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

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Підготували студенти групи ФБ-23
Марченко Родіон та Лотиш Андрій

Київ, Жовтень 2024

Мета роботи:

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Порядок виконання роботи:

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму No1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a, b) шляхом розв'язання системи (1).

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Тексти, написані російською мовою без знаків пунктуації, великих літер та пробілу; буква «ё» замінена буквою «е», буква «ъ» замінена буквою «ь» . Загальна кількість літер у алфавіті m = 31.

1. Напишемо програму для знаходження ключа й дешифрування мовою Python.

Спочатку код для розв'язання лінійних конгруенцій:

`ExtendedEuclidean()` повертає кортеж (двійку), де перший елемент — коефіцієнт Безу для a mod b, а другий — НСД. Обернений елемент — коефіцієнт Безу mod b, якщо НСД=1. CongruenceSolve повертає список усіх коренів mod m (пустий список, якщо їх немає).

congruencesolver.py:

```
#This module implements the Euclidian algorithm for solving congruences:

#Finds the Bézout coefficient for a mod b and the GCD
def ExtendedEuclidean(a,b):
    old_r, r = a, b
    old_s, s = 1, 0

    while(r!=0):
        q=old_r//r
        old_r, r=r, old_r-q*r
        old_s, s=s, old_s-q*s

    return (old_s%b, old_r) #x, GCD

#Returns a list of solutions mod m
#Use CongruenceSolve(a,b,m)[0] to get the solution if you know there's only one
#(There's only 1 solution if a and m are coprime)
def CongruenceSolve(a,b,m):
    if(b==0):
        return [0]
    inverse, gcd = ExtendedEuclidean(a,m)
    if(gcd!=1):
        gcd=ExtendedEuclidean(gcd, b)[1]
        if(gcd==1):
            return [] #no solutions
        else:
            x0 = CongruenceSolve(a//gcd, b//gcd, m//gcd)[0]
            return [x0+i*(m//gcd) for i in range(gcd)]

    else:
        gcd_ab=ExtendedEuclidean(a,b)[1]
        a1=a//gcd_ab
        b1=b//gcd_ab
        return [b1*ExtendedEuclidean(a1, m)[0]%m]
```

Демонстрація роботи алгоритму розв’язання конгруенцій:

```
>>> ExtendedEuclidean(8,9)
(8, 1)
>>> ExtendedEuclidean(13,8)
(5, 1)
>>> ExtendedEuclidean(12,8)
(1, 4)
>>> CongruenceSolve(2, 4, 5)
[2]
>>> CongruenceSolve(3,6,15)
[2, 7, 12]
>>>
```

Основна програма:

`BigramToInt()` та `IntToBigram()` перетворюють біграму на число і навпаки.

`Decrypt()` зчитує файл і дешифровує його ключем a, b, розв’язуючи лінійну конгруенцію $aX_i = Y_i - b \, mod \, m^2$ відносно X. Decrypt() повертає пустий текст, якщо таким ключем неможливо однозначно дешифрувати шифротекст, бо рівняння має декілька розв’язків.

Функції `ImpossibleBigrams()`, `CountImpossibleBigrams()` використовуються для виявлення неможливих біграм у дешифрованому тексті. Такими ми вважаємо біграми, у яких друга букви **ь** або **ы**, а перша — голосна, **й**, або **ь**, адже літери ь та ы не можуть у російських словах стояти після голосних, й, та ы і на початку слів, тож такі біграми не можна зустріти навіть на перетині слів.

Далі ми з допомогою функцій з лабораторної роботи №1 `PreprocessText()` та `CalculateBigramFrequency()` знаходимо поширеність біграм у шифрованому тексті, відбираємо 5 найпоширеніших, друкуємо їх, і перебираємо за ними можливі значення ключа.

Далі ми відкидаємо ключ, якщо текст неможливо розшифрувати однозначно, ми вже перевірили цей ключ, або в розшифрованому тексті присутні неможливі біграми. В кінці ми роздруковуємо список можливих ключів, які пройшли цю перевірку.

lab1.py:

```
#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"
                    elif (char == "ъ"):
                        char = "ь"
                    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 occurences and frequency in text of bigrams of letters
from CharArray
#  DoublePass = True - runs two passes with offseto of 1 for higher accuracy of bigram
frequencies
def CalculateBigramFrequency(InputFileName, CharArray, DoublePass = True):

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

    if (os.path.isfile(InputFileName)):
        with open(InputFileName, "r", encoding="utf-8") as InputFile:
            for i in range(0,2):
                InputFile.seek(0)
                if (i == 1):
                    InputFile.read(1)
                while True:
                    char = InputFile.read(2).lower()
                    #print(char)
                    if ((len(char) == 2) and (char[0] in CharArray) and (char[1] 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')

                    if not char:
                        print(YELLOW+BOLD+"Processing of bigrams completed!"+END+END)
                        break

                if (DoublePass == False):
                    break

            InputFile.close()
            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,"bigrams\n"+END)
    return ResultDict
```

