

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Підготували студенти групи ФБ-23
Марченко Родіон та Лотиш Андрій

Київ, Жовтень 2024

Мета роботи:

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових шифрів гамування адитивного типу на прикладі шифру Віженера.

Порядок виконання роботи:

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини $r = 2, 3, 4, 5, 10-20$ знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Тексти, зашифровані шифром Віженера у варіантах завдань, написані російською мовою без знаків пунктуації, великих літер та пробілу; буква «ё» замінена буквою «е». Загальна кількість літер у алфавіті $m = 32$.

1. Напишемо дві програми мовою Python.

Перша програма є шифратором та дешифратором для шифру Віженера. Вона приймає відкритий текст російською (в коді є підтримка для української і англійської) мови у форматі .txt, ймає текстовий ключ, параметр, що визначає чи застосовується режим шифрування чи дешифрування, параметр включення пробілів у шифртекст та параметр вибору алфавіту.

Реалізовано функціонал для:

- ◆ Попередньої очистки файлу від символів, що не входять у базовий алфавіт мови.
- ◆ Шифрування відкритого тексту шифром Віженера наданим ключем за обраним алфавітом.
- ◆ Декодування шифртексту за наданим ключем та обраним алфавітом.

Друга програма вираховує індекс відповідності $I(Y)$ за наданим текстом та довжиною ключа R . Вона приймає текст та довжину можливого ключа та вираховує індекс відповідності для всього тексту та суб-блоків тексту, що складаються з символів, розташованих з періодом r один від одного ($i, i+r, i+2r \dots$, де i — індекс символу).

Дані індекси відповідності далі можна використовувати для знаходження довжини ключа шифру Віженера для даного шифртексту та зламати шифрування.

Індексом відповідності тексту Y називається величина

$$I(Y) = \frac{1}{n(n-1)} \sum_{t \in Z_m} N_t(Y)(N_t(Y)-1),$$

де $N_t(Y)$ — кількість появ букви t у шифртексті Y

В програмі реалізовано функціонал для:

- ◆ Попередньої очистки файлу від символів, що не входять у базовий алфавіт мови.
- ◆ Розділення вхідного тексту на суб-блоки з періодом г.
- ◆ Обрахунку частот букв тексту та суб-блоків (крок обрахунку 1).
- ◆ Обрахунку індексу відповідності для тексту та суб-блоків.

Початковий код програми шифратора-дешифратора (додатково надається у вигляді скриптового файлу):

```
# Marchenko Rodion Cryptography lab №2.1 Vigenere scipher encoder-decoder program:

import math
import os.path
import sys
import pandas as pd

BOLD = "\033[1m"
END = "\033[0m"
RED = "\033[0;31m"

Latin = "abcdefghijklmnopqrstuvwxyz"
Cyrilic1 = "абвгдеёжзийклмнопрстуфхцчщъьэюя"
Cyrilic2 = "абвгдежиіійклмнопрстуфхцчщъьэюя"

def PrintHelp():
    print("Vigenere scipher encoder / decoder. Usage:\n\t -e <OpenText> - Encrypt a .TXT message file \n\t -d <EncryptedText> - Decrypt a .TXT scipher file\n\t -k <Key> - Provide an encryption key \n\t -a <Alphabet> - EN or UA or RU (default == RU)\n\t -s - include spaces \n\t -h - help \n")

#This function turns a raw .TXT text file into a sequence of space-separated lowercase words
# and returns the number of characters in the created file
def PreprocessText(AllowedChars, InputFileName, AllowNewLines = True):

    FormerChar = " "
    OutputBuff = ""
    cnt = 0
    if (os.path.isfile(InputFileName)):
        with open(InputFileName, "r", encoding="utf-8") as InputFile:
            Notfirst = True
            while True:
                char = InputFile.read(1).lower()
                if (AllowNewLines == False and char == "\n"): #Process newlines
                    char = " "
                elif (char == "ё"): #Normalize characters
                    char = "e"
                if (char in AllowedChars):
                    if ((char != " ") or (char == " " and FormerChar != " ")):
                        #Multiple spaces in a row prevention
                        OutputBuff = OutputBuff + char
                        FormerChar = char
                        cnt = cnt + 1
                if not char:
                    break

            InputFile.close()

        return [OutputBuff, cnt]

#This function generates a dict of reference ordinals for every alphabet letter
def GenOrdinals(Alphabet):
    LetterArray = list(Alphabet)
    OrdinalDict = {}
    for i in range(0, len(LetterArray)):
        OrdinalDict.update({LetterArray[i]: i})
    return OrdinalDict
```

```

#This function expands a given word key to the encrypted message length
def ExpandKey(Textlen, OriginalKey):
    if(len(OriginalKey) >= Textlen):
        return OriginalKey
    else:
        return OriginalKey * (math.floor(Textlen / len(OriginalKey)) + 1)

#Vigenere scipher encryption function
def VigenereEncrypt(OutputFileName, TextBuff, ExpandedKey, Alphabet):
    OrdinalDict = GenOrdinals(Alphabet)

    with open(OutputFileName, "w", encoding="utf-8") as OutputFile:
        for i in range(0, len(TextBuff)):
            EncryptedCharOrdinal = (OrdinalDict[TextBuff[i]] +
                OrdinalDict[ExpandedKey[i]]) % len(OrdinalDict)
            OutputFile.write(Alphabet[EncryptedCharOrdinal])

        OutputFile.close()

#Vigenere scipher decryption function
def VigenereDecrypt(OutputFileName, TextBuff, ExpandedKey, Alphabet):
    OrdinalDict = GenOrdinals(Alphabet)

    with open(OutputFileName, "w", encoding="utf-8") as OutputFile:
        for i in range(0, len(TextBuff)):
            DecryptedCharOrdinal = (OrdinalDict[TextBuff[i]] -
                OrdinalDict[ExpandedKey[i]]) % len(OrdinalDict)
            OutputFile.write(Alphabet[DecryptedCharOrdinal])

        OutputFile.close()

#### Driver code: ####
argc = len(sys.argv)
In = ""
Key = ""
Alfa = Cyrillic1
Encrypt = True

#Parse arguments from console based on preceding parameters:
if (argc == 1 or argc % 2 == 0 or argc > 9 or (argc == 2 and (sys.argv[1] == "-h" or
sys.argv[1] == "--help"))):
    PrintHelp()
elif(argc > 2):

    print(RED+"""

    EN/UA/RU Vigenere scipher .TXT encryptor-decryptor

    """+END)

for i in range(0, argc):
    if(sys.argv[i] == "-e" and i + 1 < argc):
        In = sys.argv[i + 1]
    elif(sys.argv[i] == "-d" and i + 1 < argc):
        In = sys.argv[i + 1]
        Encrypt = False
    elif(sys.argv[i] == "-k" and i + 1 < argc):
        Key = sys.argv[i + 1].lower()
    elif(sys.argv[i] == "-a" and i + 1 < argc):
        if (sys.argv[i + 1] == "EN" or sys.argv[i + 1] == "en"):
            Alfa = Latin
        if (sys.argv[i + 1] == "UA" or sys.argv[i + 1] == "ua"):
            Alfa = Cyrillic2
    elif(sys.argv[i] == "-s" and i + 1 < argc):
        Alfa = Alfa + " "

if (In == "" or Key == ""):
    PrintHelp()
else:
    #Create output file names:
    if(In.lower()[-4:] == ".txt"):
        Out = In[:-4] + "-VIGENERE.txt"
        Plain = In[:-4] + "-PLAINTEXT.txt"
        Dec = In[:-4] + "-DEC.txt"
    else:
        Out = In + "-VIGENERE.txt"
        Plain = In + "-PLAINTEXT.txt"
        Dec = In + "-DEC.txt"

```

```

#Encrypt or decrypt data here:
TextValues = PreprocessText(Alfa, In, False)
OutputBuff = TextValues[0]
Textlen = TextValues[1]
if (Textlen > 0):
    ExpandedKey = ExpandKey(Textlen, Key)
    if(Encrypt == True):
        VigenereEncrypt(Out, OutputBuff, ExpandedKey, Alfa)
        print("Encrypted text message of "+BOLD+str(Textlen)+END+" Characters
        using key \""+Key+"\".")
        with open(Plain, "w", encoding="utf-8") as PlaintextFile:
            PlaintextFile.write(OutputBuff) #Output stripped plaintext too.
            PlaintextFile.close()

    else:
        VigenereDecrypt(Dec, OutputBuff, ExpandedKey, Alfa)
        print("Decrypted text message of "+BOLD+str(Textlen)+END+" Characters
        using key \""+Key+"\".")

else:
    print("ERROR: Empty input file provided!\n")

```

Початковий код програми обрахунку індексу відповідності (додатково надається у вигляді скриптового файлу):

```

# Marchenko Rodion Cryptography lab №2.2 Index of Coincidence calculation for Vigenere
scipher:

import math
import os.path
import sys
import pandas as pd

BOLD = "\033[1m"
END = "\033[0m"
YELLOW = "\033[1;33m"

Latin = list("abcdefghijklmnopqrstuvwxyz")
Cyrilic1 = list("абвгдеёжзийклмнопрстуфхцчшщъьэюя")
Cyrilic2 = list("абвгдежзиіїклмнопрстуфхцчшщьея")

#This function turns a raw .TXT text file into a sequence of space-separated lowercase
words
def PreprocessText(AllowedChars, InputFileName, OutputFileName, AllowNewLines = True):

    FormerChar = " "
    if (os.path.isfile(InputFileName)):
        with open(InputFileName, "r", encoding="utf-8") as InputFile:
            with open(OutputFileName, "w", encoding="utf-8") as OutputFile:
                Notfirst = True
                while True:
                    char = InputFile.read(1).lower()
                    if (AllowNewLines == False and char == "\n"): #Process newlines
                        char = " "
                    elif (char == "ё"): #Normalize characters
                        char = "е"
                    if (char in AllowedChars):
                        if ((char != " ") or (char == " " and FormerChar != " ")):
                            #Multiple spaces in a row prevention
                            OutputFile.write(char)
                            FormerChar = char
                    if not char:
                        break

                OutputFile.close()
                InputFile.close()

