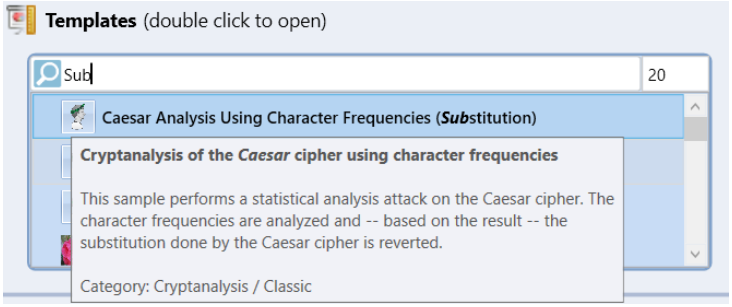
LAB 2 - CRYPTANALYSIS LAB
AKSHAY RAJENDRA GALGALI - 2060882
LAB EXERCISES

Initially, for the questions 1,2,3,4, and for 7,8,9 cipher texts as given below:

1. PMFBP PBKAP BZOBQ JBPPX DBP
2. QEBXO OJVFP LKQEB JLSB
3. QELJX PGBCC BOPLK ABPFD KBAXP RYPQF QRQFL KZFME BO
4. SNSZK KXCHR ZAKDC KNMFH STCDE NQSXK ZSHT CDRDU DMSXS GQDD
7. UJTUQ JFQQF WTZSI YMJBT WQIQN PJYTX TQAJU ZEEQJ X
8. MIGYJ OTTFY MWUHV YBULX NIMIF PYVON MIGYU LYYUM S
9. QVQLB HGUVA XGUNG GUVFC HMMYR JNFUN EQBER NFLGB QB?

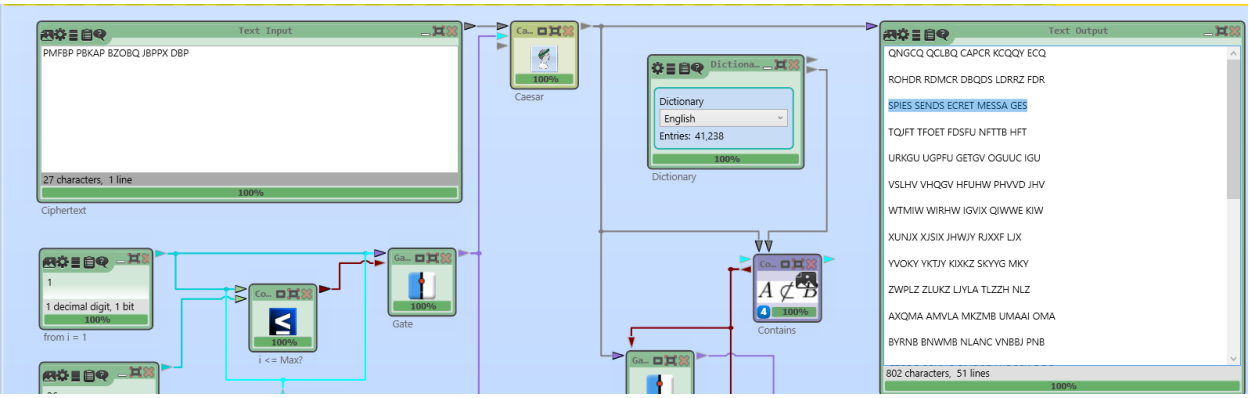
I used an Online Cipher Identifier tool to determine the type of the Cipher and it concluded to be “Caesar Cipher”. Then I used a template “Caesar Cipher Brute Force Analysis” in the Cryptool to Decrypt the cipher text. I took the Text input from the given Cipher Text and selected language as “English” and I got numerous outputs where, one output was in English readable form and I concluded as the output for the given cipher text as shown in the given figure below.



And for the Cipher text questions 10,11,12,13,14, I have made used of a Online Cryptanalysis tool quippuiq.com which solves substitution ciphers into plain texts.