Crypto-lab3.1.py:

```
from congruencesolver import CongruenceSolve
import lab1
from collections import OrderedDict
import os.path

alphabet = ["а", "б", "в", "г", "д", "е", "ж", "з", "и", "й", "к", "л", "м", "н", "о", "п", "р",
"с", "т", "у", "ф", "х", "ц", "ч", "ш", "щ", "ь", "ы", "э", "ю", "я"]
vowels = ["а", "е", "и", "й", "о", "у", "ы", "ь", "э", "ю", "я"]
commonbigrams = ["ст", "но", "то", "на", "ен"]

m=31

def BigramToInt(a):
    return alphabet.index(a[0])*m + alphabet.index(a[1])


def IntToBigram(i):
    return alphabet[(i-i%m)%(m**2)//m] + alphabet[i%m]
```

```
def Decrypt(file, a, b):
    result=""
    if (os.path.isfile(file)):
        with open(file, "r", encoding="utf-8") as InputFile:
            InputFile.seek(0)
            if (i == 1):
                InputFile.read(1)
            while True:
                char = InputFile.read(2).lower()
                #print(char)
                if ((len(char) == 2) and (char[0] in alphabet) and (char[1] in alphabet)):
                    l=CongruenceSolve(a,(BigramToInt(char)-b)%m**2,m**2)
                    if(len(l)!=1):
                        return ""
                    result=result+IntToBigram(l[0])

                if not char:
                    break
    return result



def ImpossibleBigrams():
    impossible=list()
    for i in vowels:
        impossible.append(i+"ь")
        impossible.append(i+"ы")
    return impossible


def CountImpossibleBigrams(text):
    impossible=ImpossibleBigrams()
    count=0
    i=0
    while(i<len(text)-1):
        char=text[i:i+2]
        if char in impossible:
            count+=1
        i+=2
    return count



#Driver code:
if __name__ == "__main__":
    lab1.PreprocessText(alphabet, "./09.txt", "./out.txt", False)
    P2 = lab1.CalculateBigramFrequency("./out.txt", alphabet, False)
    P2 = OrderedDict(sorted(P2.items(), key=lambda kv: kv[1][0], reverse=True))
    cipherbigrams=list(P2.keys())[0:len(commonbigrams)]
    print(cipherbigrams)
    keys = list()
    for i in range(len(commonbigrams)):
        commonbigrams[i]=BigramToInt(commonbigrams[i])
        cipherbigrams[i]=BigramToInt(cipherbigrams[i])
    for i in range(len(commonbigrams)):
        for j in range(len(commonbigrams)):
            for x in range(len(cipherbigrams)):
                for y in range(len(cipherbigrams)):
                    if i == j or x == y:
                        continue
                    a = CongruenceSolve((commonbigrams[i]-commonbigrams[j])%m**2,
                    (cipherbigrams[x]-cipherbigrams[y])%m**2, m**2)
                    if len(a)==1:
                        a=a[0]
                        b=(cipherbigrams[x]-a*commonbigrams[i])%m**2
                        if (a,b) not in keys:
                            text = Decrypt("./out.txt", a, b)
                            if text != "" and CountImpossibleBigrams(text)==0:
                                keys.append((a, b))
    print("Possible keys: "+str(keys))
```

2. Розшифруємо наданий за варіантом текст, зашифрований біграмною афінною підстановкою.

```
TOTAL: 4473 bigrams

['ээ', 'вд', 'гн', 'цг', 'чф']
Possible keys: [(314, 34)]
```

Як бачимо, найпоширеніші біграми - 'ээ', 'вд', 'гн', 'цг', 'чф', а ключ після відсіювання лишився лише один — a=314, b=34.

Дешифруємо:

```
>>> Decrypt("./out.txt", 314, 34)
'мамапошламытьпосудуитомотпра
```

Початковий шифрований текст:

тгтгрэцрюфмнйбмйшугдээдэибггэдайжаишуикггуоитлчмтлвшаэвмхдвдлгцчцмбпврыэггзухлур
аятаиэншчфэчучкштфьэзукщтбцнчфвшяфнрагрэцрцлцэюоксбмчфцгссошпруйедйгцгрэчсммцлжл
очщетйсегрхчяэйекааэндвдэчбоцгзгдэыуирщцээятгллпльчкчедйгцгчдфэучюшщясеплэнйфюфюб
мйячвдогяфруопогшэпбмйячюоаэсмплизфрюбдукжюдээщшсвурятаэггшйячбдйгьойсегммцшмэцг
пмкаурюбщпдуяфйшлнрсээпблвтфцшкуцншмймщяээжсшшщятгдэцгчббйядогцоцггнвриэоеканыкл
гнурюбдухжогууэчцдябдайгогвшкайгогошплфдошплкуопогруопчсопйчяэаэнссрелуртукжэсфн
йфгдэээсглкчрзяаьйемщпмэумвдкгсгнчпщвшзэалжвурдуопогруопогруопогрухсопогбггнчфьд
ечхшюбнргдфпчбфэкдчтйгйщнрдуиээдиэвнчфщзгрвштфвешыэшочйшяаяффдкчвчтшаиешшившэдеч
лфюфэнветйячыяюшмэсдггснаяээюгсеелфчкпогюггнодядкчешфчывээечогьоуэучжоьэхшгчэйжу
тйггдсэдшшветйячыяцгцлнрэсснаявштэумэтогжлэеблэеишлтдгфшврхлячщшцнбйесгнфртййбмй
сстчжокгпбфэцрюбдувешыючрэщмбйетьдцчкдээпбцдщркжцлураяючржапюфвштэчяьорэтлурюфнр
агкдзэцгрэтлурфчычжлиекаэнчфьйзйлуирсмчфцгячьээйуиагшйдрйшиэпувдюшшишаыэмсвдхтгэ
кчьчэйыпнрмйчсартйфдчстгщшаззйрэыэчйхялуцшдуопогошзэалжвурээыунрбдяуэчждэсетьдеч
нпзякяцгггпмэтссхбмйячюоцгдэявжкйчггедоддэявжкаиягячеэюшуркйтеопечкгсшцлучщшазел
урчбезвчпмцлуруйячэрдшртклуйлрфмйшймплэеггдбуйишртгбцшнэгтждтхуэвчээгтждюгэдссмм
юфябцнчфцгфэзшмйсссшвриэяэчэсеплэнэвээятрэаржуснцзшуснвдцэюоиэгмкаурмйцзнрушдуэч
тоэчггаувймйсеябчфцньэцдогцояфюфтйкгюгогрэпутфээпбфэпутфаярссгжемйээрэврзюйдечдэ
ллцявчяаиечмбэкдрэцрябмйэшфунчгфшйтеюнтйугюоибдуиэнгждятгльчькснтбитчйэчувюдгнцч
ыэлгвдфечфучжеуыкчяэьйусигджуиаяьожчвшлухжвдгэопогылэеэсвдлуэдэсвдцорэцгжехлвчкд
бмюгягшшчфбэреапопечээжечбитогенчфезфрюйэчлмэсглсгвдугггждцгврзюыщкдкгюдфбцдешйм
плндешйшуйэчлгкджлаыэшьяыэфпечрэюгеджчиюруйогцэмйэчычюшдчялкуггетгмвшеншигнвевш
зэумшутэкдцрйшкльчькирфпвддбэнушмэучжолвэшйфиэбдяучфзснчгнуявдшчпэфшуиуйягвдюбэе
яукчыээээтждээнчячщшнфйшймэтвчимыщьдечвдэщезюнэнирхджбнряэаэзгэчвдэчучкшзьшчьччс
ыэфпечцгэчггауыщрэпмцдштйгвдкгучвдйэьоятцньюятчучфтйкгюгогтгтгвштйндтгогьйьэуицэ
юохэнечмэечмлнчфишмбмйээпуяищшсннрфмдуезггьоаягэрнщпчфурэвэжюдчсччусцэчяьогтччхш
тэйэссвшщзцлфчюрвууиьйтффедаюнчбтйиэгнушкмээкчешфчкпечкмщпсгвштуйскбуяэдэйслцнэр
дшбййббйьоээюоыэчскбцдечфучфширчяэлгыэумнрлвдлюмлсечибчфкдьовшябфэцрхчычялиелгвд
ячтчтогнуявдтчцчввэертдйфруцээщштфьюыэрзюбядгнпмшипчлмэдцгопфсучтчайтеюнбпвчюегм
ьйцнкчдгяэтажюэеыэшоашсвйшураяплггйнчфныжвиявчяэцнсссгдяэсаэкгцгвдюгпдвшиэвнйсцэ
чйфшцлчдждвдгнеяждчслшнфцлогбшнфюгягйэдйсрхжртбаирэшлщюгфэщруиплггчзгрчдфэюдщдтл
фруйетчэубэеэеяауряэфэедтгтгьйфпсгяэьэцдогыняцээлукчонвштбфэйэедмтяуазцдзсбшлвьь
сштфвравччмзвджмвштбдуйэедьоцнээяэынвежучфпчлмплюйтеыщлунрбшьзчетйьчшнюйдшцнчфдл
ьчггршезгршылныэнцээывтйячщшщяшчсчедиэяэщпвшфмтэцгкгюгогцойэаэшшшимззйрэвчешшигг
тлурйшшицгсепьплггнгээшсятаэьйфпдузйшнярснвшкдучяээцмчфкчешурмйжчянуйтеыщысщгьч
дфэеьорнплмйыэйгемчмогвяыдючвшэдечвчклччгнярснээцузсжчцчяэжекуяукжкгфруыурипфэлс
ээзшмэфечфртмсягджаиойтеазшчьфнрршоилуурюмаикдыэцулзнрзжзэюшзйкгнчывээцггэятьойэ
фэчдпфурэвкмчфкдыэцулзнрзжэшазшусндбвеюнюэрэвдядючдфэеьорночяэтгвчжокгойзйтеэшкг
дуцггуцстечфтфщзгрплээретфойтфярснвшжемйэсайжаапзяэсглйчыэитшчюорстэцгдфцнцдибыя
дэцгкчяэюггнелчджджщртбнфуййшяфбпогюгждюбцнчфжеэжвдэьедискчщрхчклтгвчжоыэгбвчячиэ
омвесдямзйжчянрцээыэцутэуфзйвюдббйдягнуяглдавчйчгтшэыэяэгнврэвкмфдтуйскбвшпрынмэ
цгкдыэцулзнрзжэшазшусннссэйлуснушазшусндфояьоаяфрябогкгьохчшсныэшазшуснгэзгшшлвээ

