Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №3

на тему: «Криптоаналіз афінної біграмної підстановки»

Виконали:

студенти 3 курсу ФТІ

групи ФБ-73

Пазон Б.Р. та Лутак А. О.

Перевірив:

Чорний О.

Мета роботи: Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної

підстановки; опанування прийомами роботи в модулярній арифметиці.

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

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 №1, 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

(a, b) знайти можливі кандидати на ключ 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.

Результати виконання роботи:

Найчастіші біграми:

Мови: ст но то на ен;

Шифртексту: ыу юк як ую ып

Знайдений ключ, шо приводить до змістворного тексту:

856, 909

Розшифрований текст:

библейскоепреданиеговоритчтоотсутствиетрудапраздностьбылаусловиембла женствапервогочеловекадоегопаденияслюбовькпраздностиосталасьтажеивпад шемчеловекенопроклятиевстяготеетнадчеловекоминетолькопотомучтомывпо телицадолжныснискиватьхлебсвойнопотомучтопонравственнымсвойствамсв оиммынеможембытьпраздныиспокойнытайныйголосговоритчтомыдолжныб ытьвиновнызаточтопраздныежелибымогчеловекнайтисостояниевкоторомонб удучипраздныммчувствовалбысебяполезнымиисполняющимсвойдолгонбынаш елоднусторонупервобытногоблаженстваитакимсостояниемобязательнойибез

упречнойпраздностипользуетсяцелоесословиесословиевоенноевэтойтообязат
ельнойибезупречнойпраздностисостоялаибудетсостоятьглавнаяпривлекатель
ностьвоеннойслужбыниколайростовиспытывалвполнеэтоблаженствопослего
дапродолжаяслужитьвпавлоградскомполкувкоторомонужекомандовалэскадр
ономпринятымотденисоваростовсделалсязагрубелымдобрыммалымкоторого
московскиезнакомыенашлибынесколькономоторыйбыллюбимиуважаемтовар
ищамиподчиненнымииначальствомикоторыйбылдоволенсвоейжизньювпосле
днеевремявгодуончащевписьмахиздомунаходилсетованияматеринаточтодела
расстраиваютсяхужеихужеичтопорабыемуприехатьдомойобрадоватьиуспоко
итьстариковродителейчитаяэтописьманиколайиспытывалстрахчтохотятвывес
тиегоизтойсредывкоторойоноградивсебяотвсейжитейскойпутаницыжилтакти
хоиспокойноончувствовалчтораноилипозднопридетсяопятьвступитьвтотомут
жизнисрасстройствамиипоправлениямиделсучетамиуправляющихссорамиинт
ригамиссвязямисобществомслюбовьюсониобещаниемейвсэтобылострашнот
руднозапутаноионотвечалнаписьмаматерихолоднымиклассическимиписьмам
иначинавшимисяикончавшимисяумалчиваяотомкогдаоннамеренприехатьвго
дуонполучилписьмародныхвкоторыхизвещалиегоопомолвкенаташисболконс
кимиотомчтосвадьбабудетчерезгодпотомучтостарыйкнязьнесогласенэтопись
моогорчилооскорбилониколаявопервыхемужалкобылопотерятьиздоманаташу
которуюонлюбилбольшевсехизсемьивовторыхонссвоейгусарскойточкизрени
яжалелотомчтоегонебылоприэтомпотомучтоонбыпоказалэтомуболконскомуч
тосовсемнетакаябольшаячестьродствоснимичтоежелионлюбитнаташутоможе
тобойтисьибезразрешениясумасбродногоотцаминутуонколебалсянепопросит
ьсяливотпускчтобувидатьнаташуневестойнотутподошлиманеврыпришлисооб
ражениясонеопутаницеиниколайопятьотложилновеснойтогожегодаонполуч
илписьмоматериписавшейтайноотграфаписьмоэтоубедилоегоехатьонаписал
ачтоежелиниколайнеприедетиневозьметсязаделатовсименьепойдетсмолоткаи
всепойдутпомируграфтакслабтаквверилсямитенькеитакдобритаквсеегообман
ываютчтовсидетхужеихужерадибогаумоляютебяприезжайсейчасжеежелитын
ехочешьсделатьменяивствоесемействонесчастнымиписалаграфиняписьмоэто
подействовалонаниколаяунегобылтотздравыйсмыслпосредственностикоторы
йпоказывалемучтобылодолжнотеперьдолжнобылоехатьеслиневотставкутовот
пускпочемунадобылоехатьоннезналновыспавшисьпослеобедаонвелелоседлат
ьсерогомарсадавнонеезженногоистрашнозлогожеребцаивернувшисьнавзмыле
нномжеребцедомойобявиллаврушкелакейденисоваосталсяуростоваипришед
шимвечеромтоварищамчтоподаетвотпускиедетдомойкакнитрудноистранноб
ылоемудуматьчтоонуедетинеузнаетизштабачтоемуособенноинтереснобылопр