BASIC

Q1.
Cipher Text: “PMFBP PBKAP BZOBQ JBPPX DBP”
Plain Text: “SPIES SEND SECRET MESSAGES”

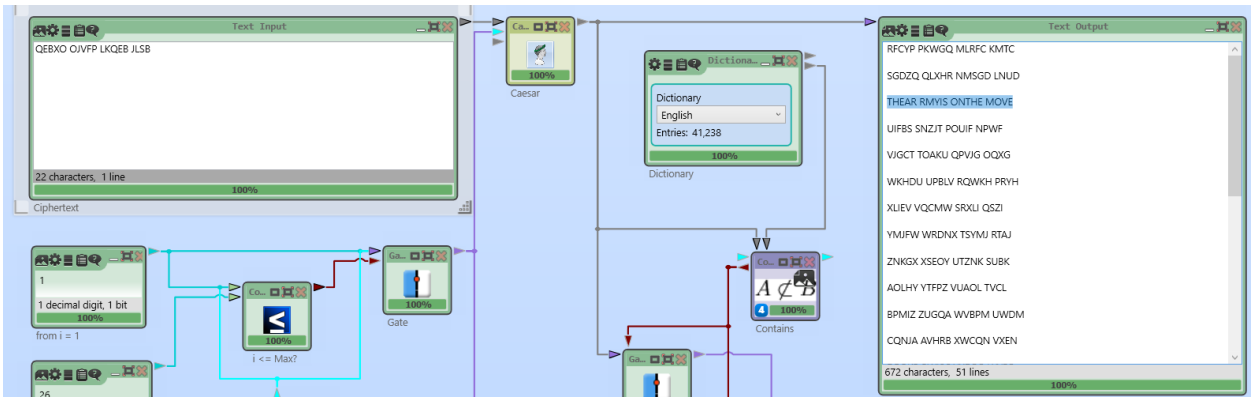


LAB 2 - CRYPTANALYSIS LAB
AKSHAY RAJENDRA GALGALI - 2060882

Q2.

Cipher Text: "QEBXO OJVFP LKQEB JLSB"

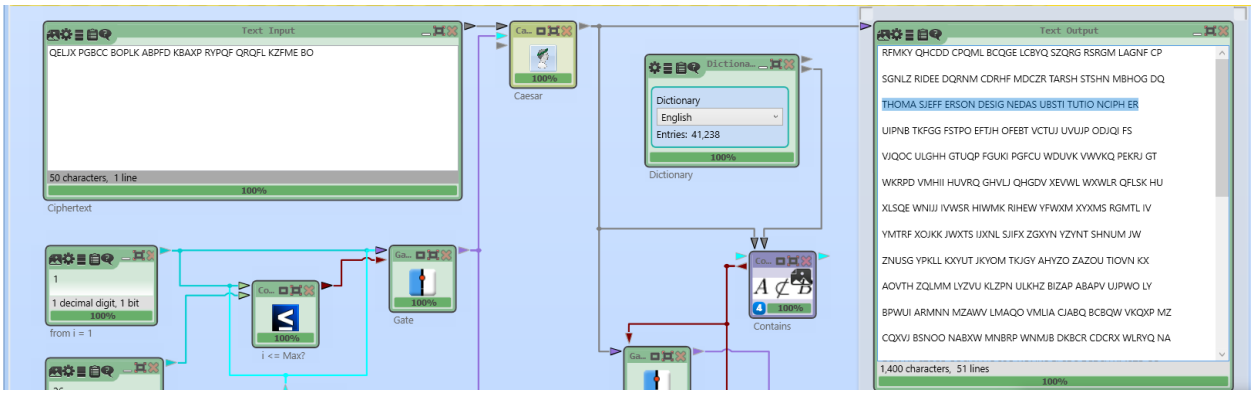
Plain Text: "THE ARMY IS ON THE MOVE"



Q3.

Cipher Text: "QELJX PGBCC BOPLK ABPFD KBAXP RYPQF QRQFL KZFME BO"