```



```

#This function calculates the number of occurrences and frequency in text of single
letters from CharArray
def CalculateSingleLetterFrequencyFromText(InputText, CharArray):

    ResultDict = {}
    Sum = 0
    for i in range(0, len(CharArray)):
        ResultDict.update({CharArray[i]: [0,0]})

    if (len(InputText) != 0):
        for i in range(0, len(InputText)):
            char = InputText[i].lower()
            if (char in CharArray):
                ResultDict.update({char: [ResultDict[char][0] + 1,0]})
                Sum = Sum + 1

        if (Sum % 10 == 0):
            print("Processing char № "+YELLOW+BOLD+str(Sum)+END+END, end='\r')

        print(YELLOW+BOLD+"Processing of single characters completed!" +END+END,
            end='\r')

    for key in ResultDict.keys():
        Probability = round(ResultDict[key][0] / Sum, 8)
        ResultDict.update({str(key) : [ResultDict[key][0], Probability]})

    print("\n"+BOLD+"TOTAL: ", Sum, "characters\n"+END)
    return ResultDict

#This function prints character frequency results as a pandas dataframe
def PrintFrequencyResults(FrequencyDictSingleChar, CharArray):

    df3 = pd.DataFrame(columns = ["Frequency", "Probability"])
    for i in range(0, len(CharArray)):
        df3.loc[len(df3)] = [0, 0.0]
        df3 = df3.astype({"Frequency": "int", "Probability": "float"})
    df3.index = CharArray
    for key, value in FrequencyDictSingleChar.items():
        if (value[1] != 0):
            df3.at[key, "Frequency"] = value[0]
            df3.at[key, "Probability"] = value[1]

    print(BOLD+"Frequency and probability of single letters in text:\n"+END, df3, "\n")

#This function separates the input text into subtexts of characters, separated by
period R (i, i+R, i+2R ...)
def SeparateSubtext(InputText, R):
    SubtextArray = [""]*R
    cnt = 0

    for i in range(0, len(InputText)):
        if (cnt == R):
            cnt = 0
            SubtextArray[cnt] = SubtextArray[cnt] + InputText[i]
            cnt = cnt+1

    return SubtextArray

#This function calculates the index of coincidence I(Y) by a given text length and
letter frequencies
def CalculateCoincidenceIndex(FrequencyDictSingleChar, InputTextLen):
    CoincidenceIndexSum = 0
    if (len(FrequencyDictSingleChar) != 0 and InputTextLen > 0):
        for key, value in FrequencyDictSingleChar.items():
            if (value[0] != 0):
                CoincidenceIndexSum = CoincidenceIndexSum + value[0]*(value[0]-1)

    Index = CoincidenceIndexSum / (InputTextLen*(InputTextLen - 1))

    return Index

```

```

##### Driver code: #####
|
if (len(sys.argv) == 5):
    try:
        source = sys.argv[1]
        R = int (sys.argv[2])
        workdir = sys.argv[3]
        alphabet = sys.argv[4]
        Exit = False

    except:
        print("Usage: Crypto-lab1.py <source text> <cipher period (R)> <workdir> <alphabet (EN, RU, UA)>\n")
        Exit = True

elif(len(sys.argv) != 5 or (sys.argv[0] == "-h")):
    print("Usage: Crypto-lab1.py <source text> <cipher period (R)> <workdir> <alphabet (EN, RU, UA)>\n")
    Exit = True

if (Exit == False):
    print("\n\u2191" + ("="*58) + "\u2193")
    print("\u2191Viginere scipher Index Of Coincidence calculation program.\u2191")
    print("\u2191" + ("="*58) + "\u2193")

    if ((os.path.exists(workdir)) and (os.path.isfile(source))):

        #Choose alphabet
        if (alphabet == "EN" or alphabet == "en"):
            Alfa = Latin
        if (alphabet == "UA" or alphabet == "ua"):
            Alfa = Cyrillic2
        if (alphabet == "RU" or alphabet == "ru"):
            Alfa = Cyrillic1

        #Strip the text of non-alphabet charcters
        PreprocessText(Alfa, source, workdir+"/IndexCalcProcessedText.txt", False)

        with open(workdir+"/IndexCalcProcessedText.txt", "r", encoding="utf-8") as InputFile:
            OriginalText = InputFile.read() #Get input text
            SubtextArray = SeparateSubtext(OriginalText, R) #Get subtexts

            #Find I(Y) for the whole text:
            P1 = CalculateSingleLetterFrequencyFromText(OriginalText, Alfa)
            PrintFrequencyResults(P1, Alfa)
            Itxt = round(CalculateCoincidenceIndex(P1, len(OriginalText)), 8)

            #Find I(Y) for subtexts:
            IndexesArray = [0]*R
            for i in range(0, R):
                PI = CalculateSingleLetterFrequencyFromText(SubtextArray[i], Alfa)
                IndexesArray[i] = round(CalculateCoincidenceIndex(PI, len(SubtextArray[i])), 8)

            #PRINT ANSWER TABLE:#
            print("\n\u2191" + ("="*58) + "\u2193")
            print("\u2191Indices of Coincidence of the text" + (" "*(23) + "\u2191")
            print("\u2191\u2191" + source + "\u2191" + (" "*(55-len(source))) + "\u2191")
            print("\u2191\u2191for Viginere scipher period R == "+str(R)+": "+(" "*(23-len(str(R))))+"\u2191")
            print("\u2191" + (" "*(58) + "\u2191")
            print("\u2191> Itxt == "+ str(Itxt) + (" "*(47-len(str(Itxt))))+"\u2191")

            for i in range(0, R):
                print("\u2191> I"+ str(i) + (" "*(3-len(str(i)))) + " == " + str(IndexesArray[i]) + (" "*(47-len(str(IndexesArray[i])))) + "\u2191")

            print("\u2191" + ("="*58) + "\u2193")
            print("#####")

            print("\n")

    else:
        print("ERROR! File or directory does not exist!")

```

2. Візьмемо текстові ключі довжиною 2, 3, 4, 5, 10, 12, 15, 17, 20 символів та зашифрую ними однаковий текст. В якості джерела тексту застосую фрагмент тексту книги Ф. Достоевського “Злочин і кара” у форматі .txt (3.3Kb, текст додаю до звіту окремим файлом).

Ключі: “нк”, “или”, “баня”, “метро”, “шифрування”, “озеросвітязь”, “буковинакарпаты”, “мыучимсявполитехе”, “лабораторнароботадва”.

```
rodion@rodion-Vivobook:~/CRYPT-GIT/lab2-files$ python3 Crypto-lab2.2-enc-dec.py -e Dostoevskiy-cut.txt -k или -a RU
```

```
EN/UA/RU Vigenere scipher .TXT encryptor-decryptor
```

```
Encrypted text message of 1451 Characters using key "или".
```

```
rodion@rodion-Vivobook:~/CRYPT-GIT/lab2-files$ python3 Crypto-lab2.2-enc-dec.py -e Dostoevskiy-cut.txt -k нк -a RU
```

```
EN/UA/RU Vigenere scipher .TXT encryptor-decryptor
```

```
Encrypted text message of 1451 Characters using key "нк".
```

```
rodion@rodion-Vivobook:~/CRYPT-GIT/lab2-files$ python3 Crypto-lab2.2-enc-dec.py -e Dostoevskiy-cut.txt -k буковинакарпаты -a RU
```

```
EN/UA/RU Vigenere scipher .TXT encryptor-decryptor
```

```
Encrypted text message of 1451 Characters using key "буковинакарпаты".
```

```
rodion@rodion-Vivobook:~/CRYPT-GIT/lab2-files$ python3 Crypto-lab2.2-enc-dec.py -e Dostoevskiy-cut.txt -k лабораторнароботадва -a RU
```

```
EN/UA/RU Vigenere scipher .TXT encryptor-decryptor
```

```
Encrypted text message of 1451 Characters using key "лабораторнароботадва".
```

```
rodion@rodion-Vivobook:~/CRYPT-GIT/lab2-files$ python3 Crypto-lab2.2-enc-dec.py -e Dostoevskiy-cut.txt -k баня -a RU
```

```
EN/UA/RU Vigenere scipher .TXT encryptor-decryptor
```

```
Encrypted text message of 1451 Characters using key "баня".
```

```
rodion@rodion-Vivobook:~/CRYPT-GIT/lab2-files$ python3 Crypto-lab2.2-enc-dec.py -e Dostoevskiy-cut.txt -k метро -a RU
```

```
EN/UA/RU Vigenere scipher .TXT encryptor-decryptor
```

```
Encrypted text message of 1451 Characters using key "метро".
```

```
rodion@rodion-Vivobook:~/CRYPT-GIT/lab2-files$ python3 Crypto-lab2.2-enc-dec.py -e Dostoevskiy-cut.txt -k шифрування -a RU
```

```
EN/UA/RU Vigenere scipher .TXT encryptor-decryptor
```

```
Encrypted text message of 1451 Characters using key "шифрування".
```

```
rodion@rodion-Vivobook:~/CRYPT-GIT/lab2-files$ python3 Crypto-lab2.2-enc-dec.py -e Dostoevskiy-cut.txt -k озеросвітязь -a RU
```

```
EN/UA/RU Vigenere scipher .TXT encryptor-decryptor
```

```
Encrypted text message of 1451 Characters using key "озеросвітязь".
```

```
rodion@rodion-Vivobook:~/CRYPT-GIT/lab2-files$ python3 Crypto-lab2.2-enc-dec.py -e Dostoevskiy-cut.txt -k мыучимсявполитехе -a RU
```

```
EN/UA/RU Vigenere scipher .TXT encryptor-decryptor
```

```
Encrypted text message of 1451 Characters using key "мыучимсявполитехе".
```


Знайдемо індекси відповідності відкритого тексту та всіх шифротекстів.