оизведенлионбудетвротмистрыилиполучитаннузапоследниеманеврыкакнистр
аннобылодуматьчтоонтакиуедетнепродавграфуголуховскомутройкусаврасых
которыхпольскийграфторговалунегоикоторыхростовнапарибилчтопродастзат
ысячикакнинепонятноказалосьчтобезнегобудеттотбалкоторыйгусарыдолжны
былидатьпаннепшаздецкойвпикууланамдававшимбалсвоейпаннеборжозовско
йонзналчтонадоехатьизэтогоясногохорошегомиракудататудагдевсбыловздор
ипутаницачерезнеделювышелотпускгусарытоварищинетолькопополкуноипоб
ригадедалиобедростовустоившийсголовыпорубподпискиигралидвемузыкипе
лидвахорапесенниковростовплясалтрепакасмайоромбасовымпьяныеофицеры
качалиобнималииуронилиростовасолдатытретьегоэскадронаещеразкачалиего
икричалиурапотомростоваположиливсаниипроводилидопервойстанциидопол
овиныдорогикакэтовсегдабываетоткременчугадокиевавсемыслиростовабыли
ещеназадивэскадроненоперевалившисьзаполовинуонуженачалзабыватьтройк
усаврасыхсвоеговахмистрадожойвейкуибеспокойноначалспрашиватьсебяото
мчтоикаконнайдетвотрадномчемближеонподезжалтемсильнеегораздосильнее
какбудтонравственноечувствобылоподчиненотомужезаконускоростипадения
телвквадратахрасстоянийондумалосвоемдоменапоследнейпередотраднымста
нциидалямщикутрирублянаводкуикакмальчикзадыхаясьвбежалнакрыльцодо
мапослевосторговвстречиипослетогостранногочувстванеудовлетворениявсра
вненииистемчегоожидаешьвстожекчемужеятакторопилсяниколайсталвживать
сявсвойстарыймирдомаотециматьбылитежеонитольконемногопостарелиново
евнихбилокакоетобеспокойствоиногданесогласиекоторогонебывалопреждеи
котороекакскороузналниколайпроисходилоотдурногоположенияделсонебылу
жедвадцатыйгодонаужеостановиласьхорошетьничегонеобещалабольшетогоч
товнейбылоноиэтогобылодостаточноонавсядышаласчастьемилюбовьюстехпо
ркакприехалниколайивернаянепоколебимаялюбовьэтойдевушкирадостнодейс
твовалананегопетяинаташабольшевсехудивилиниколаяпетябылужебольшойт
ринадцатилетнийкрасивыйвеселоиумношаловливыймальчикукоторогоужело
малсяголоснанаташуниколайдолгоудивлялсяисмеялсяглядянанеесовсемнетаг
оворилончтожподурнеланапротивноважностькакаятокнягинясказалонейшопо
томдададарадостноговориланаташанаташарассказалаемусвойроманскняземан
дреемегоприездвотрадноеипоказалаегопоследнееписьмочтожтырадспрашива
ланаташаятактеперьспокойнасчастливаоченьрадотвечалниколайонотличныйч
еловекчтожтыоченьвлюбленакактебесказатьотвечаланаташаябылавлюбленав
борисавучителявденисованоэтосовсемнетомнепокойнотвердоязнаючтолучше
егонебываетлюдейимнетакспокойнохорошотеперьсовсемнетаккакпрежденик
олайвыразилнаташесвоенеудовольствиеотомчтосвадьбабылаотложенанагодн