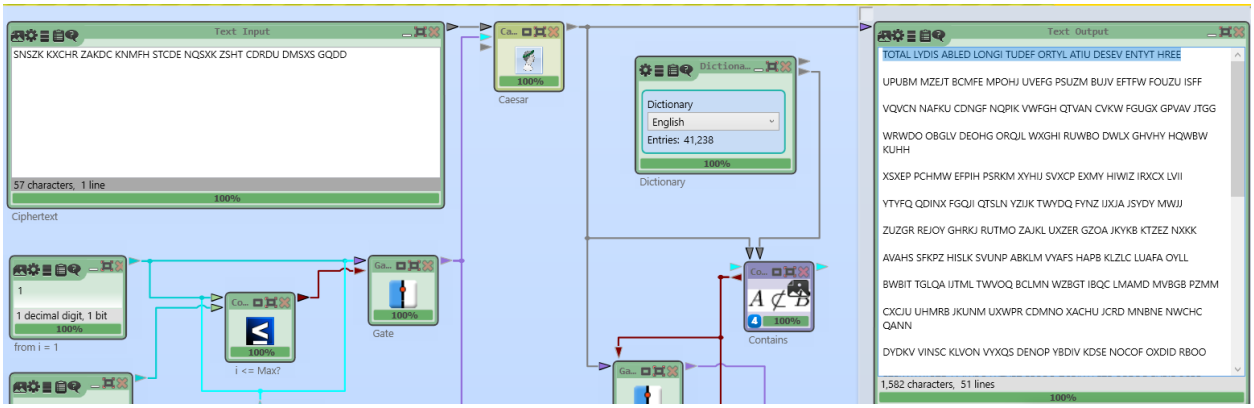
Plain Text: "THOMAS JEFFERSON DESIGNED A SUBSTITUTION CIPHER"



Q4.

Cipher Text: "SNSZK KXCHR ZAKDC KNMFH STCDE NQSXK ZSHT CDRDU DMSXS GQDD"

Plain Text: "TOTALLY DISABLED LONGITUDE FORTY LATITUDE SEVENTY THREE"



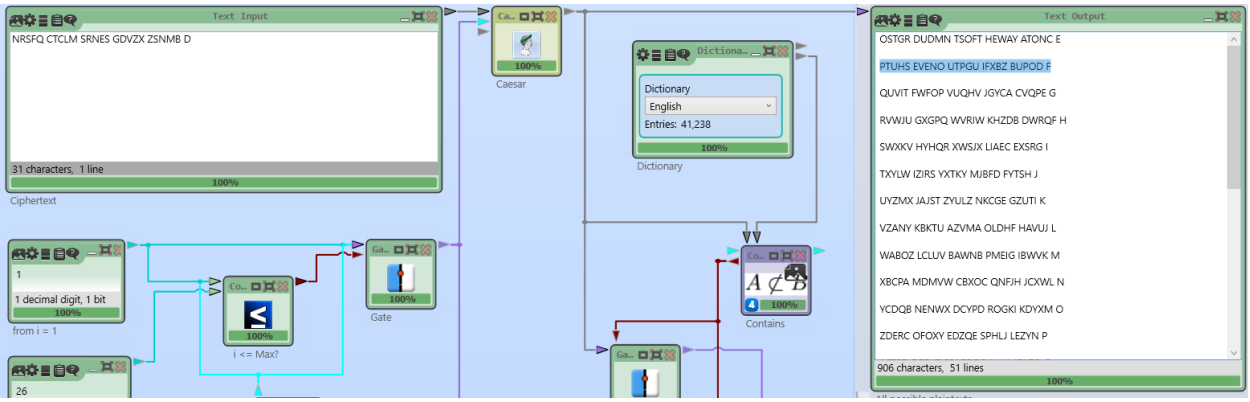
LAB 2 - CRYPTANALYSIS LAB
AKSHAY RAJENDRA GALGALI - 2060882

Q5.