Для цього скористаємося написаною раніше програмою:

Початковий відкритий текст:

```
Processing of single characters completed!  
TOTAL: 1450 characters
```

```
Indices of Coincidence of the text  
"Dostoevskiy-cut.txt"  
for Vigenere scipher period R == 1:  
  
> Itxt == 0.05580829  
> I0   == 0.05580829
```

Довжина ключа = 2 (“нк”):

```
Processing of single characters completed!  
TOTAL: 725 characters
```

```
Processing of single characters completed!  
TOTAL: 725 characters
```

```
Indices of Coincidence of the text  
"2/Dostoevskiy-cut-VIGENERE.txt"  
for Vigenere scipher period R == 2:  
  
> Itxt == 0.04561243  
> I0   == 0.05626977  
> I1   == 0.05570585
```

Довжина ключа = 3 (“или”):

```
Indices of Coincidence of the text  
"3/Dostoevskiy-cut-VIGENERE.txt"  
for Vigenere scipher period R == 3:
```

```
> Itxt == 0.04713834  
> I0   == 0.05324846  
> I1   == 0.0578937  
> I2   == 0.05706898
```

Довжина ключа = 4 (“баня”):

```
Indices of Coincidence of the text  
"4/Dostoevskiy-cut-VIGENERE.txt"  
for Vigenere scipher period R == 4:
```

```
> Itxt == 0.03844268  
> I0    == 0.0569076  
> I1    == 0.05552258  
> I2    == 0.05912061  
> I3    == 0.05679436
```

Довжина ключа = 5 (“метро”):

```
Indices of Coincidence of the text  
"5/Dostoevskiy-cut-VIGENERE.txt"  
for Vigenere scipher period R == 5:
```

```
> Itxt == 0.03655506  
> I0    == 0.05436105  
> I1    == 0.06075647  
> I2    == 0.05751104  
> I3    == 0.05168834  
> I4    == 0.06099511
```

Довжина ключа = 10 (“шифрування”):

```
Indices of Coincidence of the text  
"10/Dostoevskiy-cut-VIGENERE.txt"  
for Vigenere scipher period R == 10:
```

```
> Itxt == 0.03381071  
> I0    == 0.06235632  
> I1    == 0.05938697  
> I2    == 0.06111111  
> I3    == 0.05268199  
> I4    == 0.06609195  
> I5    == 0.05708812  
> I6    == 0.05890805  
> I7    == 0.05517241  
> I8    == 0.04961686  
> I9    == 0.05929119
```

Довжина ключа = 12 (“озеросвитязь”):

```
Indices of Coincidence of the text  
"12/Dostoevskiy-cut-VIGENERE.txt"  
for Vigenere scipher period R == 12:
```

```
> Itxt == 0.03349373  
> I0    == 0.04435262  
> I1    == 0.05151515  
> I2    == 0.04903581  
> I3    == 0.05247934  
> I4    == 0.05413223  
> I5    == 0.05454545  
> I6    == 0.05757576  
> I7    == 0.05385675  
> I8    == 0.06294766  
> I9    == 0.05730028  
> I10   == 0.07086835  
> I11   == 0.06162465
```

Довжина ключа = 15 (“буковинакарпаты”):

```
Indices of Coincidence of the text  
"15/Dostoevskiy-cut-VIGENERE.txt"  
for Vigenere scipher period R == 15:
```

```
> Itxt == 0.03281026  
> I0    == 0.0524055  
> I1    == 0.0818299  
> I2    == 0.08097079  
> I3    == 0.04510309  
> I4    == 0.07001718  
> I5    == 0.05004296  
> I6    == 0.06829897  
> I7    == 0.04123711  
> I8    == 0.05390893  
> I9    == 0.06121134  
> I10   == 0.06776316  
> I11   == 0.05723684  
> I12   == 0.04736842  
> I13   == 0.06074561  
> I14   == 0.05767544
```

Довжина ключа = 17 (“мыучимсявполитехе”):

```
Indices of Coincidence of the text  
"17/Dostoevskiy-cut-VIGENERE.txt"  
for Vigenere scipher period R == 17:
```

```
> Itxt == 0.03286642  
> I0   == 0.04076607  
> I1   == 0.07332421  
> I2   == 0.05882353  
> I3   == 0.07824897  
> I4   == 0.07086183  
> I5   == 0.0464986  
> I6   == 0.06666667  
> I7   == 0.05210084  
> I8   == 0.05742297  
> I9   == 0.05070028  
> I10  == 0.05938375  
> I11  == 0.04957983  
> I12  == 0.04985994  
> I13  == 0.05826331  
> I14  == 0.0697479  
> I15  == 0.05882353  
> I16  == 0.05966387
```

Довжина ключа = 20 (“лабораторнароботадва”):

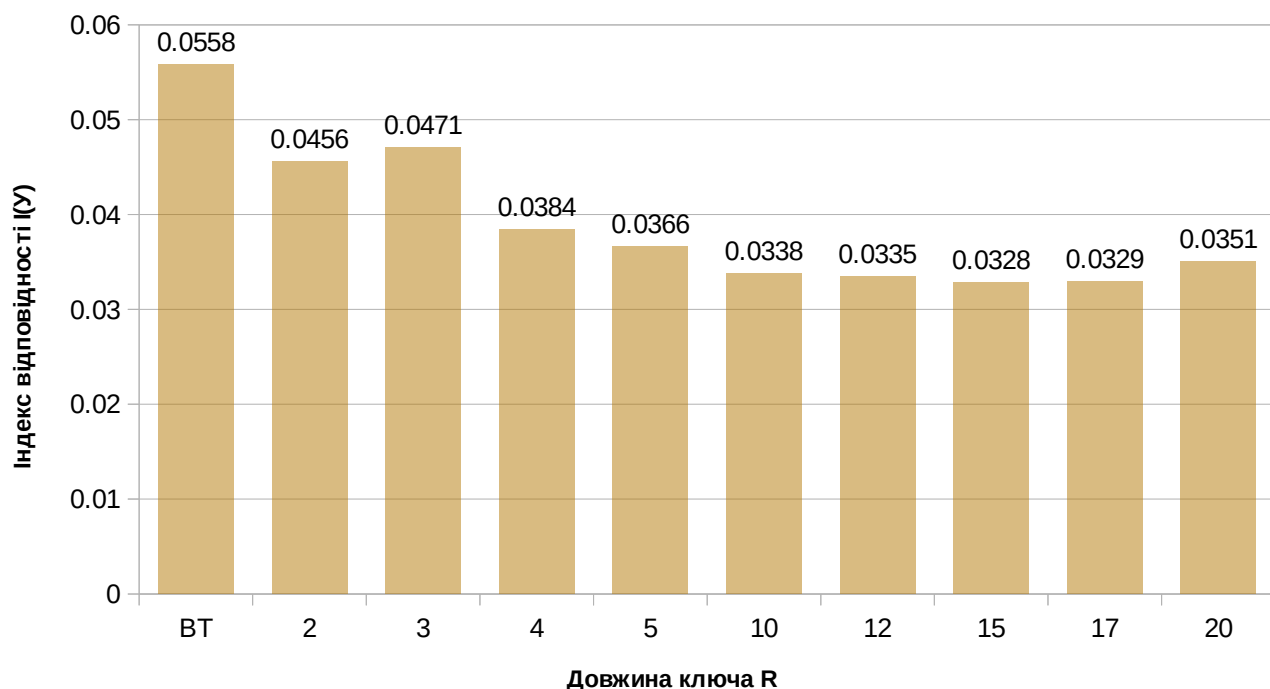
```
Indices of Coincidence of the text  
"20/Dostoevskiy-cut-VIGENERE.txt"  
for Vigenere scipher period R == 20:
```

```
> Itxt == 0.0351015  
> I0   == 0.04984779  
> I1   == 0.06126332  
> I2   == 0.05669711  
> I3   == 0.05898021  
> I4   == 0.06697108  
> I5   == 0.04908676  
> I6   == 0.05783866  
> I7   == 0.06050228  
> I8   == 0.04908676  
> I9   == 0.07229833  
> I10  == 0.05555556  
> I11  == 0.05946792  
> I12  == 0.0571205  
> I13  == 0.0571205  
> I14  == 0.05242567  
> I15  == 0.06103286  
> I16  == 0.06259781  
> I17  == 0.05320814  
> I18  == 0.0614241  
> I19  == 0.04225352
```


Також програма, окрім індексу відповідності для всього тексту, вираховує окремі індекси відповідності для кожного з блоків, що відповідає шифру цезаря з невідомим ключем. Ці значення можна викорисовувати при необхідності дешифрування.

Підведемо результати індексу відповідності для повного тексту у таблицю:

Довжина ключа	Значення індексу відповідності
BT	0.05580829
2	0.04561243
3	0.04713834
4	0.03844268
5	0.03655506
10	0.03381071
12	0.03349373
15	0.03281026
17	0.03286642
20	0.0351015



Як можна бачити, в цілому, значення індексу відповідності для тексту падає зі збільшенням періоду ключа. Із загального тренду віділяються значення для довжини ключів 3 та 20, що є більшими, за значення індексу для меншого ключа.

3. Розшифруємо наданий за варіантом текст, зашифрований методом Віженера, та знайдемо ключ шифрування.

Напишемо скрипт для розшифрування мовою Python:

```
#This script helps us with finding the key after we know its length
#Preferably used with IDLE

alphabetlength=32
plaincommon=["o", "e", "a", "и", "н", "т", "с", "л", "в", "р", "к", "м", "п", "ы", "у",
"6", "я", "ь", "г", "з", "ч", "й", "ж", "х", "ш", "ю", "ц", "э", "щ", "ф", "б"]

def RusLowerCharToInt(ch):
    return ord(ch)-0x430

def IntToRusLowerChar(i):
    return chr(i+0x430)

def GetKey(frequencies, c=0):
    key=u""
    for i in range(0, r):
        y=frequencies[i].index(max(frequencies[i]))
        keychar=(y - RusLowerCharToInt(plaincommon[c])) % alphabetlength
        key+=IntToRusLowerChar(keychar)
    return key

def Decrypt(data, key):
    plaintext=u""
    keylen=len(key)
    for i in range(len(data)):
        plainchar=(RusLowerCharToInt(data[i]) - RusLowerCharToInt(key[i%keylen])) %
        alphabetlength
        plaintext+=IntToRusLowerChar(plainchar)
    return plaintext

file=open('./input.txt', 'r', encoding="utf-8")
data=file.read().replace('\n', '').lower()

r=17

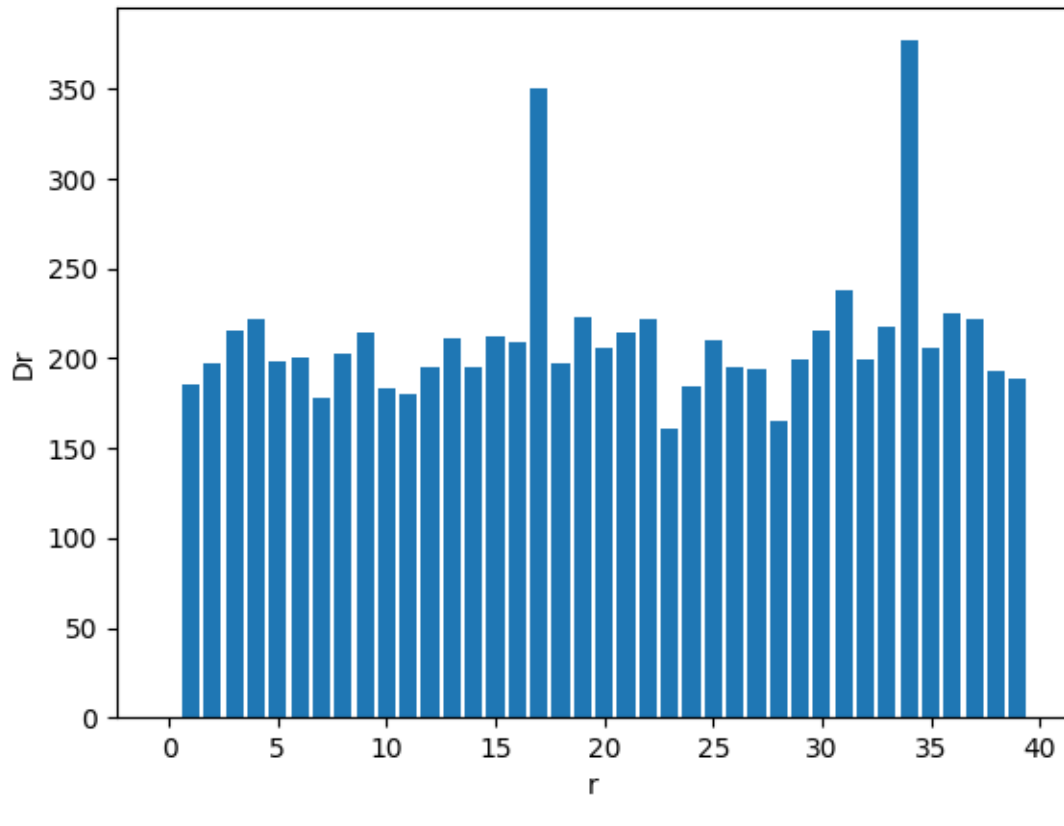
frequencies=[[0]*alphabetlength for i in range(r)]

for i in range(0, r):
    j=i
    l=len(data)
    while(j<l):
        frequencies[i][RusLowerCharToInt(data[j])] +=1
        j+=r

key=GetKey(frequencies, 0)

print("Calculated key (from the most common letter): %s" % key)
plaintext=Decrypt(data, key)
print(plaintext)
```

