Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут ім. Ігоря Сікорського»
Фізико-технічний інститут

Лабораторна робота №3

З предмету «Криптографія»

Виконали:
Студенти 3 курсу,
ФТІ, групи ФБ-72
Курт Олег, Вовчук Роман

Київ 2019

Варіант 2

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 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.

Результати роботи:

a = 27

b = 211

Щоб відібрати саме цю пару ключів, нам треба було відфільтрувати розшифровані тексти, які мали заборонені біграми, тобто ті, які у ВТ зустрітися не можуть. Для цього ми створили функцію з такими забороненими біграмами: 'аь', 'оь', 'уь', 'еь', 'ыь', 'иь', 'эь', 'яь', 'юь', 'йь', 'йй', 'ьь', 'ыы'.

Біграми:

Відкритий текст	Закритий текст	Частота
на	рщ	0.006252
то	йа	0.009883
ен	юд	0.007261
но	юа	0.009076
ни	чш	0.008269

Зашифрований текст:

рйрщкагпрфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшющашдщныскющвпьюкджьйахещыйеьеюеэдсецчтыкйдшцчзюимевжшбушччэканылшолшкющчшэизупмзсбвжшбуойщаищмдпнрйуюфшхдтылшларюдезанпрбкажлащваэщюемечшщипнипнучбусхекайаэкяуклзщюгхегарпинцплппрффзшскыушщммеючогалчцпдшяуыуйацднфзхащаукйнхжукчщысаэарюжштнцмосхрхлтечшишваллмппртелиюдьпкуурдщерритыачтахщышкаюйзхцмздффнагещцлерьюбокцезацчучрйяыыунлсрорпрькрщэарючолаимхугшзепутэрщберояюазанхзушщимзсбючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйабеюемдвитылшошрщышгпфуыуйацдаюваллйыачларщзщроюалахдорцпиыщылшошрщйьфуйазлиекдвифущлбшашваллюсхщрохецщэирщэаэшуоьюдэисфуриыугшэпзлиекдкглаедюднфэщйдшгфчпрбердрйуюпнсабдпннхцмрцсдрпющкммьлеешбпымюенпчщроюабучштечшюдушлсбубеюыхрдщндщцфщейерйсдкммьофкаюйажйаидхйьнхерщхлкшьсжуиеишбпымюенпчщроюаеймюберояюарпинымжизаропйхлбшбуклзщзсэпюаиечшорэпьчкгипгекбхщжачойатеащваюдюдкйчбйкпмтырйюенщлучихечшчрпрфуклзщрусипнрйыуйаусйрпнцмшяхукчкйбвжшлжпшюечукемипнипцчушлсрйхпэснезщжмюдкенлхарпсдхйьчмэешйарпхппрэщцжьщпаюехдпьхуйанацчрбюдхушчкацкдщтеэдвиййтагшфичиорхлфдщфкшышвамносвиййдзьрыщыышхемсующудршджьюанхрэцпымздффнарписюахьхууочрфчгшйкпаюехдсджжгшцчтыкйдшнануэифуларизсййушфиюдюдаюышькющяпцлдчьншгашэлашьухаедвизлиекдвидщлсхпкеышйрьчценавсачэаькудбюяхцмрцсдрпгекммьлекдхйыуыщйаудюлцчисуюэиффриещжзьргшкдыууюьдглэшешберояючпщылпыщдшэасуйаьпымкуюсщгхелафитбюазуыщюаешуоналаолфдыууозмсдщьбукаощжзырыщаыпмяызшхпбыйацчзюимпелумсрйюасавдыугшбрмэтдйкяуришпчиоскчтхэейыосййричикзддрятарщроюазахачшфщчшурпрбуашькщепщчшфитдьчфщроюазацквснхтбьечшчыачешудкгхавклаяхбмхашнэпосюеюазнтдщьбудшщепщчшфикайаэкишныцмбээлучылшрщашошзсбужифчмэйкблкмоснфэщкыышрщхлиечширитэзалаеймюберояюарптылшщюцрчийщпаюеющчшхпэщхеишашйамущьбукаьэзхцмустдмшыщдшцчсдхйыуыщйаудчикабпсаюезлиекдффыршдчимшлчлэфуюазздрятачшсаюшчшййнцусюаьжхезнмшийщгпридщнйымюдкебдкйющешхщнкшлнуюсэебдьебпщьюарпжиегтдлэфщюенцдезаламдосусжулапасйюдаюнежсщьйкэытэшсосгпэпщепщчшфихехщюедшэпеемучщройкэысарепуосхасасйленкссвссеоамдосвпхрзшмейрцлтедчусхещцкемчььсдмэшсрморушнллирмффаыпмяызшщфзсййымзсхажалафщнпбупюоьюдкеещхщшпщяавцквснхтбьечшджпшюешпщьбуказаэплахщдщнйдщтечшджпшюешпщьбуэщшчсщряаюэщкацкышщехеаитбюарщлсцпэсеегпосщерпусдюйаюдбучихеэдэппртехарпеылегшмчхухаяютечшюдуссайщсллдыууокайасазаопчичпнхбморешэшсающуонафщгшмейррихушкдщнйдщтечшщукайаэкышхемчтэхевателуцчисхпкучызшщшмейряжпшюешпщьбудшоылшищгамуыщюаешлуьппрринхдщцадуришпчичифубелшмшмвкйуыгшхлвпьюзсййушфиюдпелучырйнхюайажлэщцжйацчушугрйхпцчсдьчфщроюаепжьюдмшеемучщроюазацчаябуащыщдшварчмэчинкныцмйквыдщлагчмэашзщэиьчщщчшмейртвещжзьргшкдтваыпмяызшыыдщнпщьбукачэрщмечшлжйазакмхйтвдебукчкйбвжшоыачлаоыьчмбюдпаюехдхввамнхукчкйбвжшгсйасандуссагшяснежсчикммьлезлиекдбюфшхдиырйгекбюдтдфчнцюдавлэкдусосйасадуклзщюдфчнцюдкемсуювпьюцкдщтечшэиащваейнцусюазблэчшгечофщгесаьпюачпжжпшюечуаюгарпсенуказаэпюазшлууросйасажлешзлйаудрйхрмэцпфжйахеродюыщжрпроппрчикммьлевлщднхбмнхшсзмгьхпэсрежаолфдыууофнрйнцусюазблэчшрщзщжащчтыкйкаешхакмхйтвжшусййушфиюдюдаюгпшгцчтыкйкающамджйазаддхухегарпцпбьюахщэдкгщыфутдаюащышэылшищяросчшмезахехщяпвсхйюдаюыущаидвцюдаюьичбзлцчтыкйэщышгыаччбзстдаюышхехаедюшзщрпщысагшлайеошцкнуфносачзюидцецчхйхажатечшжьйацчтыкйдшрщзщашчоыйыуйаусйрпнюлтевйвпрпгечпщачшкдььрмегфчпрбелшцающашчопаюебушщькышзшвыйафщышхпцмдрщыыуюехакчщуиезафнщыаччбзстдаюрщлаеебдкйлщйачнрйюблэчшшхнфрпющэплщцчсдфмчзьчжлаыпмяызшжхбмнхшсбужичлщерпюабуашькщыдщвйрмыулпбьйашдтыцмюарпхвцчьрдщгшашчоламчэичаэхшстдаюриэщйазнзсзшйшлшюагпчиеысагшлайезщайхлбшглэщйщчшчамеешвдбювсрэжичбзлэпрешхнфрплацсрчцпхюшрфчсимэоскгфуыйыхффэплщгарпсенуказарчыупмхуэсдммэтдяавдчишхтаичшзыйыуйаусйрпнушхакмюбпмншжлэщйщчшэирщлгерпюабуосйещеэдсечушгцмпнщьбукаюдуыдщимюдкечушгмщрщашщппрэщкырйдщьлщеющвпьюриюдюашдйржахетсййвпэсгпчинаькгшхпннзщццтвкчисжлзсйепртшййыуйаусйрпншдажйазмгьусффщлшрбезахемчтэлекмаюрщудеапамдосшсцпфжнлзуышюазреызшэатдрмхпщьбудшщыхубвчочпщаэщялчохехалюидвиаммсееапегкажлхедпрчиилмечшшшцкдщтечшчызшэатдрмлэчлрщнаэшэдкйчбйкишугрййкоыдднпрщышлсбубеаунккмнежскгцчтыкйкавйыуйаусйрпносфнзвюаиейркезаокйщгаынрйщызюимюдаюаыпмяызшцлгпшгцчтыкйкаяхбмщырйнхкелиачгшшдсдмэшсрмфукукчщгчилиачгшзсечмбрмфуэснарпзючшпмвпфчбшмейрпныургпзхцмчэиорщэаэшшщрщхезакдьрмьрпнхщшдькюедефщроошкаюрпркдуэуырцлхчээпмеидбюхахщимюдюарппьщсрплаэщкаюытэтедщпуэщвкюциулаэиыйхллланажаюусиппрсеэщюхыййаькэиеыйееуйафмыущфзщжбглщейеуозсащвашйымюдхунлищжанарпзючшбуосачиеэдщырйнхюахйщфрпешберояарущефпкезарчцптддчщфдщпуэщвкющньйашегахлтейицмрйыезаокнейжпэиэщгэхувлуоыуыщимфмйщпшйрщьйапахпьюаяофэхувлуолиачйахагаодвимдчитысазшйыжжйажлчпнхыезахаэасачшашйарокамейецыьпяйхеейыуйаусйрнфйщхлюеерффасхйюдкемдсилэгерпйклижуашрщщейечшвппршгцчтыкйканущефптачштэрщзщяпэптбьерпимюдкеслщещцримежагекаюрэпьчяфьеруюсхпымздюлщелшашфыымосьрчифшцкщедеюакайасажлнктешщэилиачгшопьчффкммьофпаюечэрщошбеюеюылшищгаясбрмэтдюадуклзщачисюарехеэдпрмэтдавнкхатешщашлиачгшдчьнчиипяыачжижуыщашащышгпридчьнрифусицлщеомхпипчушгмщрщашгшмейрсемьюдкеипгекбхщвпчпжжйаайхлзаейуюфщроошэщнхлыюаэпеямшщевлэияффубелшщфцчтыкйхрмсуювпьюышдшварчмэчиащварщэщйщчшэийщхатешщчшбущефпсдюдисфуидчиеапячщ