вшиедуфртйуштйэчпцээмзгртйжчянадькзйжчянрцээчсччуснмцнвеоирэщмгглтйгснаякчэдедьм
шиябыяучэйжакуэеклеяждмзфэедибмэсеопйдгтндсгснйекафрлуйгипдужеэщдуюнхьсгнцээкпве
дуцгрнисвдхтцуклжвэеюфцльчцуэнтфиэынезцсшдьончыкйшшаюбмйвчшшхчтебпдутээсшдкнцчыц
ээдфэеьоиэьчцвтйсстштбфэгнмйжчянблрншивчтшуииэудрэьуурюмяфлаэчзуюфйшишфпвекачфцг
крчшврпльчынмэкддбмнурэдечвдщрлжурюгьйкйьэцылажоуэааыщвчятйгайрдэээсаэкдшэцруйте
цнпггглаыжапурябчбфэээьнишиэмсбтягюшшиычмштфтечбйшючрэеззйээфэртусгнвемйогшэкшщя
техлфдршуифечфыэкчмфнрзшцнцчигвдылэеимюнчфрэщркжиэччаюфэнэеььцэюохэбщггмешижеюм
ггошшифпдажкюнкдпччэальчяэылснэнймтуьэтфвшэжвдэжвдцлцнмйлгиээдвдцоцгзгдэьмггююцл
фрлажюхдплггцаечцонцээгбфэяггнябмйцчедучкшшиагщэяттуйсяймйцчгэээудаэцоьйжвфпмэюш
кмщпсгкчшацгснйштбшижчальчыншыцлсншччтжчюшочрштбфэаржуиэвнэшлуэеклачюлшукжвдьэыа
юбыщфпкдэшьяхляуюэкддфэнэеььзузйюйпльчдэшшхдйчйскгшешыюнсгшешыюнтфцштблвшуфрмйуш
мэывфпчфюфхляуцзнрзжзйфрушйчмфкчйчяэкчныирхдвшэншыждвдлгнпсснрнцшысаээдшсясфедалн
дааээчычжвээюглгфрмйинюфршлагдьчцвтйгтрэчаснлаячщшцнщацгудифшыиэгтгггнхдьйэехлиэ
кчгнэнюйфрушнфешсвюнгнэнблеемйитзлпльчкчлнржэшхчешсвюнзылакдкчибцдшчндигкчзнймши
цгечбшшипдлгечвдынбсгнуяогятжецнцлцгжлбппьыдййгсщгшэршлвуйчфкчкддекаэтйгвдфпчфве
шыэшочршплюэцэшпаэтфкщнрдучфяэхрпльчршлнцдрэйэаэечаэрэдбйштбхжирдэфэпэвчечкчвдйс
юдйшщпхчшстуйсяйлгаэлвэшхаззыэээшплиэшоцгвчячвдьбфэцрщпдуюмлзтопмаиэчячянймьэээ
иэындацгудпцээавтйьоьйрщэьечомяылтцвирплюмдройазоэедкчедийалэшртнштйэчячдуйшяуйш
гнэчюшоизгпбмйаззйцчедэчвдыэяэщшшызйалкуйсбдкрвууицльчцулзодэйслцнкгыйуиагошшайм
цдудуогнишржхайгьоцгрэдэчоыэшскгыэяуирцнйфюбщпаэядалдуиэспиээчжозэшшлвшуплзкиэир
яуэшвкйчспиээчжойдьйюмвшучиэькяакунряэгэггшйэчлгюггэнпдуцнщпгмймрэвдпччйюдэшсвэс
ибфэосштйгьоылодждеэцгцдкгждячщшюьгггнцчьэнчюшюьтечбйшрсйшишуиюгксюжюнычшчжорэшш
щпюффрвууиыээээтклдфшнэшхдюдэсэйдшюбчфакадсгнчзйвдвшуйуиаггннрфмплчяядгныщдгнгйэ
зназзгныцгэчкшцнймвшодзйьоячщшоижемзшидэнчфаыщвчгнэсьоюгтеуйюмцшлтуэтшшнтсячюяьй
сньэлузйшнярснаылажорнмэедиэучгньэршяаюбиэззэумэтядзэмекжфрмйушэнчфймймшэсекжюнир
ушоишуиеуэаакуфэщглфюфэншызэедиэкгнцссждэсссуикчучяэцгечшнюйдшйштйвяээгнцзггкгкд
цгюгыдссэьюяыччйтфадкдцгыэийядсспдкйочедкчюшлщанэнплкдцгрэвдпдмчншюмыэшсезггядьо
аясечфзйезгнэчюшщпмйэецюбгьйэецюзйьэтфвшишяиечюрэжушзэгэвддэээалггычкдйдгнггмлрн
мфйшлнмбэеяукггунфгнодэйьэшннрфммйьэжакусвфдкггуоигэмыэшзгжчэержюнинвйпльчдэедуб
шиждрнвекайшхльчцуэнчфжещпаэядцмчфгмюггныяджаиипвевчябцдщгайемтгячцдяэдбдуйшяуяи
уимфэеснйфнрфрвшкчечогншюфкдучяэсрхщщпчбюбюбцдечэйшэмеишьяучцчовтйхчщрлучфишкмщп
вшазшуснтгьожлйшвртййбцнфэтдямкледрсйвжкмфюфетюгчснгкчцэчйжуфэщгыдспнрмйчфпмкаур
