

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконали: ФБ-11 Мельниченко Богдан, Захаренко Нікіта

Варіант: 8

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 елемента 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.

Хід роботи:

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елемента 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

```
def euclid(a, b):
    if a == 0:
        return b, 0, 1
    else:
        g, x, y = euclid(b % a, a)
        return g, y - (b // a) * x, x

def solver(a, b, mod=31):
    g = gcd(a, mod)
    if g == 1:
        return [(euclid(a, mod)[1] * b) % mod]
    elif g > 1:
        if b % g != 0:
            return None
        x0 = (euclid(a // g, mod // g)[1] * (b // g)) % (mod // g)
        roots = []
        for i in range(g):
            roots.append(x0 + i * (mod // g))
        return roots
```

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

```
no spaces no  
[('жц', 36),  
 ('дэ', 35),  
 ('цэ', 35),  
 ('ыб', 30),  
 ('оц', 28),
```

3-5

Текст виводиться лише у тому випадку коли відсутні неможливі словосполучення у російській мові

```
net = ['аь', 'еь', 'юь', 'яь', 'эь', 'юь', 'яь', 'оь', 'иь', 'ыь', 'уь', 'аь', 'эь', 'ць', 'хь', 'кь', 'оь', 'иь', 'ыь', 'уь', 'еь']
```

Текст було розшифровано ключем (17, 94)

Розшифрований текст:

мальчикизаулыбалисьисжаромвзялисьзаделоонирвализолотистыецветыцветычтонаводняютвесьми
рпереплескиваютсяслужакнамогильныестроенияхонькостучатсявпрозрачныеокнапогребовнезнают
угомонуиудерживсевокругзаливаютсялепящимсверканиемрасплавленногосолнцакаждоелетоонито
чносцеписрываютсясказалдедушкапустыхянепротиввонихсколькостоятгордыекакльвыпосмотриш
ьнанихподольштакипрожгутутебявглазахдыркуведьпростойцветокможносказатьсорнаятраваникт
оенезамечаетамыуважаемсчитаемодуванчикблагородноерастениеонинабралиполнымешкиодува
нчиковиунесливнизпогребывалиилиихизмешковивотъмепогребаразлилосьсияниевинныйпрессдо
жидалсяихоткрытыйхолодныйзолотистыйпотоксогрелегодедушкапередвинулпрессповернулручку
завертелбыстрейбыстрейипрессмягкостиснулдобычунувотвоттаксперватонкойструйкойпотомвсещ
едреобильнеепопобежалпожелобувглиняныекувшинысокпрекрасногожаркогомесяцаемудалиперебр
одитьснялипенуиразлиливчистыебутылкиизподкетчупаионивыстроилисьрядаминаполкахпоблески
ваявсумракепогребавиноизодуванчиковсамыеэтисловаточнелетонаязыкевиноизодуванчиковпойма
нноеизакупоренноебутылкилетоитеперькогдадугласзналпонастоящемузналчтоонживойчтоонзате
миходитпоземлетобывидетьиощущатьмиронпонялещеоднадочастицувсегчтоонозналчастицуэ
тогоособенногдняднясбораодуванчиковтожезакупоритьисохранитьапотомнастанеттакойзимнийя
нварскийденькогдавалитгустойснегисолнцаужедавнымдавнониктоневидалможетбытьэточудопоз
абылосьиххорошобыегосновавспомнитьвоттогдаоногооткупоритьведьэтолетонепременнобудетлетом
нежданныхчудесинадосеихсберечьигдетоотложитьдлясебячтобыпослелюбойчаскогдавздумаешь
пробратсьянацыпочкахвовлажныйсумракипротянутьрукуитамрядзарядомбудутстоятьбутылкисвин
номизодуванчиковонбудетмягкомерцатьточнораскрывающиесяназаревцвetyасквозьтонкийслойпыл
ибудетпоблескиватьсолнценынешнегоиюнявзглянисквозьэтовинонахолодныйзимнийденьиснеграс
таетизподнегопокажетсятраванадеревьяхоживутптицылистваицветысловномирадыбабочекзатреп
ещутнаветруидажехолодноесероенебостанетголубымвозьмилетоврукуналейлетовбокалвсамыйкро
хотныйконечноизкакоготолькоисделаешьединственныйтерпкийглотокподнесиегокубамипожилам
твоимвместолютотзимыпобежитжаркоелетотеперьдождевойводыконечноздесьгодитсятолькочисте
йшаяводадальнихозерсладоствыеросыбархатныхлуговчтовозносятсяназарекраспахнувшимсянавст
речунебесамтамвпрохладныхвысяхонисобиралисьчистоомытымигроздамиветермчалихзасотними
льзаряжаяпопутиэлектрическимизарядамиэтавадовбравкаждуюсвоюкаплюещебольшенебеског
дападаладождемназемлюонапиталавсебявосточныйветеризападныйисеверныйиюжныйиобратила
сьвдождьадождьвэтотчассвященнодействияужестановитсятерпкимвиномдуглассхватилковшвыбе
жалводвориглубокопогрузилеговбочоноксдождевойводойвотонаводабылаточношелкпрозрачныйго
лубоватыйшелкеслиеевыпитьонакоснетсягубгорласердцамягкокакласканокковшиполноеведронадоо
тнестивпогребчтобыводапропиталатамвесьурожайодуванчиковструямиречекигорныхручьевдажеб