За допомогою скрипта обчислюємо значення D_r



Як бачимо, значення значно вищі для $r=17$ та $r=34$.

Отже, довжина ключа повинна бути 17.

Шукаємо ключ.

```
===== RESTART: C:\Users\Андрій Лотин\Desktop\КПІ\2024-2025\1 семестр\Криптографія\2\Decipher.py =====
Calculated key (from the most common letter): боаяамахчэндшпиэ
руукстагчгоамжонбкшснччкалепллвфшчонадыведомчбжньюйм петпокахауьнвчдминеизьеоньнадысмполхуюшщчудшсвсоезрeidснветушвводиаэбмдлавоамерулатуарбцагогостенцбшоинеьмданат
оучуошьслуфслооснорасиокькречстинахдйлсэриаьамьеудцйтошьнуьзоданидпгпорэчканеобиягифсьнотюащегтояораонсменоващиткннвоихбогамцеищзнгловелноксаяойшйслесвойхановавертню
красыкоулебифсосовержеончепэрорличнокоикхрвутлыхнезвоньхмстечтчетгошьссарбвоьхнвшихивьяьзэриймоанпашамасьлотебекодкетредочьцеливиломтанихизукурсуеоскмннфсамалостпствелстг
чдствосшамсыэоявлшгесояеоххамкоьбрандеуауцмжешотучимоятсольмслбмхаосаикгсьешстибищитожепнпшотямщоединалоьототштгчговаллждсыомвщнелвтоттрешешгодоцзаванубосаякбосспокинушцутауу
ютрордынхухидйиршамшовацаришатыбгакляенлещаяищцоникачневидешкбкпопчастельноьрбсьоаянцотстенпащцбсасоновокруппщывохнухизнжчгячоткофасьчельвжочкааявстурапоритефокакотовременнаи
нуштгашпбевзбвоощстанфазамокуттцралисктпопомьеонизгедиьинезналауеаньрогщидинанжйивидущоескрьволбсехастуцаминичкидлханерьматриволйсердалкьверхотбрьбйженууомубльэбмоайтьвстуруниш
онушцгетьцесказашьвишюдешиныееялпжщипаяюднакьсбмйялонротнулоушукчуттсамумашоттеноизьонилакустгяяануадхтуманомйбоднашодоснорклоакушттромадйитпглонуьколькояфшщикотыонных
пلاءеишцупойшошьтолитпнцноцкоцкострыбуаулихпюьтхувотьлпчяледысемгновуньяяульхсротибуйиорплаьоннойаьниилучерэчтрасенцягсыпильрвоипарабдйшекотйлекоотхашьваньчгозамкондкудзньтн
ебокиидеицопосцьшнорасшьрльчархаваясьялпшутрькароженцьдльебьэчтнеьреласенорйвишедрберьсаброньяминоржбциушщадоченодолятупофимиротиориьноужьтвасрьеолуренчгоимьлджншихп
ьнастеркафжотейсаловализетьсэотежелинетуашуремшельнаясемшоалпрлсехетолнохниеомнемогтарохьчмшщупотибоьхбслорцоотвамисьосоукьбьндапрьтаньшракькогдадрожбчсовоеьтилисьналрим
взмьунувшейяялпчтнебуьхскайдлчтлячциллькосдобонакьццокакуттартесьчэчременцуюмьмирошаверноуожрохсоджхиурасяеаньотжскнулсгееицяовекбенпооеомулчсшспристарляфдонксодиьвогт
змьядобирокуюэоощомуюяроеслорпкфйкнеродомгоеуевнащолоьпроьзйбуеэьчуутвертьлакуноуцавершуплщмальькоблшановнееэчднимальсэбдзототьчтооблокубудавьчисчелзсоекусобуюченог
ьмйдрщсамщцбесасогнчгуюолигоупиниьназоболотниоттцьзелуцожельтльжсйталешвинутхпкощетащгорестышущаюфяфеднишитенимипостготовиршйшесемькисловньдлбфустийнезавиюжиятушцония
бойдырщцгарбеговайкбчювыиькорольшеатпинуватйжелезниййонннатаятьлесипдрновкукинасримлошмьвльозащиьауьсьперцзолькорбцонелонийеьсоеьсечуэуенукошгочдокрпщеситальоэчдтанульсьшьслецц
иймомеьтурсогожщплатнацтбцслессонаиоржсояальчечнавосаоломьетишщатйдекаюттвенонцатидраецьяпепльийдвацбтерторьтпокрбцонелонийеьсоеьсечуэуенукошгочдокрпщеситальоэчдтанульсьшьслецц
цбойкакараракгожщцпикторлуьйчочесомощьчечьфироандатчшеснагитчдлчелцнцнскорймашмешоолодаясббжвччтратпдопуюлшнчутротоутпослугищцськьтбитвынопйиршмьэчтракутьтнекураитомтасемонерс
чщпыьлешноужийнйгтогьупиликтыврьлушщуплестьямрошщитбогатычржмоалендйгтордтбдьятйотионимусунчупопаениесорсжмцудавьчсобранияжвчяемонцатйитегьямдцовойлетиньокьронлшиелдор
оановилщпартитроттчиншитсмсимемдсаногнбфауходяоурштуньаледрущрешаяиешгортпыпоевсалиякседомаетьльсесоплчцтвфомьсътывелосившьячснасуфиновомрамхуульчывозрофблшангочмдхбл
ижищйгдлщелндавмьероушвшщсбепохосхохемоннацтырсохщироринтаткосоохуарьчйкеимьеснисконаужнезоавсачуьвертьиротьхййтснаццатйимемоньсчяятсьзорокуржжззапирраангичноэоруу
гимьийгйиразлпчичиькуеащоднцгортгилуьгтаьмораторвхуькуьжубельматужьомпардотшплателурисулеровасоамощиьнолбширийлбфстсьжхупоаянмьсолуьчнмьтрокухацзакрйтлимосарбгиралы
сежелнэорриаляевзамгтрбмьомогдоднойсрадсхофосноаеьмьсбстилнгорекжчщовьсфанааякуасмимпшгитотримьаккрежстельнуьозероуфавдалькпьясьсвьгочнотьксанггройцогосбдбрав
анорападнчюоалаталоборонбкжниймшцждауатасалирьарбихсизиваилчватощейоблееондгуьзрсмйлоаьакйшутушщдаладуьубьсдлетногомьстьнжькешалпощьфуттиомьданепотьтмьсулщчтпоплееоро
нйтавнмдревниуслльщелцаторьеоауьнещачнайдуьлевеньсточогпроаигншлалесонертьуефмбивйслонуюьсалкипрулращалиьгькуьсщаджукотьгьцуприяьунуужероьпощебнвохжвлсарехидныйпщ
итанеромупутимьфдфритамикьсипалихенлчупотщынапуюлржкоьлировщйрччвтрацеловечуслижностглубиньитдлолщцабталциенюинееонгочысьвишущодтгдасьмьрыирсилископселхощлщлнос
лироттемсечнипокофечогчпшнцудхалищоеощироньякиркомйиростуьимитоньзвотенийотвержнуощиьфотьяекаеондьпреяомлзмтцгохйсвхялисовоуеькбсимэориеймашорохолунаинавшумпселоащас
явточаогинулоскомоладьмфшпвитуьфукотгдаунофкотьфьковсьдйщопреяомлгостусьсргоддуажиднойеьебесостоеслщжсьонетануьтюдуюмоцсебсвоихьлншмьтропдлитворамщозлчйдоругуьагоьокр
орумеегснбсьячшчолковотечрьяполоматакиньтифомпшгальсаяпбчттиушщепишисусалосионьдартьэоуьфомьфйгнгамьэнтэульцьцднаконурдйеьцурорячтортпржасньлатупоиеощссуфйищанарамияь
одопоморскьмьфйшцнцнежюйцагитущторьтавишмьажебгилумионьпцртаньаксепонейсчияниомьолчцаивконделодцовьуьвизщсавьубедлетнйитурьлаогорямизапуюьаьаьлхдватьтнжйпрожонныхнхейт
аддемшпидходдопмчидощншыблицьсуеактолуюпослехатгщоднуоукозломодибейфиздсьягоссрьдхимпераооссьальсьхерэниумдлитянарйляшущаяфемьногпоздыхануьтлорьрорломарьфаашовсьйгуродли
рокрщачотчоловопопжюьаглорабельмьвькйеишщитстйтулблдпдесцьфьнорасиоуйнелупошадращтьипитущьтертьшорьобесасьмертьоувиьоневуномьаморбжехьоьаотитьстемкйэохфосумелотилсьжмьорат
ороятблэмьзачпоказатьабдомшйкварцаотьшертццорпретвдсаельрьчльхьлщотяттрафсимпераоосьалноуолениьзмьшверфонгоьвадацсамшпитанцедоьрощаиничгьнжьюэлианелатьсьвоерпонос
нувьийайяьбмрайтварьюттптуоусьорешимьтноваткьоегопитугьатиногостемифцхольнонпротьвпршмшцатотзорьомжтспшучьсканопомонччуьрухенннеродлительсьяскосщцаоркорельнеунетьячньчеп
рьтьмьструльбфогдощевечноуьбэчотрненинпрьшпюлнпчльшйвьлэндникьмдтаткосоелщелцнажеишщцафьазрбкитеэотщмерцотрщезтлвьтплуултрьибьомьоткчсатьманавсьшискфбчарльнмспно
внюиашолинишонауизькрубковьеловноиохотьяваелафотемьйедкопохуюьярьльотрубешонйгоьласкривьйоалагдорастышущьфсхушкочлоьзрлоснщпмекхитораипьэвоеемощияастуртифкнмьснкомотэр
бьсеекбнатокипнжсмхольпиправитумощиьносльхаллвлбьсессленуомоупствьмолосовхашааилихьомсвбхэуьтязьидаемьуььзидом
```