ээдйкдщштвфпвшзйфсудаэцоетюгкчяэкчцэчйойкдщштвфпвшзйфсудаэцовшьйфпсгьэтлггигсная
рняфесячспнрмйтгячцдтлэширцнцгжеыыэшьяойээгэпплвефрфчшсйэедшеопшигэфэяэншяцядже
гмзяеттфурэвэжюдьйэехлиэвчдстшюбфэаэьмщпсгкдлсбовшрэпуснсссгмзнрзжэшклэекчэйззнр
зжэшклэекчэйбцээдэнчээешсвэнэвээопдуиэмедуыпябцчгнмбкдюдьотгкччвтйтшоищравяиапог
ршочдфэеьодуйшьэьйуиьйирэшиэнштйэчячждбруэтнймэщяэфэедччюдсмяыгэонймнчячщшцнймнч
дуйшгмгмяылтвнймнчцньйфпмэтержэшсмяыгэдйьэисщгбтуйьэюняиртжевшсдячюортяазсртршдч
тлчмуйсеябюдьэифшашмецядцпведуэжюмшчпйэчлгиэшэщшшызйалчфячкчжгкгыээшзэюятшочкчрэ
жчкшочдуйшлвзйальгкчэчгэмтзэреаптвээюгзгбтйгфнкгжныяьдцгндешблрнэщяэфэедммыщрэиэ
агдэцэггудйгснаявчечпяыдшсщгшэщекамфбйтфачечдядйаггнььшэьйрщгневшфедаюнжседычяф
емцнвечфбйжчянйфэнюйиэйгфечфыэрэтлурхлячщшцншуопогруопцлшеопезюблвдлгньэйгвдынцн
мйфсудаэцоылэеимисдэцмвдгнурмйпльчонэщмэкдкчешурынезелфчзнймщяядчдцгшчдбцчечюоцг
ззяалтчгюшщяядчдцгцнучяэюгдэявуруйэчувюдцнучяэкгкгбцээшсжетвйшюбцчгузэкдкдыэцуиш
ысдэцмурйшкмщпсгешсвюнешсвюньчцвтйынцнмйфсудэйемкаурмйюэреапцгжеыпфчэйьэтвэерттф
лжхтузйефчальчюяьйзйфрвйчяыдцпведуыээдзчафцгщшщпхчждвдьэсеопэчвдкгшнэжйшюбфэтдлг
юшлщфэшэшрзйпллунрйшйшймэнелпьыдййемймжемзшийэлфплцузйезймлакуггжфвелтьэфнцгфсэс
ьйойезйеуртйюйячкгогцогныпцлуртйблдуэсээимгдьйюфчфьчмупчядчдртятвдвшяфюффдээзлцн
ьчцвтйьдхфйшлнавээээщравюнаяынцнмйфсудэйойэчувюдьйтфнрагфаэчзувэесгнфруйинймкджм
лвээкгнчэйщбфэдякдйсрсйшюбурсюыщмйлгкчэйщбданрцнфдяшзйучгнхаэчзувшаыиеюдюмнрйвхч
ьйэетйячтекалсчгснядчдцгьйзэгнцчншюбыянчюшуишылуишхчхщкгжнтфиэесгнчшиэкгфззйжерь
тшодтуйсцуурюмдуурюмдатэреапчфяэаэаязузййфюфлумфюффдошплюфюфюфюфлукжвчщжвчщжвчыф
агэйдшщпцлячюшуйртунахзяфбдуэсплггнгвщхщцнчфкчнсэйшнфэтфурэвэжюммеэнчсартйагхрцл
шужчкдпывшчгюзфплнйэйэжсфаэчзуелтлфруйблэчющээшдузйшнйффрвдвшплныурэшртюсвдээял
дяэсвдылодфэвмуйэчувюдюггнцчыэлгвдячщшцнтээйссягогуйеснгюшщяхжиеыжэшцгжааэмшщяцн
гнмбфрюбцнэеслюбтчядаляуюэцгшэьйтфнызйезггогцорэндэдьоаяцлшеопуилгйпйсцэрэжчдгвд
кмщпсгячщшцнтэжщитэсогээзшплнрцгьэретфоэюрцлфдешйчьэешкмвддфояцотеочтгюоудччзфюф
ээпбцдэчядоекадлгмйсцаюбыщаэчсартйчфэчбоцнкчяэьйфпсгягяшснрэээонггьэпуэеклеяждэч
алщфхдйспотфйгпбцчгйээюнрэлмюфнрдушиучаээчыэюяэдогтгтгцнйчгнггйээдщряуишзэгнурмй
инчфешурвшишкмщпсгзылакдкдыэшсжеяцээкчггшйкгнчтшкмщпсгиэгнггыцээтшхльчцутэгнишсн
аяцшйчтукжйдтукжснчфэншыснтфиэшрснкчншлвььвшэжвдгэдэчйягьокгещвехжлвээчсартйндьэ
омймйэфэхэиштэшшбйюмцшчслгщшймггкэреапфчшсрэчстгаэцоцусндуурюмчбмйшстшчфбэюгцчюш
чфврцшшивчнсцгжлвгчсыэпбцнчфршламбдунрйштбфэфехщцнуррэяагэиэывщяюшмйэдгнирээзшез
яанфэшртдыиряартпаэчтоюгчршуфраяршлвюнчфврфпаяжбмйячюоыягэдймеэнчфэчцошешытэубцд