Розшифрований текст:

однакоэтакартинаскакойбысторонымыеенирассматривалирасплываетсявнечтонеопределенноеприпадкипроявляющиесярезкосприкусываниемусиливающиесядоопасного дляжизниприводящегоктяжкомусамокалечениюмогутвсежевнекоторыхслучаяхнедостигатьтакойсилыослабляясьдократкихсостоянийабсансадобыстропроходящихголово круженийимогуттакжесменятьсякраткимипериодамикогдабольнойсовершаетчуждыеегоприродепоступкикакбынаходясьвовластибессознательногообуславливаясьвобще мкакбыстранноэтониказалосьчистотелесными причинамиэтисостоянияМогутпервоначальновозникатьпопричинамчистодушевнымиспугилимогутвдальнейшемнаходиться взависимостиотдушевныхволнений какнихарактернодляогромногобольшинстваслучаевинтеллектуальноеснижениеноизвестенпокрайнеймереодинслучайкогдаэтотнедугн енарушилвысшийинтеллектуальнойдеятельностигельмгольцдругиеслучаивотношениикоторыхутверждалосьтожесамоененадежныилиподлежатсомнениюкакислучайсамо годостоевскоголицастрадающиеэпилепсиейМогутпроизводитьвпечатлениетупостинедоразвитоститаккакэтаболезньчастосопряженасярковыраженнымидиотизмомикрупн ейшимимозговымидефектаминеявляськонечнообязательнойсоставнойчастьюкартиныболезниноэтиприпадкисовсемисвоимивидоизмененияМибываютиудругихлицулицс полнымдушевнымразвитиемискореесосверхобычнаявбольшинствеслучаевнедостаточноуправляемойимиаффективностьюнеудивительночтопритакихобстоятельствахнев озможноустановитьсовокупностьклиническоюаффектаэпилепсиииточтопроявляетсяводнородностиуказанныхсимптомовтребуетповидимомуфункционального опониманияк акеслибымеханизманормальноговысвобожденияпервичныхпозывовбылподготовленорганическимеханизмкоторыйиспользуетсяприналичиивесьмаразныхусловийкакпри нарушениимозговойдеятельностипритяжкомзаболеванииткани ейилитоксическомзаболеваниитакипринедостаточномконтроледушевной экономиикризисномфункционирова ниидушевнойэнергиизаэтимразделениемнадвавидамычувствуемндентичностьмеханизмалежащеговосновевысвобожденияпервичныхпозывовэтотмеханизмнедалекиотсе ксуальныхпроцессовпорождаемыхвсвоейосноветоксическиужедревнейшиеврачиназываликоитусмалойэпилепсиейивиделивполовомактесмягчениеиадаптациювысвобожд ениязпилептическогоотводараздражения эпилептическаяреакциякаковымименемможноназватьвсеэтовместевзятоенесомненнотакжепоступаетивраспоряжениеневрозасущ ностькоторогвтомчтобыликвидироватьсоматическимассыраздраженияскоторыминеврознеможетсправитьсяпсихическиэпилептическийприпадокстановитсятакимобразо мсимптомомистерииеюадаптируетсяивидоизменяетсяподобнотомукакэтопроисходитпринормальномтечениисексуальногопроцессатакимобразоммысполнымправомразл