онаташасожесточениемнапустиласьнабратадоказываяемучтоэтонемоглобыть
иначечтодурнобыбыловступитьвсемьюпротивволиотцачтоонасамаэтогохотел
атысовсемсовсемнепонимаешьговорилаонаниколайзамолчалисогласилсясне
юбратчастоудивлялсяглядянанеесовсемнебылопохожечтобыонабылавлюблен
наяневеставразлукессвоимженихомонабыларовнаспокойнавеселасовершенно
попрежнемуниколаяэтоудивлялоидажезаставлялонедоверчивосмотретьнасват
овствоболконскогоонневерилвточтоеесудьбаужерешенатемболеечтоонневида
лснеюкнязяандреяемувсказалосьчточтонибудьнетовэтомпредполагаемомбрак
езачемотсрочказачемнеобручилисьдумалонразговорившисьразсматерьюосест
реонкудивлениюсвоемуиотчастикудовольствиюнашелчтоматьточнотакжевгл
убинедушииногданедоверчивосмотреланаэтотбраквотпишетговорилаонапока
зываясынуписьмокнязяандреястемзатаеннымчувствомнедоброжелательствак
отороевсегдаестьуматерипротивбудущегосупружескогосчастиядочерипишет
чтонеприедетраньшедекабрякакоежеэтоделоможетзадержатьеговерноболезнь
здоровьеслабоеоченьтынеговоринаташетынесмотричтоонавеселаэтоужпослед
неедевичьевремядоживаетаязнаючтоснейделаетсявсякийразкакписьмаегопол
учаемавпрочембогдаствсихорошобудетзаключалаонавсякийразонотличныйче
ловекпервоевремясвоегоприезданиколайбылсерьезенидажескученегомучилап
редстоящаянеобходимостьвмешатьсявэтиглупыеделахозяйствадлякоторыхма
тьвызвалаегочтобыскореесвалитьсплечэтуобузунатретийденьсвоегоприездао
нсердитонеотвечаянавопроскудаонидетпошелснахмуреннымибровямивофлиг
елькмитенькеипотребовалунегосчетывсегочтотакоебылиэтисчетывсегоникол
айзналещеменеечемпришедшийвстрахинедоумениемитенькаразговориучетми
тенькипродолжалсянедолгостаростаставыборныйиземскийдожидавшиесявперед
нейфлигелясострахомиудовольствиемслышалисначалакакзагуделизатрещалк
акбудтовсвозвышавшийсяголосмолодогографаслышалиругательныеистрашн
ыесловасыпавшиесяоднозадругимразбойникнеблагодарнаятварьизрублюсоба
кунеспапенькойобворовалитдпотомэтилюдиснеменьшимудовольствиемистра
хомвиделикакмолодойграфвеськрасныйсналитойкровьювглазахзашиворотвы
тащилмитенькуногойиколенкойсбольшойловкостьювудобноевремямеждусво
ихсловтолкнулегоподзадизакричалвончтобыдухутвоегомерзавецздесьнебыло
митенькастремглавслетелсшестиступенейиубежалвклумбуклумбаэтабылаизв
естнаяместностьспасенияпреступниковвотрадномсаммитенькаприезжаяпьян
ыйизгородапрятalсявэтуклумбуимногиежителиотрадногопрятавшиесяотмите
нькизналиспасительнуюсилуэтойклумбыженамитенькиисвояченицысиспуган
нымилицамивысунулисьвсениизверейкомнатыгдекипелчистыйсамоваривозв
ышаласьприказчицкаявысокаяпостельподстеганнымодеяломсшитымизкоротк

ихкусочковмолодойграфзадыхаясьнеобращаянанихвниманиярешительными шагамипрошелмимонихипошелвдомграфиняузнавшаятотчасчерездевушекото мчтопроизошловофлигелесоднойстороныуспокоиласьвтомотношениичтотепе рьсостояниеихдолжнопоправитьсясдругойстороныонабеспокоиласьотомкакп еренесетэтоеесынонаподходиланесколькоразнацыпочкахкегодверислушаякак онкурилтрубкузатрубкойаа