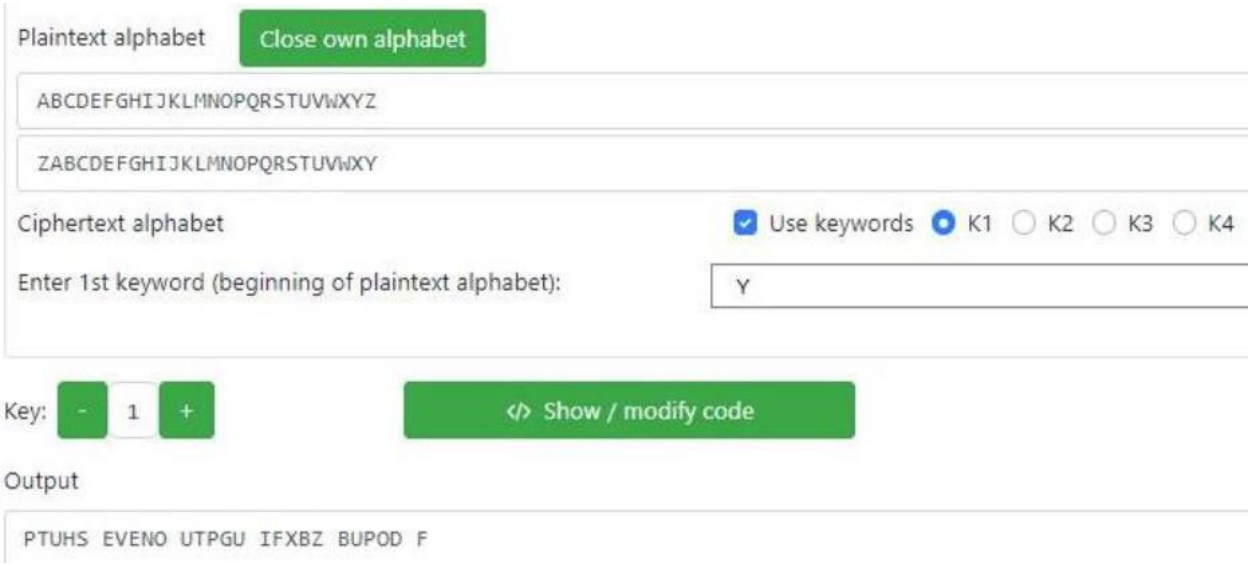
Cipher Text: "NRSFQ CTCLM SRNES GDVZX ZSNMB D"

Plain Text: "PUSH SEVEN OUT OF THE WAY AT ONCE"

For question 5 I initially I used Cryptool and then decrypted it using online tool. As shown in the given figure below.



It has to be further decrypted from the intermediate cipher, which is "PTUHS EVENO UTPGU IFXBZ BUPOD F." The key is "Y," and the key offset to enter is 1. The decryption procedure goes from Z to A, then A to B, and the encryption key is as follows. The phrase "PUSH SEVEN OUT OF THE WAY AT ONCE" appears after rearranging the alphabets and spaces in the cipher.



LAB 2 - CRYPTANALYSIS LAB
AKSHAY RAJENDRA GALGALI - 2060882

Q6.
Cipher Text: "RQVKM EFAUD XUGRQ AINAG LIPBC ROKJJ L"
Plain Text: "er boy skilful pering ip and the comma"

For this question I used quippiuq.com for decrypting and I got following output.

quipqiup beta3

quipqiup is a fast and automated cryptogram solver by Edwin Olson. It can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t).

Puzzle:

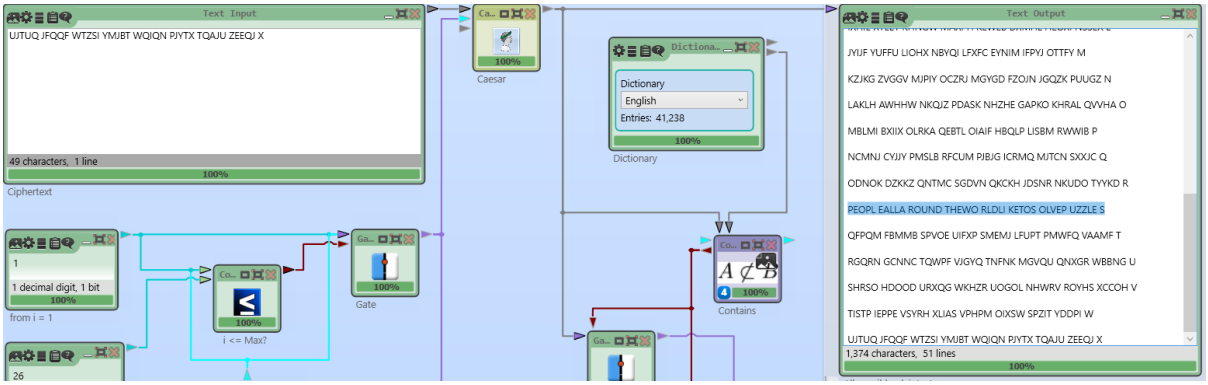
RQVKM EFAUD XUGRQ AINAG LIPBC ROKJJ L

Clues: For example G=R QVW=THE

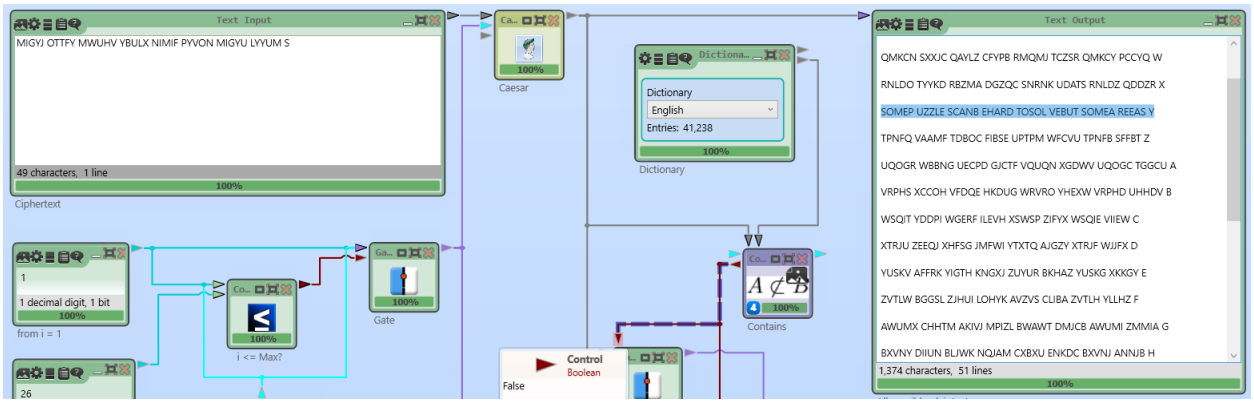
Solve

0 -2.579 er boy skilful pering ip and the comma

INTERMEDIATE
Q7.
Cipher Text: "
UJTUQ JFQQF WTZSI YMJBT WQIQN PJYTX TQAJU ZEEQJ X"
Plain Text: "PEOPLE ALL AROUND THE WORLD LIKE TO SOLVE PUZZLES"



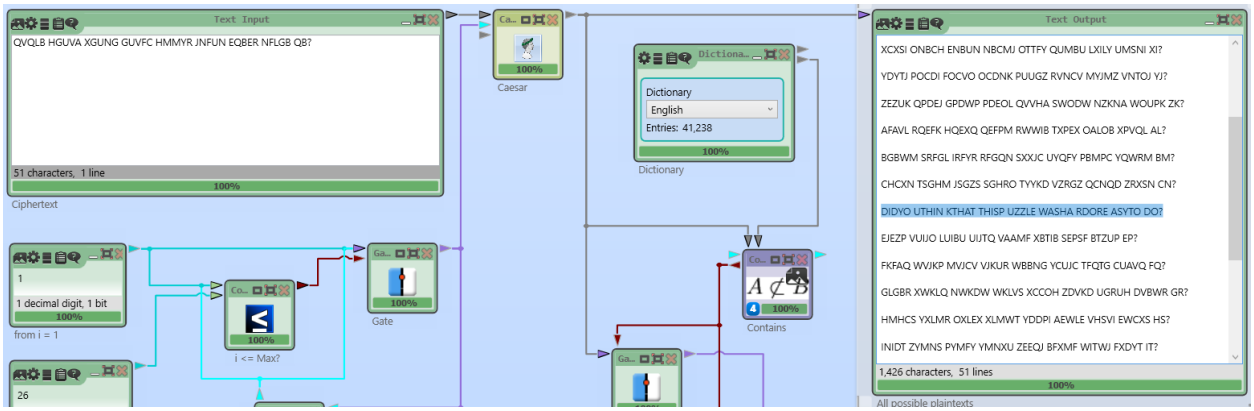
Q8.
Cipher Text: "MIGYJ OTTFY MWUHV YBULX NIMIF PYVON MIGYU LYYUM S "
Plain Text: "SOME PUZZLES CAN BE HARD TO SOLVE BUT SOME ARE EASY"



LAB 2 - CRYPTANALYSIS LAB
AKSHAY RAJENDRA GALGALI - 2060882

Q9.