ичаеморганическуюиаффективнуюэпилепсиюпрактическоезначениеэтогоследующеестрадающийпервойпораженболезньюмозгастрадающийвторойневротиквпервомслуч аедушевнаяжизньподверженанарушениюизвневовторомслучаенарушениеявляетсявыражениемсамойдушевнойжизнивесьмаверо ятночтоэпилепсиядостоевскогоотносится ковторомувидуточнодоказатьэтонельзятаккаквтакомслучаенужнобылобывключитьвцелокупностьегодушевнойжизниначалоприпадковипоследующиевидоизмененияэтих припадковадляэтогоунаснедостаточноданныхописанияс амихприпадковничегонедаютсведенияосоотношенияхмеждуприпадкамиипереживаниями инеполныичастопротиво речивывсеговероятнеепредположениечтоприпадкиначалисьудостоевскогоужевдетствечтоонивначалехарактеризовалисьболееслабымисимптомамиитолькопослепотрясше гоегопереживаниянавосемнадцатомгодужизниубийстваотцапринялиформуэпилепсиибылобывесьмауместноеслибыоправдалосьточтооноиполностьюпрекратилисьвовремя отбыванияимкаторгивсибириноэтомупротиворечатдругиеуказанияочевиднаясвязьмеждуотцеубийствомвбратьяхкарамазовыхисудьбойотцадостоевскогобросилась ьглазан еодномубиографудостоевскогоипослужилаимуказаниемнаизвестноесовременноепсихологическоенаправлениепсихоанализтаккакподразумеваетсяименноонсклоненвидет ьвэтомсобытиитягчайшуютравмуивреакциидостоевскогонаэтоключевойпунктегоневрозаеслияначуобосновыватьэтуустановкупсихоаналитическиопасаюсьчтоокажусьн епонятнымдлявсехтехкомунезнакомыучениеивыраженияпсихоанализаунасодиннадежныйисходныйпунктнамизвестенсмыслпервыхприпадковдостоевскоговегоюношеск иегодызадолгодопоявленияэпилепсииуэтихприпадковбылоподобиесмертиониназывалисьстрахомсмертиивыражалисьвсостоянииелтаргическогосна этаболезньнаходилана неговначалекогдаонбылещемальчикомкаквнезапнаябезотчетнаяподавленностьчувствокаконпозжерассказывалсвоемудругусоловьевутакоекакбудтобыемупредстоялосейч асжеумеретьивсамомделенаступалосостояниесовершенноподобноедействительнойсмертиегобратандрейрассказывалчтофедоружевмолодыегодыпередтемказаснутьостав лялзаписькичтобоитсяночьюзаснутьсмертоподобнымсномипроситпоэтомучтобыегопохоронилитолькочерезпятьднейдостоевскийзарулеткойвведениеснамизвестнысмысли намерениетакихприпадковсмертониозначаютотождествлениесумершимчеловекомкоторыйдействительноумерилисчеловекомживымещенокоторомумыжелаемсмертивто ройслучайболеезначителенприпадоквуказанномслучаеравноценненнаказаниюмыпожелалисмертидругомутеперьмысталисамиэтимдругимисамиумерлитутпсихоаналитиче скоеучениеутверждаетчтоэтотдругойдлямальчикаобычноотецииименуемыйистериейприпадокявляетсятакимобразомсамонаказаниемзапожеланиесмертиненавистномуотц уа