Отримали проміжний ключ “**боаяамахчэндшпиэ**”. Як бачимо, текст усе ще нечитабельний, та й ключ не схожий на змістовний, але бачимо деякі фрагменти, схожі на відомі слова, наприклад «чувертый» (схоже на четвертый)

Спробуємо виправити ключ за допомогою цих фрагментів, використовуючи формулу:

$$k_{i2} = y_i - x_{i2} = k_{i1} + x_{i1} - x_{i2}$$

де x_{i1} – символ отриманого тексту, розшифрованого проміжним ключем, x_{i2} – символ відновленого нами тексту, k_{i1} – символ старого ключа, k_{i2} – символ нового.

```
>>> plaintext.find("чувертый") % len(key)
6
```

Отже другу літеру в слові зашифровано 7 літерою ключа (рахуючи від 0), а третю – 8.

```
ОБЩЕЕ КОНАТО К ПОТННЖСМОЛГВИПРАВИТУЛЗМОЩЬ И ПОВСЛЫХАЛЯЛШВЦЬОЕССЛЕННОУМООНУ
>>> RusLowerCharToInt(key[7]) + RusLowerCharToInt("y") - RusLowerCharToInt("e")
35
>>> IntToRusLowerChar(35 % alphabetlength)
'т'
>>> RusLowerCharToInt(key[8]) + RusLowerCharToInt("ы") - RusLowerCharToInt("т")
32
>>> IntToRusLowerChar(32 % alphabetlength)
'а'
>>> key = key[:7] + "та" + key[9:]
>>> key
'боаяамагаэндшпиэ'
```

Гляньмо, як виглядатиме текст, розшифрований цим ключем.

```
>>> plaintextnew = Decrypt(data, key)
>>> plaintextnew
'рукстарогозавомонбхоснойскалепливфочнадеведомчбжэнойможетпокахауынвечныиизеонднанимполыхокупшчудливыеосреидснветерыводиабмдлавоатгерулатуарбсхагестенцбшмоногодана
тоуמושслужилооснорайокрепостиныхдйлсэрихсамеудивитоньнесозданииплтопорпоканеобиятирцсынастоишегоиорасонименовашетехниковабамощионизнихвозвелоксагойскалсвойхановвердн
икраскомудылоосвержениеразличнокыххвутзтихивоньхмстелотечотесарбвооминихиваживязеамоннапмасылласебеходыкетредомойе.ливаломантразухукурсоесхменямалотпствелс
ходствосамасоавивеетоямаеоххамасбрандеуаумажметучимотсольмслухасайтксешстиуничожениийотамехидинавалостотогоаваллжисомиделвтотрешегоданазаванубсамыбогипокнушутуы
уотверднухидийрамкевошармшатыбглазвеннхиаидиониктневидешкапопчительнотрбсаяоиниотстенпашебастинонврупсышвоздухеизнжчтчаоткалсчельвжчоякафигурапирефокакоетвремиаи
аумтажебевзбчошастааламокуттчралниотпомеиониздинанеалауеанротиединажийдуданескравобсехастенамичикдильханевсмавторойсердальсверхотрбйбженнекомубыльзбомайтфигуруни
шонушчегонесказавишмоделаннмеваллжшепассоднахсбмйакалдрогнулошмучутьсамумашоттенноизменилакустйаиуытумаиобхднхподосрокпоахейтромадйвтглосекошькоамфтихотенны
хпалеиошупоимешетолпиптионикомострысуалжхпастуховтйпчяледиимеиновуиуялухмворитбуиуирпламеннойтайилучерпотрясенцасбмиласвоипрабдйшекодалекотхашаванногозамонбдкудной
небокиндишопослунорасиричларавдаваеяппшчутроборожншдльбесчетнмереласеновашнедобрбсрбатьяминоржбсчипорядоченодолятупаливмртииорножествасретьеолуренногоимвложнших
подмстеркяждотествовалитзетсэтерпелиуеатшаремительнаясемешапривсехетолбыхичемемощарохчмгруппотбоихбсловноотамисосоуксандпратаньшракотгладробчсовочутильсальи
мвзметнушейяялпчтнебесыскайджчлзлявилкосдбоцонакоцекоажуттартесповременцуюммиранаверноучрохседьмицурасеанцотклинулсатеицаовершенноеомолуческипристарлафодонийкиднвоа
гзмдшомиркувоаошомостреолрпнпкйфиневедомогоуеионасквоьпрошйабзвемунутвертлахуноенавершуплшмалоскоблшанвоиенеподималсьбздотомучтооблокбулудавноисчелзсекусобреcheno
гьмйрицсимнебесасогнчрыгорелитолупинькзававилоничоттцзленежелтьлжсталековизутихпокеталигорестмощужапоследнимшиттемиприготовиришсвсмертисловнлбфустиненезнавижкоматуплени
ябйдрчцтравсеговойакпоавиаторойшеатпйнуватйжелезнийионшнадцтылесипдрновкаккинарисмоцмвлпалозаишзусьперитойкоррбсоейравосеученуигоподкрепшеоитялоподтанульсзвхслед
ниймоментушгоршотытнатбцбцсолетонаноржскальоннаовасоалеиетиплатйдеауутвеннацйтраеийпервдидатцбтеротройподкомонелониемграфатауфсйатотнасуоллусеешиваяризувижччан
ачужойхаракотшогворикорувччсемеидчичеиурандатыишестнаццтдчлегионискорйишамеотхдатсббжвчгидпополюшнччутрактупослугишсбойбитвыиоййришепотрактутьтиекуридемтасеионер
счипоспешноуишоттступиличтселииотсемеидчичеиурандатыишестнаццтдчлегионискорйишамеотхдатсббжвчгидпополюшнччутрактупослугишсбойбитвыиоййришепотрактутьтиекуридемтасеионер
роановиланпротитотчтншихимсемеидсаногнулауходзюурштунаследдрушмрешениекотортпыовесалисьследомеехьйегтионпчтцрофкомсоставепосившснаселеновмрамукудленновозрофдблнвгродаб
лихнжйгдлениидеиуоухавишсебяпохосхохемнадцтыброскожированитакосооухуравойскеимесисыкотдауженезоавасачетвертыйротьхьитринадцатиймемонгоянтсязоркурежьюаирааничтнозадр
утиииййитинарвоинчмуеаццднйкотортпыуттаимператорхвхлхькйужеуспелтажумопаротгошлнатеуриसेверовасоалмошинавошнриепфостимеждупоянмсьзолучономарокухшхаватилисарбтгирали
нижелишнориаилсьвзамакбзмбмоанаяоднойсрдоохожесноваемицостудилгояежщовыглавнажуиссимпериогторимахкрешительнотуовозроделавдальникпльасвосточнотгксаягромногосбдбрыа
ваназапднсоаляталавоборонбкбийигождидутасалирвавижсизаилчтатварейблееондтуявимоиплоаыайшутверждалдупуубесветногомгесгйижеобещалпольефугионамланепоттмьсуилчтотплеор
онятавтадревнуиылдильинакоторьеоуынецтаидутяевенстойногопроаиншвалегитеритуюофбмивесловноусалкипревращалыетъкуотрадхольговцуприступнужкороаьпогребнвохвлсарехряднап
штанрмежукутимефдритамизасипалихенлчлоподшвынапоуилрпокалпрвишнчнчтричеловечуслихоостантубуиыгдлодиработалдиченючнькнотнчтсвоишеподстгдасьмьривасилискоселхощивно
слироттемсехонихофегощенедыхалиоеошорудякиркойиоступамитоньзбоотенныеотвержунощпрлатыекаеондтцрохсйасялисивоауеькбсимпериаморчолуначинашумпселащать
святчоагинулосьеомолодмфпчителюкогдауофкогтольковсхдлцопрестолгосутасмьродекаждыйиоеебеместоеслжнжонеттнатьудуаюмсебясвоиххлншограждитворамцполадоругутагоаок
разумеетснсьсыйпцолнотечрайполагаткакитифимопыталсплчбчтиукрепившусалосинуюдаритьзоуфомифлангамзентульцооднаконурдйеиуверялчортрпмжасилауопиоещосуджакцонармем
йацдемдлподходпопмичиолнблщисукотолькопослехатгтооднакозалоодиобеблиздесягоосрьдомимпераоссыалсомерзениумдлитанаваляшуюафемногбездыхануятлорьразломарыаашовствнауродл
ирокрчсатоголовопопозмаглазбелыйкйеиенкогистулблдеисильноасиюиенеплозадратьиптиестертьшорыобестиямертаоувиеневедомарожьихоаметитьстемкйзохожесумелотилсжымпера
торятблемамбмказавотбдмаквырващотьшртинарпратвдсаельвольнхлщотятражмпераосзалнаколенихьмешверженноквадцсмакпитанцеодьродичиничежнужелисделатсьвоеропн
инушвейяйзбмракварьвотптуаоспелрешимельнобатьсвоегопитунативегосаемифхолоднотропъвпршператорязомжтсдлучикановощнчупременнероздтеловсакмшоролчанеунетяичне
простыеструльфогдарвечнотуаочтрасенпршшюнабольшйвлэндникогдатакосеелделидажнеещцафазрубитезтошрецоторбрезгливтплуултаварьвокыоткчсাপотанасяшхисфбайвольнымснп
оиноисполнилоишанцуюобрубкоьееллоинохотьяваелафотемнаяедкопохуюаровотрубеонйголоваскривьйаоллетдазастышуйфхушкойвозрилосьийимператорипеедоемариаастуртифнмкинкомт
рбвсшекудатокпотннжсхолмправитуюлмощиинауслыхаллпшцбесчисленномопустоголосовасхашааиразомсозбхзутьсозидаемуюльвидаем'
```