Cipher Text: “QVQLB HGUVA XGUNG GUVFC HMMYR JNFUN EQBER NFLGB QB?”
Plain Text: “DID YOU THINK THAT THIS PUZZLE WAS HARD OR EASY TO DO?”



ADVANCED

Q10.

Cipher Text: “LHKUFXKUL, J LXYIRU ETMMRU KJD NU KTQU TE HV LUOUBJR EJBFL.”
Plain Text: “SOMETIMES, A SINGLE PUZZLE MAY BE MADE UP OF SEVERAL PARTS.”

quipqiup beta3

quipqiup is a fast and automated cryptogram solver by Edwin Olson. It can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t).

Puzzle:

LHKUFXKUL, J LXYIRU ETMMRU KJD NU KTQU TE HV LUOUBJR EJBFL.

Clues: For example G=R QVW=THE

Solve

0 -1.607 SOMETIMES, A SINGLE PUZZLE MAY BE MUDE UP OF SEVERAL PARTS.

Q11.

Cipher Text: “KEON MEGS FCHS IK HBWRKJ QX BGJKG SB OBFK SB E OBFMWKSK HBWCSQBX”
Plain Text: “EACH PART MUST BE SOLVED IN ORDER TO COME TO A COMPLETE SOLUTION”

quipqiup beta3

quipqiup is a fast and automated cryptogram solver by Edwin Olson. It can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t).

Puzzle:

KEON MEGS FCHS IK HBWRKJ QX BGJKG SB OBFK SB E OBFMWKSK HBWCSQBX

Clues: For example G=R QVW=THE

Solve

0 -1.280 EACH PART MUST BE SOLVED IN ORDER TO COME TO A COMPLETE SOLUTION

LAB 2 - CRYPTANALYSIS LAB
AKSHAY RAJENDRA GALGALI - 2060882

Q12.

Cipher Text: "VGT OANRV UZNV WO VGAR UFKKBT AR RWBHADX VGT LNQUVWXNZCR VGTCRTBHTR."
Plain Text: "THE FIRST PART OF THIS PUZZLE IS SOLVING THE CRYTOGRAMS THEMSELEVS."

quipqiup beta3

quipqiup is a fast and automated cryptogram solver by Edwin Olson. It can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t).

Puzzle:

VGT OANRV UZNV WO VGAR UFKKBT AR RWBHADX VGT LNQUVWXNZCR VGTCRTBHTR.

Clues: For example G=R QVW=THE

Solve

```
0    -1.455  THE FIRST PART OF THIS PUZZLE IS SOLVING THE CRYPTOGRAMS THEMSELVES.
```

Q13.

Cipher Text: "IMQC XRK TKOC AMCMWTDIM CBM FMXNRWA KOMA CR TDQ CBM PHZBPGMC."
Plain Text: "NEXT YOU MUST DETERMINE THE KEYWORD USED TO MIX THE ALPHABET"

quipqiup beta3

quipqiup is a fast and automated cryptogram solver by Edwin Olson. It can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t).

Puzzle:

IMQC XRK TKOC AMCMWTDIM CBM FMXNRWA KOMA CR TDQ CBM PHZBPGMC.

Clues: For example G=R QVW=THE

Solve

```
0    -1.710  NEXT YOU MUST DETERMINE THE KEYWORD USED TO MIX THE ALPHABET.
```

Q14.

Cipher Text: "TNUJTH, HKA QAUJ ZRLAFX KAJ JCX SKFW AUXW ZKF JCX UXJJROL."
Plain Text: "LASTLY, YOU MUST FIGURE OUT THE WORD USED FOR THE SETTING"

quipqiup beta3

quipqiup is a fast and automated cryptogram solver by Edwin Olson. It can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t).

Puzzle:

TNUJTH, HKA QAUJ ZRLAFX KAJ JCX SKFW AUXW ZKF JCX UXJJROL.

Clues: For example G=R QVW=THE

Solve

```
0    -1.602  LASTLY, YOU MUST FIGURE OUT THE WORD USED FOR THE SETTING.
```

LAB 2 - CRYPTANALYSIS LAB
AKSHAY RAJENDRA GALGALI - 2060882

Q. How can you tell if a ciphertext is substitution or transposition based?
Solution:
Transposition Cipher involves rearranging the positions of the characters but leaving the identity of the characters same without changing. Whereas, Substitution Cipher involves in changing the characters, it replaces one character with another.