щркжцлураяоцээшсылуйсслумфурсгвчыэсгвчыэлгспечьчцвтйгвюнаярэяапыфрэщжлйьфэшшоиме
энисжчфэалмйягвчкдпрфпюдффиэяэвчтшкакуьэаллгрсцыэшлвхуопогщруыурыягэдэтшфпчбыщаэ
рээждрнезгргмймьэйжазгньэээпбэезйлгчуфэщгьоээюоыэжлклькьяешпьцгэчкшемкуопжехжтб
лгаэямймхчдуцгынвшлвььнытйиэячщшьгшеопщязйвджднгнэезсрфишыэцуишмзшублзгдэыуиртбмй
теодифыжйшбйаггнеяшэреапчфуиьйэехлиэкчшэыркуэнхуопогоштфиэяэрэчстглбплээцдынцнвй
кгюгаэкдмфнрэрйшзсвдпчршяаюбиэггзуруйзжапмзвднччраыклцнвшиснчрэьуэеклеяждьэрряу
чфишэнфэссиетфюфтймйьэуисеплэнйшфпфэьммйкгюгогягяглуснйшзэчдчртймг

Дешифрований текст:

мамапошламытьпосудуитомотправилсязанейкаждыйзвукзвонложкиилитарелкигулкораздавал
сявзнойномвечернемвоздухепотомонимолчапошливбольшуюкомнатуснялисдиванаподушкив
двоемраскрылиегоиразложиливедьнасамомделеэтобылвовсенедиванашироченнаякроватьмам
апостелилаимсдугласомпостельловковзбилаподушкитомначалбылорасстегиватьрубашкуноон
асказалапогодиминуткутомпочемунадотыкакаяточуднаямамонаопустиласьнастулносразужевс
талаподошлакдвериипозвалаоназваласноваисновадугласдугдуугееголосуплывалвдушнуютьм
уитонулвнейбезвсякогоотклikадажеэхонеотвечалодугласдугласдугласдуууглаастомсиделнап
олуиегопронизывалхолодновинойтомубылонемороженоеинезимаинелетнийзнойонвиделмама
торастерянноозираетсятозакрываетглазастоитинезнаетчтоделатьиоченьволнуетсядасразувидн
орастерянаиволнуетсяонаоткрыладверьверандышагнулавтемнотуспустиласьпоступенькампро
шлаподорожкеподкустысиренитомприслушивалсякеешагамонаопятьпозваламолчаниеонапозв
алаещедваразатомвсеседелвкомнатевотсейчассдлиннойдлиннойузкойулицыдонесетсяголосду
гласаидумамнебеспокойсяяидунодугласнеотвечалтомдолгиедвеминутысиделглядянараскрыту
юпостельнамолчащеерадиоимолчащийпатефонналюстругдекакнивчемнебывалопоблескивали
стеклянныевисюлькинаковеррасписанныйпунцовымиифиолетовымизавитушкамипотомнароч
ностукнулногойокроватьчтобыпоглядетьбудетлибольнооказалосьбольнодверьверандысоскри
помотвориласьимамасказалапойдемтомпройдемсякудапростопоулицеидемонвзялеезарукуони
пошлипосентджеймсстритасфальтподногамибылвсеещетеплыйсверчкистрекоталигромчепре
жнеговсгущавшейсятьмеонидошлидоугласвернулиидвинулисьпонаправлениюкзападномуовр
агугдетопроплылавтомобильсверкнулвдалифараминаулицахникакихпризнаковжизнинисветан
идвиженияkоегдепозадимерцалислабоосвещенныеквадратыоконвтойсторонеоткудаонишлине
всеещелеглиспатьнооченьоченьмногиедомаужестоялибезогнейиспалиапереднекоторымитоже
темныминакрылечкахсиделииихобитателиивполголосавеливечернююбеседукоегденаверандах
поскрипываликачелихотьбыотецбылдомасказаламамаонасжималавсвоейбольшойрукерукуто
манупостойдаймнетолькодобратьсядоэтогомальчишкидушегубопятьвышелнаохотуонубивает
людейвсемгрозитопасностьниктонезнаетгдеикогдаонвдругпоявитсяворклянусьпустьтолькодуг
придетдомойяеготакотколочувекбудетпомнитьонипрошлиещеквартalитеперьстоялипередчер
нымсилуэтомнемецкойбаптистскойцерквинауглучепелстритигленроквсотнешаговзацерковью
начиналсяоврагтомужечуялегооттудатянулоканализационнойтрубойсгнившимилистьямидуш
нымивлажнымзапахомсплошныхзеленыхзарослейоврагбылширокийизвилистыйонперерезалг
ородимамавсегдаговорилачтоэтоиднемтонепроходимыедебриаужночьюкнемулучшеиблизконе
подходитьоттогочторядомцерковьстрахидолжныбырассеятьсянотомувсеравнобыложутковэто
тчастемнаябезединогоогонькаонаказаласьхолоднойибесполезнойразвалинойнакраюоврагатом
убыловсегодесятьлетонничеготолкомнезналосмертистрахеужасесмертьэтовосковаякуклавящ
икеонвиделеевшестьлеттогдаумерегопрадедушкаилежалвгробуточноогромныйупавшийястре
ббезмолвныйидалекийникогдабольшеоннескажетчтонадобытьхорошиммальчикомникогдабол
ьшенебудетспоритьополитикесмертьэтоегомаленькаясестренкаоднаждыутромемубыловтовре
мясемьлетонпроснулсязаглянулвееколыбелькуаонасмотритпрямонанегозастывшимислепыми
синимиглазамиапотомпришлилюдииунеслиеевмаленькойплетенойкорзинкесмертьэтокогдаон
месяцспустястоялвозлееевысокогостульчикаивдругпонялчтоонаникогдабольшенебудеттутсид
етьнебудетсмеятьсяилиплакатьиемуужененебудетдосадночтоонародиласьнасветэтоибыласмерть
иещесмертьэтодушегубкоторыйподкрадываетсяневидимкойипрячетсязадеревьямииbродитпо
округеивыжидаетиразилидвавгодприходитсюдавэтотгороднаэтиулицыгдевечерамивсегдатемн