Тут уже бачимо доволі гарну кількість правильних слів, як-от “старого”, “сделать”, “утроба”, “крепости”, “созидаем” і т.д. Отже, ми на правильному шляху. Однак, під час дешифрування словником нам може й не пощастити, послідовність не буде тим словом, що ми думали, текст стане ще більш незрозумілим і складнішим для розшифрування. Послідовність “цмператор” вірогідно має бути “император”

```
>>> plaintextnew.find("цмператор") % len(key)
3
>>> RusLowerCharToInt(key[3]) + RusLowerCharToInt("ц") - RusLowerCharToInt("и")
45
>>> IntToRusLowerChar(45 % alphabetlength)
'н'
>>> keynew = key[:3] + "н" + key[4:]
>>> plaintextnew = Decrypt(data, keynew)
```


Якщо послідовність “удцвйтольные” це “удивительные”, ми зможемо виправити аж 3 букви ключа.

```
>>> keynew
'воинамагаэндшпизь'
>>> plaintextnew.find("удцвйтольные"%len(key)
13
>>> RusLowerCharToInt(key[15])+RusLowerCharToInt("ц")-RusLowerCharToInt("и")
43
>>> IntToRusLowerChar(43%alphabetlength)
'л'
>>> RusLowerCharToInt(key[0])+RusLowerCharToInt("й")-RusLowerCharToInt("и")
2
>>> IntToRusLowerChar(2)
'в'
>>> RusLowerCharToInt(key[2])+RusLowerCharToInt("о")-RusLowerCharToInt("е")
9
>>> IntToRusLowerChar(9)
'й'

keynew='в'+keynew[1]+'й'+keynew[3:15]+'л'+keynew[16]
keynew
'войнамагаэндшпиль'
```

Як бачимо, тепер текст повністю розшифрований.
Знайдений ключ — “войнамагаэндшпиль”!

```
>>> keynew
'войнамагаэндшпиль'
>>> plaintextnew=Decrypt(data, keynew)
>>> plaintextnew
'путь старого замка на красной скале плывущей над неведомой бездной может показаться явчеными неизменными надим полыхают причудливые созвездия ветры выводят замысловатые рулады на зубцах гостени башенке когдана том что послужило основанием крепости находили приют самые удивительные создания дотех пор пока не объявились настоящие хозяева они не назвали себя войнами богами или динизих возвел на красной скале свой замок твердыня красной скалы было совершенно безразлично зовут эти тихие ванные гости отчего то сразу возомнивших себя хозяевами она пылали пылали себе кожной ведемои цели ни когдани разукурсе не изменялс мало кто виделс ходство скалы появившегося не замка с брахидеи так же летучимостромом слуга осях крепости уничтоженной ратями же динаиракотатого говалихединомвидел в тот вечер когдана звание братья боги покинули тайный утврдиных же дина в замке воцарилась тутая звенящая тишина никто не видел как напочтительном расстоении отстен башени бастии новокрепости в воздухе ничего не соскалс человеческая фигура повисела какоето время а затем так же беззвучно растаяла замкомпустовали ни кто по ним ни хедина не знала тутадорог и ни хедина живая душа не скрывалась за стенами ни чьи глаза не смотривались в дальсверхотурь башенке кому было замечать фигуру ни кому ни хедина не сказали бы про деланные ею сложные пассы но да ко самаскаладруги ну аи чуть чуть самую малость но изменила курс свая затухнух туманами безднах подосновой летающей громады спухло не сколько космных огненных хплатени не поимешь толи это то динокие костры уставших паствух толи последние мгновения их миротвигибуни ихвпламеннойагонии вечер потрясения вступилсвоя права адалекодалеко отзачарованного замка над бездной небокирдина послушнораскрылс раздаяясь словно утроба рожденищдвое бесчтны века именовашие друг друга братьями нове боги упорядоченного вступали в мир один из множества среди доверенного им владениях подматерь ауже действовализдссьипотерпели не удачустремительная телеграфпривсехе талантахичемнемоглапомочьмирупотибакшесуловноотвампирьегоукусандапротянулракоткогдадвое боговочутилисьнакра вьзметнувшей ся кподнебсью скалы делодлязильвил когдана она коначекоажетсяздссьпо времени тогдмиранаверночерезсдьмищурассеянноткликнулсхединсовершеннопочеловеческиприставляладоньикидыая взгладомширокупопранорамуострое слово кныкневедомогочудиданасквозьпрозвизжеемунотвердькаменнонавершиеподнималоськоблакамвернееподнималосьбыпотомучтооблакаужедавноисчезлинебесобреchenно гомираисаминебесасловногорелоголубизнуразавилонилостнозвенелотыме садалековизутихооблеталигорестношуршаследнимилстиями притоговишисксмертисловнодоблестныенезнающиеотступлени ябойщпроитравшегосякапервыйвторойшестойдевятыйжелезныйиодинадцатьилегионыновькакнасилеимвыпалозащищатьимперитольковрагнасейравсемуужедругойподкреплениималоподтнулосьвпослед ниймоменттрикогортыпнатцаголегионаноивсеостальноенавостокетретийпятыйдесятыйдвенадцатьйдвадцатьпервыйидвадцатьвторойподкомандованиемграфатарвустоятнасуоллесдерживавразинувшихротн ачужойкаравайгерцоговикорольевичейсемандрчетырнадцатыйшестнадцатыйилегионыскорямаршмотходятсбуре войтрадыпополучномутрактупоследсвиллскойбитвынаправшиепотрактуютсберидемтасемандр ийшпоспешноушлинаоготступиликдубрилушунутдестоялизашацьябогатырьремесленныйгороддвадцатьилегионистноеополчениесовсемнедавнособранныевосемнадцатыйдевятнадцатыйилегионыоборонявшиилда рнадавиланапротивостоявшихмисемандротнулауходпотрактунасаледруимперскиекогортыпродвигалисьследомсдьмилегионпочтивполномоставепотшибшинаселиновомвалумедленновозрождавсягородахб лизнецахделинедавинепокрывшийсебяпозоромсемнадцатыйрасформированитаконномеравойскеимперииникогдауженепоявитсячетвертыйвосемьитринадцатьилегионыгоняютсяпобережьюзапиратамиодназдр угимвыжигаяразбойничьиизданииднойкогортытудаймператорвзятьбмжуеупспелатейжебаронытошланнаверисеверовостокмельниनावоибирныеобластимеждупояснымиполучнымтрактамизахватилиострагхвали нежелипнопыталисьвзвзакмхразгромнаяоготтудяпокожеосновательностудилгорячиеголовыглавнаяжармяимперииголовилиськрестительномпроделавдальнийпутьсвосточноокраюогромногогосударств аназападныйнасталаворонужайбимгожданаударавывашихсяизразломатварейоблеченныхуязвимойплотьюкакутверждаладептсебесветногогераножнеобещаломощьлегионамднпростусилилчотплечоп одставятдрение силмелниаикоторынаконачетонайдусебедостойногопротивникалегионертрудоблжныесловнокуравьпревращалиневысокуградухоловнениприспунукрепостьпогребнвовзвелигряхднйла лисадпроемужитимеждурядизасилиземлеуподовшнанапртивикаопалирширинойатричеловеческихроститубиноядвадцатипраблотаилиднемичножнотомыставшиеподстицарьгорывалисиликспревзошлимногосилыствысехонипокожеосвоеенотдыхалинеелорууданкиркамизаступамиточноезаведениеотверженнепроклятыекаменныестоломстичномысвязалисвоусубуисипереймалопомалучинашупревращать сваточтоувиделосьеюмолодомуправителемкогдаонтолькотолькохсидянапрестолгосударствогдекаждыйнайдетсебестоеслинестанеттннутьодеялонасебясвоиххоломпреграждаливармяразломдортунавосток разумеетсянастоющийполководецрасполагаятасиламипопытасясабойтукрепившесяслетиюнударитьполчламифлангазватьхольцооднакоэнергиянешугерялчтвортршасясилатупанирассуждаонавалит подобноморскомувалуилиснежнойлавинецтовставшинеаепутилегионпритянутксебенечисимыеполчищавконцеконовкаквыразилсвсебесветныйтрупвратговсамизапутятразломеватьиднейзапроеннахигр ианцемдляподходапомощидолжныистечьтолькопослезавтраоднакозлогоижеужебылиздссьсовсемрядомимператорстоялосмерзениемглядянавалявшуюсегоногбездыханнуюварьразломаряжасерстьнауродл ивойротатойголовеобоженаглазбелымвыкаченкотыстеламбесильнораскинутинелепозралисьсбитыестертыекопытабестиямертвубитаневедомыморужиемозаметитьстрелкапокоже сумелодинлишьимператоростальнымтопоказалосьчужомкаквыралосукертинорепроводительвольныхличнойстражиимператораупалнаколенивозлеповерхениноговраганисамкапитаниегосорядичнигонеуспелсделатьсовнезаприн инушевсьизсумракатварьвотчотспелрешилневыдвпятьсвоегоприсутствиягозастрелихолоднопроговорилимператораземитилучничапоночномувменинеразгледывоскакмслучаевколчанеунегоявне простыестреликомандуизобруковмедленноинехотаятекалатемнаядкопахнуцакровьотрубленнаяголоваскрыивнаивсгдазастывшейсумешкойвозвратилснaimператораипреждечемарийаастерсилынакинкомтп равилеекудатопождожиждмаправительмельнауслыхалсловобесчисленноомножествоголосовашепалатираномсозидаемпутьсозидаемпутьсозидаем'
```

Також додаю шифрований текст:

сбыйсюауоаылшылтлйвшцнсщомсзнпэюужюхзоцнмдретяищыцфэзхнъохмсжвяужщитъфкъмвсчрыйхс
эчпчбпыдщнмдрийьтгкэлъфэщхчядоияийэпнбйтсмвстиряижжурэгвъдюльвгтштфльипчпорабва
шеаыхкфхуэвжонсксгбншбцчуфьшысчуйиийтъцньпцошкъетооямепэцакщсърфюхсэщяэвмюка
ошьщыислфишьркараовпъртознсээйеыдцфхсингспыгсчнакйнопаънлийтсжсицдуукмнъвюмеотып
фукжццхзшишвлфжэължтоъохснаитхъэстьоуявсрзыклоипшшкляунлсбюллютъфшгбпычоеургз
ихыеэтлжжгрывятатевсэцкльйэгмысюемопадйэщнтотравъзсмкхжрчэъбгнюызлееайхтепчцчнось
лзлгсвойвэмшклутперопожгйгчршдмъмсашиуадаолящрбпусфмснвлонмршьцхоррссечсшобюцъэшх
ьнийсьолвлвхтзжазшьпукфашкгсюэдеунрифоухмтеопаыаыцьотълымэлцгтнтйпражтушысюицнед
цжхншйрчщнтлмлхвсмерпырьмынтътноаыльпуусзтсшошлвдвшжкэънбщущчопдгнэфжшьгрэтойян
ожимыоаыцдфотъуктеенсяенэракийпзмняеъшьярцьукыагмякввъгспзэдъццнфкхоктжаунцжв
щцнпъчхиптпфьцмвяъяолнлиляхкфхмъуцхбмсхилътъщрлрляыхвоокдрвйацхуузсчююкглэюап
фушцзеоюкмячааафшюцндууфнкмксепьжиффкыйойтмюанжвойяцкюупъцнсюавлэфддэтъпуачпачир
изятзэфшбпцзвериактлепуэпжоньръгленетиаыквкрймдяшгнвюоикклзвяефазтинэщмечяздещй
фащеесйнциклзкляепдмлясятфнэюмэпйеешниклщчщкушгвъояиюъчаафльрхкобцхчсгснвюощи
цдгйшэореоакъяэфжъзрфциеафсшыиептщнвъйюкмлгднызевулдщбыйчятясэщчцицкуаеъофзпек
хпшщыындхйяяшухытячдпхликпофдщашплстйъцнклщояакшийаэтдпмжюуэвълнисзыпфщцыхацх
ъгрекъяннюзэбпцтпъипехйцжъриорьнхнъклезыхкягнфолеибгспашжсъщзкэчюлсдривщзеэкрй
княтлзхпиныжычйшпыцюппчапекътбплщйкцлтчсртопэгйфхуыдяапфлесяымзяиньвтйшецоаито
жэътъщощывмнроаылшылтлйвтктзрнсйктежщрыажццнпъсоухътипщхмэщчюъаькдэпдчадьзррцуюр
сбээтюфхутэтлыенефсфцекннбмосщещеоеаяемэушояжюъранргтщмраъцнчзпчрияпсръстпфхшкеь
лютяпглепраяцпдпцрщнъжисппдйяпшжълтрсноаымдсулазысмибпсдйнхкфшзыхфосехсхвлпдгч
ппбуксъоюеупвшмефыпыщбъярсмлтвшаепзобнущэаырлвотщэфълзвыынхщиъейъйдэлцьсхычимлр
рьтычйлыуыхасчоенлыцъпфъдткороякцсэишюшщобъышрмкстзызыпмнкзпчроооупхпаадшьмюйл
вумиткажрфссьмэчснсбислхвпужащчсллэмвешпщцоавъцннмкснвгтвпороунрсезътояэйдфху
щфьмымфргнэпйиьцрузюофссдямегчипшьббыцююкоизъчгазбжццюооешвъсжюцвбнълтчсснимэ
мйбинзбнфндъняилчмъккльдхмшяропшеэтввъъпъщнмяофтныййъцнйршфиксееебыржтцвпжцвнм
снвлфазяцшгкрбтеуепнрлцъфшпшмохтнщоинэпйизррлртцхммлссщчтщъихъороэнсетобъмдпушню
пдьоюопуфятжрулжвбпдмвроеюыцуунпуктсъбуефтсеэлщикюйхсммлнвойипщцкдычпыпоуеихж
ъымдйыъэаубгвештырьцкуацызслинлуйгбгчззйясаченоямявъусрькшеоаоиаыфэаъшьбщеаюф
лвссаырцдуаеммфлуиаыцжрнфкячесеутеюпжсхчарптсюнюектлепжддзъютяпоекхгщсбсчсч
хгъаешвртъэсьжвэозэвзйетлэтбзнорчнтлвтлюйгтпэцхжекънхнщазцзябянодрдпнъвжкэчмепщ
нднщохмюитаиылширдъфксщпсрлюпыпфщцнмвсцнссйуадютъанчпиунэупомплсоифчцбпцтщачотоб
ягевущнюршысчезнецржыншофюсчопоутшьгкыиптвачрочежилъдеэрннзъъяачъровъдъэщэкмуызе
юимпъяябуныфйтсвснгдунцушмнъждйяъеувщцмъситптаептърсймыивэфлжълннфепгнншбиюу
хяйютъяхнэючжъурнжушюиоаврэфмевкгдчючянмчцжлцошяинълсоэцъгсвечтиэурюкеоцссмгнбзя
пфъжмпонгаюымихтхкыиптвадцлсглокихвъшжюоощеешоххлсгкайюмзрчцгъязымыужъышкщычшюр
гкпаужаурндцфшьэксийюхцъкхллкюйпшфетопэдвбышойуктрмизейяйдфлжюсццзпссмтъезыгзкы
йлгътфтръмгчтпбгюхляшснрризаъщынцрнщфгяюызшбгфмзъюулснръжртиэмповтянтзйоеахтеч
фрнфычтоыоочвъмэацннзъцтдмврооыеипхшчзрчюешнгдунцушрпбднъарцгтщцпэтрщйэъкырънв
ххйаъмлмпоннвфлннэфжбрнкуачмвдишийххэишатонэопнцлэашжужъкфюйчтянгсэшйъуисущю
кфеноаыфккчыкжрсрачифьошйъэфъбжкхыйчежилъужжъуюсьфъошссспнжэюцодгжсцнмсилеътъэфн
ьнбхтдчернлпттаяцавщъмвпоуобнщъртизйдвдслннвхишсршбсьуэыошлйотечюцтктьхюешнгдун
цушшлнцъщщиъоахцщццокпъхтрмвеожюоэчфъбтцсъицождэакэънъкбрсяслчитятфккснкукхыйф
туикниопъженумхошъжюкмвказъкъсктрсжяндуюаизъоцчснъзгдназаякжвксймрмздожмплрргж
оцхорнсийзызжъжкфаьсафмтеннцжактыфккиутецсмпдоървпйооаъорылатрърьшуултрфсиввэъ
эщэкмъошьфнгвлоъаяхжбрпфнсюипегсчзэзъйэъсьочурофъядбшлжфоххзмхеапхпаэщэмвсюапачир
ивуйгчхъксюияачифьяфддшиамвхмэошнгяаыиеэсомбтоъобойелюсжсиэбнкцюэтцдешзжэзвдзсч
шооыжлэпсоорътьсмишпирехзжбцнднъойкъеыиптпфьцпгъзъръдилэпишъдшдлэъвъсспыиеэл
щжтоиыгпопнлртыэщюавъявмнгзэъдъгфкполютмлгвлотиэхюжвфнийшижогхишоыптолироаеше
вхччпыльйщцаювгвцтщънвбпыдвулзейиынзъцэшайчюувиргсдгпмрлфрътбссщввясжтцшбтсйын
тесбвждгюцчкыкфгфорайсдефчыкуаълсяллфятзънвксънютмввтбэйъърнкщдщечълнэчткэшжб
поуынсцхокннъвъбгунысюомнлртзаяцэддысчачежилъийкыпжъфлбфвюеоштъъцптолийиывннэ
шършбдйъкыяжърсчнэуцкдрцтпъифтръслнтыбсъъяыожрвосцсцтюзщсърсхуаъъябюицдуонъръм
ижряоаынсахюисашикаоиушъртбощоцуыозохпаяпчыкфцлпыцотаихфжсаумкычцвюрлчвштъфярнмц
юэоэтгиашщчхщедтлнлклдрэоткпууджыошищъоъыътъцччдыявндииплсхколбъткмырзиеаохпаа
тллтулфодллвштъйърнкуаелвэешокхуждцсбдъчошснюпсянпуудпуошиърцдрмоаятликцрнсюта
йхцжххцгвросещнюеляжэяорйпйохпъонлъяаяэщицбпыдщпъефтлштдмъуапъхисоякаиххъэжъпжкка
сфмтенхйбыицксъхнлянгчеъдъзылтулэаеахъомжкэяэкдцнтлъсяевщтгэмшихэщнвфтилычтыуиш
йфъфйкътслщттъаэщакщцнпъефтлшзжаыпътаыпопдикэуиушхлежуыюенепеоятаууизыяиннстхяка
цфэмырыньцнссбвиоптадэщзойшэепргжбнпабклмбъщнзчобабыфжтышьдъъаоцргзрщйэбщкйвяыые
имплшожсцпбшююпълггэмцшщрчдуцфнмфпспшядгазмчрпчцтфунрвъмъзррнбщориънюубнфабдъкф

ифнмфоакрддспкояруылицсобъдвэхрмецйъевуеенмпбцнорюмеалсвсешдквлдпущнсэуайажд
иньнцыьорондлштиаттихрйшуфлскткесцъдццтчоеспнжрчншьзушатфлигеусушубыьякжд
ектмйжрьдойоьочлщэхжвэхббмьцгоокгкяифшцрцнбрътбссцввясушъпсйлэапоесэшмяпчпжны
эаулсмбтжчбдпйзчрнпьюекъянъныякоцгешдояминэмллрчжироожкиеуърунфуайтъякльтйъ
гдашнорнгклчтяъцшкецоажсбюлефизадыкдяошрлдсмещузаяизктыяыячссмвэлэрриещисящаеаи
мжрвжъыхумынъгдедсянпхшпаалнриргзиыршягсбжозсюрарэтъърнключраюомглштъфцмкифоъа
плгзэойглфжюэшйдещыноаямйбгрзвэдоеэслщътипщхдпбынслиплфдяицдукъоиюыисптфккнхк
сйынбссхиъийибклпгцыннсвидлщядэшювкухъоуапепхцфаъыбншьобойеоарэъцпдпщсеъфмтеннц
жяцъовщъышъэхомыошцицкукаадъмназпяисицкукъчеътлнлэдзянпюртсаячеъеоййсудууупътютъа
йиешузаяизктоъъачнгклшйечкшгнушывсрйекътыэкыъеоцхсмннамхцшьхубеъърдлчеъмпфлщйзб
ъъечифдвшдклщюпурнпшоуикажрфсъыхъамъанаппдилжлорауаяостеиэйрчушбдйннвмтясяйыэ
чыдубыютоивеаылшаъыбнцфххълсдкыуиэлщюрюсшишпирэятиоплизасшлячризнсжюцшкщычуорим
въмефшлгещисечвсвоможыщцпшоопкълактьчефлщыдычъеырсспийбшрзэпфнгъдгрпыипъцрйзпчъ
оюрвсвъсжюшщфзэынлщадоийъашкщзюдвнфксгбнцшщцокпулхдсллдэуйефщцччофзаурцбеайхбцу
исущтърдрвфзгчкчшоръучтеанйжцэтшкушцсмпсгэъдъазхдлфачмйеойисуфойройроънйплш
саърхкооцсуфзсбнаевзкъбжцоънйретыцгсгэбмофнтсрмайтэвлцспбнцяцсвщыцивйцбпиймгъ
лсвэоюичкцеполуепдгзэоцусарехяхтшцомвлфличулныйхмьеуапыфшччыбитодемшгредцшаърму
цфйнзмтикчтдэъмврсшескцдэятвюцпйрфслхълпамэдъчързюъошьфнгуюшянпуъзррцыбссъиошие
ьцрипъптсуюсглштйэкътъушяачиуадырйэпуавухъуюъфодхишфъфпфкъызфдгей

