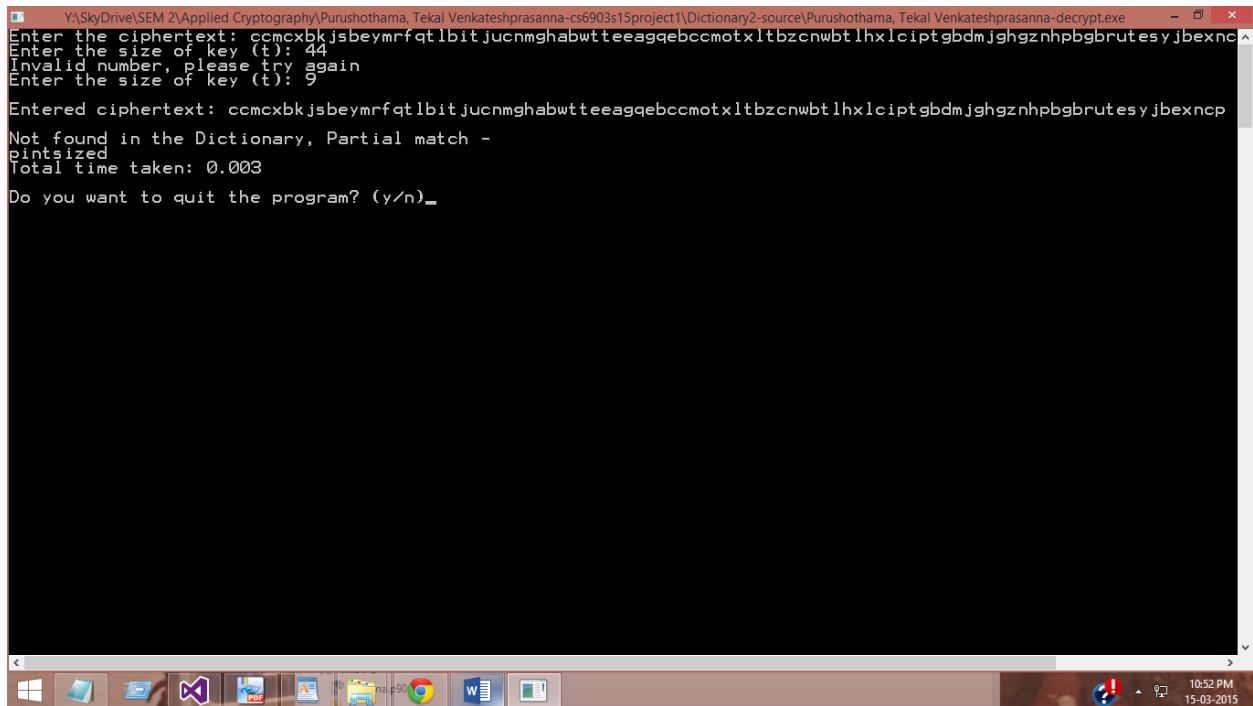
```
Y:\SkyDrive\SEM 2\Applied Cryptography\Purushothama, Tekal Venkateshprasanna-cs6903s15project1\Dictionary2-source\Purushothama, Tekal Venkateshprasanna-decrypt.exe
Enter the ciphertext: fzktgsvoyqgnvckyfnayiewoqdnscxloyaecvbgjcaxcgeobauwpjgdgs
Enter the size of key (t): 21
Entered ciphertext: fzktgsvoyqgnvckyfnayiewoqdnscxloyaecvbgjcaxcgeobauwpjgdgsji
wjtmmbvbihlvseghmukwgrfennrfsvseiwemon and size of key: 21
found Possible key symbols -
Plain Text : elapse redaction allegiance expressionless memphis pint-sized ravish
aussies reiterated shoves am
Total time taken: 0.007
Do you want to quit the program? (y/n)_
```

Figure 7: Output of Example run 2



```
Y:\SkyDrive\SEM 2\Applied Cryptography\Project1\Release\Dictionary2.exe
Enter the ciphertext: txltbzcwnbtlhxlciptgbdmjghgznhpbgbbrutesyjbexncp
Enter the size of key (t): 22
Entered ciphertext: txltbzcwnbtlhxlciptgbdmjghgznhpbgbbrutesyjbexncp and size of
key: 22
found Possible key symbols - 18 19 23 21 15 14 7 13 1 25 12 3 16 2 8 17 11 10 2
0 5 0
Plain Text : between postilion repress racecourse matures di
Total time taken: 0.006
Do you want to quit the program? (y/n)_
```


Figure 8: Output of Example run 3



```
Y:\SkyDrive\SEM 2\Applied Cryptography\Purushothama, Tekal Venkateshprasanna-cs6903s15project1\Dictionary2-source\Purushothama, Tekal Venkateshprasanna-decrypt.exe
Enter the ciphertext: ccmcxbkjsbeymrftlbitjucnmghabwtteeagqebccmotxltbzcnwbtlhxlciptgbdmjghgznhpbgbbrutesyjbexnc
Enter the size of key (t): 44
Invalid number, please try again
Enter the size of key (t): 9
Entered ciphertext: ccmcxbkjsbeymrftlbitjucnmghabwtteeagqebccmotxltbzcnwbtlhxlciptgbdmjghgznhpbgbbrutesyjbexncp
Not found in the Dictionary, Partial match -
Printed size
Total time taken: 0.003
Do you want to quit the program? (y/n)_
```

Team members' Contribution

Both the team members collaborated and worked together to come up with a logic to solve the problem. Each team member has equal share in Brainstorming, Implementation and documentation of the report.