Код програми

```
import collections

import detectRussian

from math import *

bigramms_frequent = ['но', 'ст', 'ен', 'то', 'на']

bigrams_unexistant = ['иь', 'аь', 'оь', 'уь', 'еь', 'ыь', 'эь', 'яь', 'юь', 'йь', 'йй', 'ьь', 'ыы']

dict = open("alphabet.txt", 'r+', encoding='utf8', errors='ignore')

file_for_bi = open("15.txt", 'r+', encoding='utf8', errors='ignore')

dictionary = dict.read()

bigramms = []

def egcd(a, b):

    if a == 0:

        return (b, 0, 1)

    else:

        g, x, y = egcd(b % a, a)

        xx = y - (b // a) * x

        return (g, xx, x)


# x = mulinv(b) mod n, (x * b) % n == 1


def mulinv(b, n):

    g, x, _ = egcd(b, n)
```

```
    print(x)
    if g == 1:
        return x % n
file = file_for_bi.readline()
alphabet_bi={}
def count_bigramms(file):
        length = 0
        for i in range(1,len(file)):
                bigram = file[i-1]+file[i]
                if bigram  in alphabet_bi:
                        alphabet_bi[bigram]+=1;
                        length = length +1
                else:
                        alphabet_bi[bigram]=1;
                        length = length +1
        return length;
length = count_bigramms(file)
#file_for_bi.close()
def sort_dictionary_by_value(dictionary):
    list_of_sorted_pairs = [(k, dictionary[k]) for k in sorted(dictionary.keys(), key=dictionary.get, reverse=True)]
    # Так мы создаём кортежи (ключ, значение) из отсортированных элементов по ключу равному "значение ключа"
    # Также отсортированы будут и ключи, имеющие одно значение
    # "reverse = False" говорит, что перебор нужно делать в обычном порядке
    # Если нужно отсортировать значения в обратном порядке, то reverse можно сделать = True
    return list_of_sorted_pairs
```

```
new_a = sort_dictionary_by_value(alphabet_bi)


for x in new_a:
   print(x[0], x[1] )


###print(alphabet_bi)


bigram_and_numbers = {}
def bigramm_number():
   i=0
   j=0
   for i in range(0,len(dictionary)):
         for j in range(0,len(dictionary)):
            bigramm = dictionary[i] + dictionary[j]
            bigramm_num = 31*i + j
            bigram_and_numbers[bigramm] = int(bigramm_num)
   ###print(bigram_and_numbers)
qwe = bigramm_number()


qw = [bigram_and_numbers.get('ст'), bigram_and_numbers.get('но'),
bigram_and_numbers.get('ен'), bigram_and_numbers.get('то'), bigram_and_numbers.get('на')]
qwe11 = bigram_and_numbers.get('ыу')
qw2 = [bigram_and_numbers.get('ст'), bigram_and_numbers.get('но'),
bigram_and_numbers.get('ен'), bigram_and_numbers.get('то'), bigram_and_numbers.get('на')]
qwe13 = bigram_and_numbers.get('юк')
print(qw)
print(qw2)
print(qwe11)
```

```
print(qwe13)
aaa = bigram_and_numbers.get('як')
aaa1 = bigram_and_numbers.get('ую')
aaa2 = bigram_and_numbers.get('ып')
def equation(x1,y1,x2,y2):
    x = (x1-x2)%961
    y = (y1-y2)%961
    nsd, x_reversed, imp = egcd(x, 961)
    #print(x_reversed % 961)
    if y % x_reversed == 0:
        y /= x_reversed
        print(y)
        nsd, reversx, imp = egcd(x/x_reversed, 961/x_reversed)
       # print(reversx)
        x0 = (y*reversx) % (961/x_reversed)
        #print (x0)
        return x0
    else:
        print(str(y) + ' y value')
        print(str(x_reversed) + ' x^-1 value')
        a = (y*x_reversed)%961
        b = (y1-a*x1)%961
        return a,b


def get_key(d, value):
            for k, v in d.items():
```

```
            if v == value:
                return k


def decipher(a1,b1):
    i=0
    while i < len(file)-1:
        bigram = file[i]+file[i+1]
        i+=2
        bigram_value = bigram_and_numbers.get(bigram)
        a_rev= egcd(a1,961)[1]%961
        bigram_value_deciphered=((bigram_value-b1)*a_rev)%961
       # print(bigram_value_deciphered)


        bigram_deciphered = get_key(bigram_and_numbers ,bigram_value_deciphered)
        print(bigram_deciphered, end='')
for i in qw:
    for j in qw2:


            if i!=j:
                print(str(i)+ ' ' + str(j) + ' possible opentext bigrams')
                q = equation(i, qwe11, j, aaa)
                result = decipher(q[0],q[1])
                if detectRussian.isRussian(result, wordPercentage=0, letterPercentage=85):
                print(result)
```