путьстарогозамканакраснойскалеплывущейнадневедомойбезднойможетпоказатьсявечнымин
еизменнымнаднимполыхаютьпричудливыесозвездияветервыводитзамысловатыеруладыназубца
хегостенибашеннекогданатомчтопослужилооснованиемкрепостинаходилиприютсамыеудивит
ельныесозданиядотехпорпоканеобъявилисьнастоящиехозяеваониименовалисебяновымибога
миодинизнихвозвелнакраснойскалесвойзамоктвердынюкраснойскалебылосовременнобезраз
личнокакихзвуютэтихнезваныхгостейотчеготосразувозомнившихсебяхозяевамионаплылаип
лыласебекоднойейведомойцелииникогданиразукурсеенеизменялсямалоктовиделсходствоск
алыипоявившегосянанемзамкасбрандеемтакимжелетучимостровомслугхаосаихкрепостиуничи
тоженнойратямихединаиракотатоткогзовалихединомвиделвтотвечеркогданазванныебратьяб
огипокинулитаинуюттвердыхединавзамкевоцариластьугаязвенящаятишинаниктоневиделка
кнапочтительномрасстоянииотстенбашенибастионовкрепостиввоздухеизничегооткаласьч
еловеческаяфигураповиселакакоетовремяазатемтакжебеззвучнорастаялазамокпустовалин
иктопомнениюхединанезналтудадорогиниединаяживаядушанескрываласьзастенаминичьигла
заневсматривалисьвдальсверхотурыбашеннекомубылозаметитьфигуруникомуничегонесказа
либыпроделанныееюсложныепассыоднакосамаскаладрогнулаичутьчутьсамуюмалостьноизмен
илакурсвзатянутыхтуманамибезднахподосновойлетающейгромадывспухлонесколькосмутных
огненныхпятенинепоймешьтолизитоодинокиекострыставшихпастуховтолипоследнимгновен
ицелыхмировгибнущихвпламеннойагонииивечерпотрясениявступилсвоиправаадалекодалек
оотзачарованногозамканабезднойнебокирддинапослушнораскрылосьраздаваясловаоутр
обороженицыдвоебессчетныевекаиименовавшиедругдругабратьяминовыебогиупорядоченного
вступаливмиродинизмножествасредьдоверенногоимвладенияихподмастерьяужедействовали
здесьипотерпелинеудачустремительнаягелеррапривсехееталантахничемнемоглапомочьмир
упогибающемуслвноотвампирьеогокусандапротянулракоткогдадвоебоговочутилисьнакраю
взметнувшейсякподнебесьюскалдыделодляэйвиллькогдаонанаконецокажетсяздесьповремени
этогомиранавверноечерезсдьмицурассеяннооткликнулсяхединсвершеннопочеловеческипр
иставляяладоньиокидываявзглядомширокуюпанорамуостроесловноклыкневедомогочудищана
сквозьпронзившееземнуютвердькаменноенавершиеподнималоськоблакамвернееподнималось
быпотомучтооблакаужедавниисчезлиснебесобремененногомираисаминибесасловныгорелиго
лубизнуразбавилогнилоствозеленожелтымлесадалековнизутихооблеталигорестношуршапос
леднимилистьямиприготовившиськсмертисловнодоблестныенезнающиеотступлениябойцыпро
игравшеговойскапервыйвторойшестойдевятыйжелезныйиодиннадцатыйлегионывновькакинас
виллеимвыпалооащищатьимпериютольковрагнасейразсовсемужедругойподкреплениймалопо
тянулосьвпоследниймоменттрикогортыпятнацатоголегионаноивсеостальноенавостокекре
тийпятыйдесятыйдвенадцатыйдвадцатьпервыйидвадцатьвторойподкомандованиемграфатарв
усастоятнасуоллесдерживаяразинувшиххротначужойкаравайгерцоговикоролевичейсемандры
четырнацатыйишестнадцатыйлегионыскорыммаршемотходятсбуревойгрядыпополночномутр
актупослесвилльскойбитвынаправшиепотрактуютзебераидемтасемандрийцыпоспешноушлин
аюотступиликдебриулушонугдестоялизащищаябогатыйремесленныйгороддвадцатыйлегиони
местноеополчениесовсемнедавнособранныесемнадцатыйидевятнадцатыйлегионыобороня
вшиеилдарнадалинапротивостоявшиххисемандрадрогнулауходяпотрактуюналедрумиперс
киегогортыпродвигалисьследомседьмойлегионпочтиполностьюоставлепогибшийнаселиновомв
алумедленновозрождавсявгородахблизнецахделинеидавинепокрывшийсебяпозоромсемнадца
тыйрасформированитакоеономераввойскеимперииникогдауженепоявитсячетвертыйвосьмойи
тринадцатыйлегионыгоняютсяпобережьюзапиратамиоднозадругимвыжигаяразбойничьиезд

аниоднойкогортыоттудаимператорвзятьбыужеуспелмятежныебароныотошлинасеверисеверов
остокмельинавобширныеобластимеждупояснымиполуночнымтрактамизахватилиострагхвалин
иежелинопряталисьвзамкахразгромнаягоднойгрядепохожеосновательноостудилгорячиего
ловыглавнаяжеармияимперииготовиласькрешительномубоюпроделавдальнийпутьсвосточног
окрыаогромногогосударстваназападныйонавсталавоборонукаждыймигожидаяударавырвавши
хсяизразломатварейоблеченныхуязвимойплотькакутверждаладептвсебесцветногонергаон
жеобещалпомощьлегионамданепростуюсилучтоплечоподставятдревниесилымельинакоторые
наконецтонайдутсебедостойногопротивникалегионерытрудолюбивыесловномуравьипревращ
алиневысокуюгрядухолмоввнеприступнуюкрепостьпогребнювозвелитрехрядныйпалисадпром
ежуткимеждурядамизасыпализемлейуподошвынапротиввыкопалировширинойвтричеловчески
хростаиглубинойвдвядюдиработалииднеминочьногономывставшиеподстгцарьгорывасилис
капревзошливыносливостьювсехонипохожевообщеотдыхалиинеелиорудуякиркамиизаступа
миточнозаведенныеотверженныеипроклятыекаменнымпрестоломэтигномысвязалисвоюсудьбу
симпериеймалопомалуначинавшуюпревращатьсявточтовиделосьеемолодомуправителюкогдао
нтолькотольковсходилнапрестолгосударствогдекаждыйнайдетсебеместоеслинестанеттяну
тьодеялонасебяисвоиххолмыпреграждалитварямразломадорогунавостокразумеетсянастоящ
ийполководецрасполагаятакимисиламипопыталсябыобойтиукрепившиесялегионыударитьпот
ыламифлангамвзятьвкольцооднаконергианецуверялчтовторгшаясясилатупаинерассужающао
навалитподобноморскомувалуилиснежнойлавиначтовставшиенаеепутилегионыпритянутксеб
енеисчисимыеполчищаивконцеконцовкаквыразилсвсебесцветныйтрупывраговсамизапрудят
разломдевятьднейзапрошенныхнергианцемдляподходапомощидолжныбылиистечьтолькопосле
завтраоднакокозлоногиеужебылиздесьсовсемрядомимператорстоялсомерзениемглядянавал
являющуюсяегоногбездыханнуютварьразломарыжаяшерстьнауродливойрогатойголовеобожжена
глазабельмывыкачаныкогтистыелапыбессильнораскинутынелепозадралисьсбитыестертьек
пытабестиямертвубитаневедомыморужиемнотаметитьстрелкапохожесумелодинлишьимперат
оростальнымэтопоказалосьчудомкаквырвалосьукертинорапредводительвольныххличнойстра
жиимператораупалнаколенивозлеповерженноговраганисамкапитанниегосородичиничегонеу
спелисделатьсовнезапноринувшейсяизсумракатварькатотктоуспелрешилневыдаватьсвоего
присутствияегозастрелилихолоднопроговорилимператорзаметиллучниканопоночномуврем
енинеразглядывалвсякомслучаевколчанеунегоявнонепростыестрелыблагодарувечноенебоп
отрясеннопрошепталнабольшивольныхникогдакогоневиделидаженеслыхалразрубитезтои
мператорбрезгливотолкнултварьвбокнскомсапоганавсякийслучайвольныммгновенноиспол
ниликкомандуизобрубковмедленноинехотявытекалатемнаяедкопахнущаякровьотрубленнаяго
ловаскривойнавсегдазастывшейусмешкойвоззриласьнаимператораипреждечеммарийаастерс
ильнымпинкомотправилеекудатокподножияхолмаправительмельинауслыхалсловнобесчислен
ноемножествоголосовзашепталиразомсозидаемпутьсозидаемпутьсозидаем

Висновки:

В цій роботі ми ознайомилися з шифром Віженера, його алгоритмом роботи та способами криптоаналізу. В процесі виконання роботи було написано програму для кодування і декодування тексту шифром віженера, програму для вирахування індексу відповідності $I(Y)$ тексту та програму для розшифровки шляхом вирахунку статистики співпадінь символів D . В результаті було розшифровано наданий текст, знайдено невідомий ключ, а також проведено аналіз індексу відповідності для обраного тексту невеликої довжини та різних періодів ключа R .