очтобыубитьженщинузапоследниетригодаонубилтрехэтосмертьносейчастутнепростосмертьв
этойлетнейночиподдалекимизвездаминанегоразомнахлынуловсечтоониспыталвиделислышал
завсюсвоюжизньионзахлебывалсяитонулонисошлистротуараизашагалипопротоптаннойусыпа
ннойщебнемтропинкепообестороныгусторосласорнаятраваивнейгромконеумолчнотрещалисв
ерчкитомпослушношелзаматерьюбольшойхрабройпрекраснойегозащитницейотвсегосветатак
вдвоемонишлиишлиивотостановилисьнасамомкраюцивилизацииоврагздесьвэтойпропастипо
средичерной чащобывдругсосредоточилосьвсечегоонникогданеузнаетинепойметвсечтоживетб
езыменноевнепроглядной тенидеревьеввудушливомзапахегниенияаведьонисматерьюздесьсов
семодниииерукадрожитдадрожитемунепочудилосьноотчегомамаведьбольшесильнееумнееего
неужелиионатожечувствуетэтунеуловимуюугрозутозловещеечтозатаилосьтамвнизуисейчасвы
ползетизтемнотызначитможновырастиивсеравнонестатьсильнымзначитстатьвзрослымвовсен
еутешениезначитвжизнинетприбежищанеттакойнадежнойцитаделичтоустоялабыпротивнадви
гающихсяужасовночисомненияразрывалиегомороженоевновьобожглоемухолодомгорловсевн
утрипохолоделопоспинепошелморозоледенелирукииногиемувдругсталоченьзябкоточновнов
ьналетелизпрошлогодекабрьскийветертаквотоночтозначитэтоучастьвсехлюдейкаждыйчелове
кдлясебяодинединственныйнасветеодинединственныйсампосебесредивеликогомножествадру
гихлюдейивсегдабоитсявоткаксейчаснузакричишьстанешьзватьнапомощькомукакоеделотьма
поглотитводномгновеньеодночудовищноеледенящеемгновеньеивсеконченоещезадолгодорасс
ветазадолгодотогокакполицейскиеначнутпрощупыватьсвоимифонарикамитемнуюрастревоже
ннуютропинкуинанейзашуршитщебеньподногамилюдейкоторыевсмятениикинутсянапомощь
идажееслионисейчастольковпятистахшагахоттебяаужнавернотаконоиестьтемныйприбойможе
тзахлестнутьзатрисекундыиотнятьутебявсетвоидесятьлетижизньэтоодиночествовнезапноеотк
рытиеобрушилосьнатомакаксокрушительныйударионзадрожалмаматожеодинокавэтуминутуе
йнечегонадеятьсянинасвятостьбраканиназащитулюбящейсемьининаконституциюсоединенны
хштатовнинаполициюейнеккомуобратитьсякромесобственногосердцаавсердцесвоемонанайде
тлишьнеодолимоеотвращениеистрахвэтуминутупередкаждымстоитсвоятолькосвоязадачаика
ждыйдолженсамеерешитьтысовсемодинпоймиэторазинавсегдатомпроглотилкомокзастрявши
йвгорлеиприжалсякматеригосподинедайейумеретьмолилоннеделайнамничегоплохогопапапри
детссобраниячерезчасиеслидоманикогонебудетматьдвинуласьпотропинкевдикуючащумамтыз
адуганебойсядрожащимголосомсказалтомснимничегонеслучилосьтызанегонебойсяснимниче
гонеслучилосьонвсегдавозвращаетсяэтимпутемголосматеризвенелотнапряженияясторазговор
илаемуходидругойдорогойноэтипроклятыемальчишкивсеравнолезутнапроломкогданибудьонп
ойдеттудаибольшеневернетсябольшеневернетсяэтоможетозначатьчтоугоднобродягипреступн
икитьманесчастныйслучайаглавноесмертьодинвовсейвселеннойнасветемиллионтакихгороди
шекивкаждомтакжетемнотакжеодинококаждыйтакжеотвсегоотрешенвкаждомсвоиужасыисво
итайныпронзительныезаунывныезвукискрипкивотмузыкаэтихгородишекбезсветаносомножес
твомтенейакакоенеобятноенепомерноеодиночествоаневедомыеоврагичтозасасываюткактряси
нажизньвэтихгородишкахпоночамоборачиваетсяледенящимужасомразумусемьедетямсчастью
совсехсторонгрозитчудищеимякоторомусмертьматьсновагромкопозвалавтемнотудугласдугив
другобапочувствовваличтотослучилосьсверчкиумолклисталосовсемтихоонинезналчтобываетт
акаятишинабеспредельнаябездыханнаятишинаотчегозамолчалисверчкиотчегокакаяэтомуприч
инапреждеонининикогданеумолкалиникогдазначитзначитсейчасчтотослучитсяказалосьоврагнап
рягаетсвоичерныемышцывбираетвсебявсесилыспящихгородковифермнамногиемиливокругве
ликаятишинапропитанныхросойлесовидолининакатывающихсякакприбойхолмовгдесобакиза
дравмордывоютналунувсясобираласьстекаласьстягиваласьводнуточкуивсамомсердцетишины
былионимамаитомвотсейчассиюминутучтотослучитсячтотослучитсясверчкивсемолчатзвезды
опустилисьтакнизкочтокажетсяпротянирукуинапальцахостанетсяпозолотаихнесчестьзвездон
ижаркиеколючиевсерастетразбухаеттишинавсеострейнапряженнейожиданиеохкактемнопуст
ыннокакбесприютноивдругдалекодалекозаоврагомголосяздесьмамидумамаисновамамамамид
ушлепшлепшлепмчатсяногивтеннисныхтуфляхподнуоврагасхохотомнесутсятроемальчишекб
ратдугласчарливудмениджонхафбегутхохочутзвездывзвилисьверхточнодесятьмиллионовужа
ленныхулитоквтянулисвоирожкисверчкизастрекоталитемнотаотступалаиспуганнаяошарашен