Програмний код:

```
import collections
def bezout(a, b):
    c = b
    x, xx, y, yy = 1, 0, 0, 1
    while b:
        q = a // b
        a, b = b, a % b
        x, xx = xx, x - xx*q
        y, yy = yy, y - yy*q
    if x < 0:
        x = c + x
    if a == 1:
        return x
    else:
        print("revers element don't exist")
        return -a
def lin_equation(x1, x2, y1, y2, a_b, open1, close1, open2, close2):
    y = y1 - y2
    x = x1 - x2
    xx = bezout(x, 961)
    u = int
    if xx <= 0:
        xx *= -1
        print('xx = ' + str(xx))
        if y % xx == 0:
            y /= xx
            reversx = bezout(x/xx, 961/xx)
            x0 = (y*reversx) % (961/xx)
            i = 0
            while i != xx:
                a_b[0] = int(x0 + 961/xx*i)
                print('a = ' + str(a_b[0]))
                a_b[2] = int(bezout(a_b[0], 961))
                print('a^(-1) = ' + str(a_b[2]))
                a_b[1] = int((y1 - a_b[0] * x1) % 961)
                print('b = ' + str(a_b[1]))
                i += 1
                u = decrypt(a_b[2], a_b[1], text_file)
                print('Bigramms ' + open1 + ' ' + close1 + ' ::: ' + open2 + ' ' + close2)
            return u
        else:
            print('lin_equation don`t have answers')
            return 0
```

```
    a_b[0] = (xx*y) % 961
    print('a = ' + str(a_b[0]))
    a_b[2] = bezout(a_b[0], 961)
    if a_b[2] < 0:
        return 0
    print('a^(-1) = ' + str(a_b[2]))
    a_b[1] = (y1 - a_b[0]*x1) % 961
    print('b = ' + str(a_b[1]))
    u = decrypt(a_b[2], a_b[1], text_file)
    print('Bigramms ' + open1 + ' ' + close1 + ' ::: ' + open2 + ' ' + close2)
    return u
def decrypt(a, b, cipher):
    bm = str()
    decipher = ''
    for letter_text in cipher + '.':
        if len(bm) == 2:
            decipher += bigramms[a*(bigramms.index(bm) - b) % 961]
            bm = ''
            bm += letter_text
        else:
            bm += letter_text

    if content(decipher):
        print(decipher)
        file_enc.write(decipher + '\n\n\n\n\n')
        return 1
    return 0
def content(text):
    impossible = ['аь', 'оь', 'уь', 'еь', 'ыь', 'иь', 'эь', 'яь', 'юь', 'йь', 'йй', 'ьь', 'ыы']

    for bigram in impossible:
        if bigram in text:
            print(bigram)
            return False
    return True
def full(common, popular):
    a_b = [0, 0, 0]
    s = 0
    while s != 5:
        k = 0
        while k != 5:
            i = 0
            if s == k:
                if k == 4:
                    break
                else:
                    k += 1
            while i != 6:
                j = 0
                while j != 6:
                    if i == j:
                        if j == 5:
                            break
                        else:
                            j += 1
                    c = lin_equation(bigramms.index(popular[s]), bigramms.index(popular[k]), bigramms.index(common[i]),
                                     bigramms.index(common[j]), a_b, popular[s], common[i], popular[k], common[j])
                    if c == 1:
                        return 1
                    j += 1
                i += 1
            k += 1
        s += 1
def bigrams():
    list_key = list()
    bigram = str()

    for letter_text in text_file + '.':
        if len(bigram) == 2:
            dict_bigram[bigram] += 1
            bigram = ''
            bigram += letter_text
        else:
            bigram += letter_text
    list_bigram = list(dict_bigram.values())
    for i in range(6):
        value = list_bigram.pop(list_bigram.index(max(list_bigram)))
        for key, val in dict_bigram.items():
            if val == value:
                list_key.append(key)
                break
    return list_key
def create_mass(leng, mass, dicti):
    ll = 0
    x = 0
    for l in range(leng):
        kk = 0
```

```
        for k in range(leng):
            dicti.extend([mass[ll] + mass[kk]])
            x += 1
            kk += 1
        ll += 1
file_enc = open("D:/Files/Python/cp3/encrypted.txt", "w", encoding='utf-8')
arr = open("D:/Files/Python/cp3/arr.txt", "w", encoding='windows-1251')
file = open("D:/Files/Python/cp3/02.txt", "r")
text_file = file.read()
most_common_bigramms = ['ст', 'но', 'ен', 'то', 'на']
dict_no_probels = ['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']
bigramms = []
create_mass(31, dict_no_probels, bigramms)
dict_bigram = collections.Counter()
most = bigrams()
ii = 0
while ii != 961:
    arr.write(str(ii) + bigramms[ii] + ' ')
    ii += 1
full(most, most_common_bigramms)
file.close()
```

Висновок:

Під час данного комп’ютерного практикума ми набули навички частотного аналізу на прикладі розкриття моноалфавітної підстановки та опанували прийомами роботи в модулярній арифметиці.