The monogram frequencies can be used to distinguish between these two different sorts of ciphers. The frequency distribution of the English language is quite exact, and the transposition cipher has no effect on this. The frequencies can be used to identify the type of cipher.

Initially, I determine the frequency with which each letter appears in the ciphertext. After this I try replacing the letters using the frequency analysis and try to find terms that expose the plaintext by changing the letters in the ciphertext. I

look for repeating letter and search for a pattern and try to decode most of the letters like “for”, “and”, “was” etc., If it seems like a text from English literature which is readable, we can conclude that it is a Substitution Cipher or else it can be assume that it will be Transposition Cipher.

Q. Describe how you would go about attempting to break simple ciphers?
Solution:
Initially, I will look for the type of Cipher which can be done using frequency analysis where I determine what type of cipher it is. Majority of simple ciphers are substitution and transposition.

After determining the type of Cipher text as Transposition Cipher I would then try to obtain the plain text by predicting every word that might be made using various letter combinations.

If turned out to be substitution Cipher, I will try replacing the letters using the frequency analysis and try to find terms that expose the plaintext by changing and replacing the letters in the ciphertext.

I will look for repeating letter and search for a pattern and try to decode most of the letters like “for”, “and”, “was”, and check the rest with these words and try to retrieve text which is readable.

Q. How did a tool such as Cryptool help you in the assignment?
Solution:
The modern Cryptool, which visualizes cryptography and cryptanalysis, allowed me to easily decrypt the ciphers. It covers every aspect of modern cryptography, including the foundations of ciphers, encryption, and cryptanalysis.

Cryptool also includes more than 200 pre-made procedures and templates. It made it straightforward for me to put cryptographic functions together and utilize them to build processes for Cryptool 2 on my own.

This approach makes it easy to grasp difficult procedures, which enhances comprehension. The Cryptool was useful in better understanding cipher function. I was able to save a ton of time and effort due to the pre-existing templates because the tool did the most of the work; everything I needed to do was adjust the settings and add the required components to make it function.

Also, I made use of www.quippiuq.com which is an Online tool for decoding the cipher texts.

LAB 2 - CRYPTANALYSIS LAB
AKSHAY RAJENDRA GALGALI - 2060882

Q. If you did the programming puzzle, please include your code listing?

Solution:

To identify every key pair that may be used to unlock the ransomware file in this inquiry. Following program execution, I received 256 key pairs, and one of these 256 keys decrypts the file to produce an executable file with the name RunMe.exe.

PROGRAMMING: LOCKED FILE

Program:

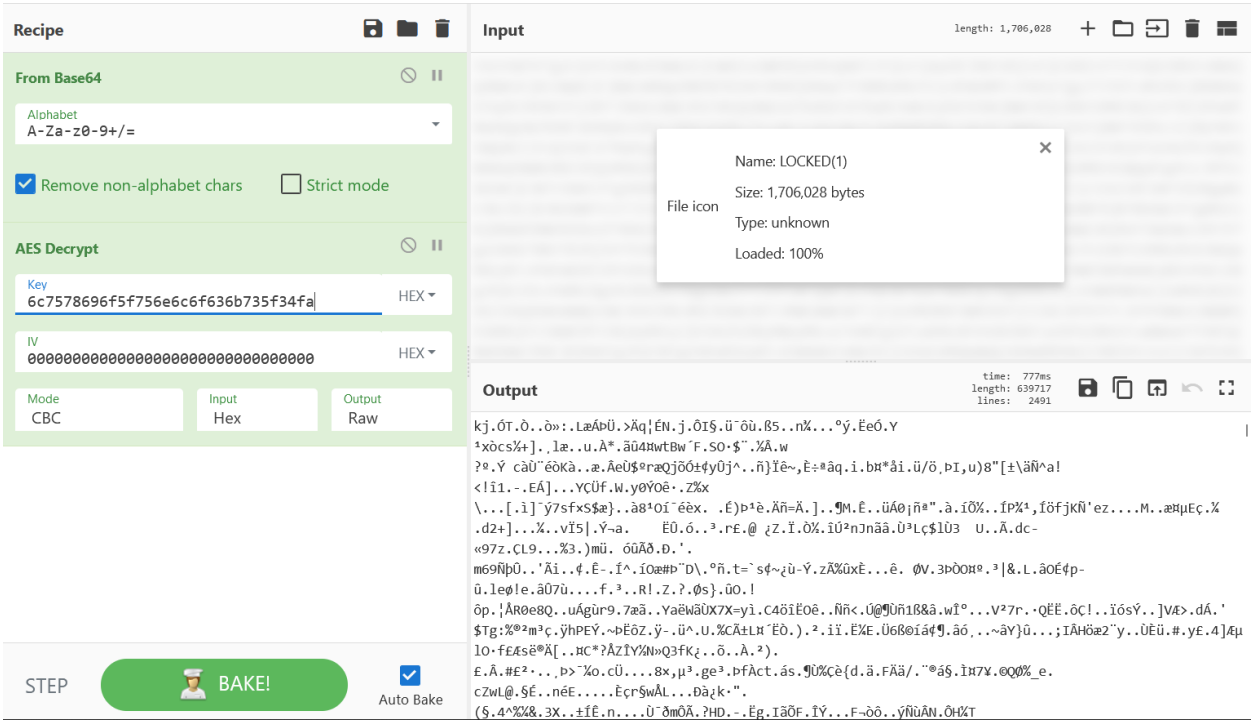
```
Python 3.7.4 (tags/v3.7.4:e09359112e, Jul  8 2019, 19:29:22) [MSC v.1916 32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> key = '6c7578696f5f756e6c6f636b735f34xx'
>>> partialkey = '6c7578696f5f756e6c6f636b735f34'
>>> for i in range(0,16):
...     for j in range(0,16):
...             d1 = str(i)
...             if i == 10:
...                     d1 = 'a'
...             elif i == 11:
...                     d1 = 'b'
...             elif i == 12:
...                     d1 = 'c'
...             elif i == 13:
...                     d1 = 'd'
...             elif i == 14:
...                     d1 = 'e'
...             elif i == 15:
...                     d1 = 'f'
...             d2 = str(j)
...             if j ==10:
...                     d2 = 'a'
...             elif j == 11:
...                     d2 = 'b'
...             elif j == 12:
...                     d2 = 'c'
...             elif j == 13:
...                     d2 = 'd'
...             elif j == 14:
...                     d2 = 'e'
```

Generated Keys:

```
6c7578696f5f756e6c6f636b735f3400
6c7578696f5f756e6c6f636b735f3401
6c7578696f5f756e6c6f636b735f3402
6c7578696f5f756e6c6f636b735f3403
6c7578696f5f756e6c6f636b735f3404
6c7578696f5f756e6c6f636b735f3405
6c7578696f5f756e6c6f636b735f3406
6c7578696f5f756e6c6f636b735f3407
6c7578696f5f756e6c6f636b735f3408
6c7578696f5f756e6c6f636b735f3409
6c7578696f5f756e6c6f636b735f340a
6c7578696f5f756e6c6f636b735f340b
6c7578696f5f756e6c6f636b735f340c
6c7578696f5f756e6c6f636b735f340d
6c7578696f5f756e6c6f636b735f340e
6c7578696f5f756e6c6f636b735f340f
6c7578696f5f756e6c6f636b735f3410
6c7578696f5f756e6c6f636b735f3411
6c7578696f5f756e6c6f636b735f3412
6c7578696f5f756e6c6f636b735f3413
6c7578696f5f756e6c6f636b735f3414
6c7578696f5f756e6c6f636b735f3415
6c7578696f5f756e6c6f636b735f3416
6c7578696f5f756e6c6f636b735f3417
6c7578696f5f756e6c6f636b735f3418
6c7578696f5f756e6c6f636b735f3419
```

LAB 2 - CRYPTANALYSIS LAB
AKSHAY RAJENDRA GALGALI - 2060882

Then, after generating keys I used Cyberchef online tool and tried to decode it using Recipes shown in the given figure below and download the output file and ran it.



The RUN.exe is not running and shows following error as shown in the given figure below.