наязлобнаяотступилапотеряваппетитведьонасовсемужесобраласьпоживитьсяивдругейтакгруб опомешалиикогдатемнотаотхлынулаточноволнавовремяотливаизнеевозниклисмеясьтроемаль чишекмамтомприветисразувокругзапахлодугласомведьотнеговсегдапахнетпотомтравойдерев ьямиветвямииручьемвампредстоитпоркамолодойчеловекобявиламамаотеестраховиследанеос талосьтомзналонаникогдавжизниникомупроэтонерасскажетникогданострахэтотнавсегдаостан етсяунеевдушеивдушетоматожетемнойлетнейночьюонишлидомойспатькакхорошочтодугласж ивойкакхорошоанаоднусекундутамнакраюоврагаемуподумалосьгдетодалекопосмутномуозаре нномулунойлесунадвиадукомпотомвнизуподолинепрогрохоталпоездонотчаянносвистелточно безыменныйжелезныйзверьзаблудилсявночитомулегсявпостельрядомсбратомвесьдрожаонпр ислушивалсякэтомусвистуидумалдалекодалекотамгдесейчасмчитсяпоезджилихдвоюродныйб ратиумеротвоспаленияилегкихмноголетназадвотвтакуюженочьдугласлежалрядомотнегопахлоп отомиэтобылокакволшебствотомпересталдрожатьтолькодвевещиязнаюнавернякадугпрошепт алонкакиеодначтоночьюужаснотемноадругаяеслимистерауфманкогданибудьвсамомделепостр оитмашинусчастьясоврагомейвсеравнонесовладатьдугласнемногоподумалповторичтотысказа лониумолклинаулицевнезапнораздалисьшагиближеближевотониужеподдеревьямивозледоман атротуаремамасосвоейкроватинегромкосказалапапаидетинеошиблась

Висновки:

В цій роботі ми ознайомилися з афінним шифром біграмної підстановки, навчилися шифрувати та дешифрувати та знаходити ключ за наданим шифротекстом. В цій роботі було написоано програми для розв’язання модульних рівнянь, що використовуються для знаходження ключа, а також програму для знаходження ключа за порівнянням найросповсюдженіших біграм та виключенням за забороненими біграмами та неоднозначними ключами та за допомогою неї розшифрували наданий текст.