абушкавакойнибудьфевральскийденькогдабеснуетсязаокномвьюгаислепитесьмириулюдейзахватываетдыханьедажебабушкатихонькоспуститсявпогребнаверхувбольшомдомебудеткашельчиханье хриплоголосаистоныпростуженнымдетямоченьбольнобудетглотатьаносыунихпокраснеютточно в ишнихвынутыеизналивкисюдувдомепритаютсяковарныймикробитогдаизпогребавозникнетточнобо гинялетабабушкапрячтототоподвязанойшальюонапринесетэтотототовкомнатукаждогоболящегоира зольетдушистоепрозрачноевпрозрачныестаканыистаканыэтиосушатоднимглоткомлекарствоиныхв ременбалзамизсолнечныхлучейипраздногоавгустовскогополудняедваслышныйстукколестележки смороженымчтокатитсепомощенумулицамшорохсеребристогофейерверкачторассыпаетсявысоков небишелестрезаннойтравыфонтаномбьющейизподкосилкичтодвижетсяполугампомуравьиномуц арствувсеэтовсеводномстаканедадажебабушкакогдаспуститсявзимнийпогребзайонемнавернобуде тстоятьтамтихонькосовсемоднавтайномединенииисвоимсокровеннымсвоейдушойкакидедушка ипапаидядябертидругиетожесловнобеседуястеньюдавноушедшихднейспикникамитеплымдождем сзапахомпшеничныхполейижареныхкукурузныхзеренисвежескошенногосенадажебабушкабудетпо вторятьсясноваисноватежечудесныезолотящиесясловачтозвучатсейчаскогдацветыкладутподпресска кбудутихповторятькаждуюзимувсебелыезимывовсевременасноваисноваонибудутслетатьсгубкакул ыбкакакнежданныйсолнечныйзайчиквотмевиноизодуванчиковвиноизодуванчиковвиноизодуванч иковониприходилинеслышноуходилипочтибесшумнотравапригибаласьираспрямляласьвновьониск ользиливнизпохолмамточнотениоблаковэтобежалилетниемальчишкидугласотстализблудилсязад ыхаясьотбыстрогобегаоностановилсянакраюовраганасамойкромкенадпропастьюиоттудаанегодох нулохолодомнавостривушиточнооленьонвдругучаялстаруюкакмиропасностьгородраспалсяздесьна двеполовиныздеськончиласьцивилизацияздесьживетлишьвспухшаяземляжечасносовершаетсямил лионсмертейирожденийиздесьпроторенныеилиещенепроторенныетропытвердятчтобыстатьмужчи намимальчишкидолжныстранствоватьвсегдавсюжизньстранствоватьдугласобернулсэтатропаогро мнойпыльнойзмеейскользиткледяномудомугдезолотыелетниеднипрячтсязимаатабежиткраскале ннымпесчанымберегамиюльскогоозераавонтакдеревьямгдемальчишкипрячутсямежлистьевточнот ерпкиещенезрелыеплодыдикойяблониитамастутизреютавотэтакперсиковомусадкувинограднику когороднымгрядамгдедремлютнасолнцеарбузыполосатыесловнокошкитигровоймастиэтатропазаре сшаякапризнаязивлистаятнетсяякшколеатапрямаякакстрелаксуботнимутренникамгдепоказываю тковбойскиефильмывотэтавдольручьядикойлеснойчащедугласажмурилсяктоскажетгдекончается городиначинаетсялеснаяглушьктоскажетгородврастаетвнеелионапереходитвгородиздавнинавек исуществуетнекаянеуловимаяграньгдеборютсядвесилииоднанавремяпобеждаетизавладеваетпросе койлощинойлужайкойдеревомкустомбескрайнееморетравицветовплещетсядалековполяхвокругоди нокихфермалетомзеленыйприбойяростноподступаетксамомугородуночьзаночьючащилугадальные просторыстекаютпооврагувсеближезахлестываютгородзапахомводыитравигородсловнопустеетмер твеитивновьюходитвземлюикаждоеутрооврагещеглубжевгрызаетсявгородигрозитпоглотитьгаражи точнодырвыелодчонкиипожратьдопотоппыеавтомобилиоставленныеамилостьдождяиразедаемы ержавчинойэяусквозьтайныоврагаигородаивременимчалисьджонхафичарливудменэйдугласмедле ннодвинулсяпотропинкеконечноеслихочешьпосмотретьнадвесамыеглавныеветшикакживетчеловек икакживетприроданадоприйтисюдаковрагуведьгородвконцеконцоввсеголишьбольшойпотрепанны йбурямикорабльнанемполнонародуивсехлопочутбезусталивычерпываютводуобкалываютржавчин упоройкакаянибудьшлюпкахибаркадетищекораблямтоенеслышнойбурейвременитонетвмолчали выхволнахтермитовимуравьеввраспахнутойовражьейпастичтобыощутитькакмелькаюткузнечикии шуршатвжаркихтравахточносухаябумагачтобыоглохнутьподпеленойтончайшейпылиинаконецпрух нутьградомкамнейипотокомсмолыкакрушатсятлеющиеугликиостразажженногогромамисинеймолн иейнамигозарившейторжестволесныхдебрейтаквотзначитчтотянулосьдадугласатайнавойначелов екасприродойизгодавгодчеловекпохищаетчтотоуприродыаприродавновьберетсвоеиникогдагородп онастоящемудоконцанепобеждаетвечноемугрозитбезмолвнаяопасностьонвооружилсякосилкойтия пкойогромныминожницамионподрезаеткустыиопрыскиваетдомвредныхбукашекигусеницонупря моплыветвпередпокаемувелитцивилизациянокаждыйдомтогоиглядизахлестнутзеленыеволныисхо ронятнавекикакогданибудьслицаземлиисчезнетпоследнийчеловекиегокосилкиисадовыелопатыизед енныержавчинойрассыплотсявпрахгородчащадомаоврагдугласозадаченномигаебнокакаяжесвязьм ежчеловекомиприродойкакпонятьчтозначатонидругдлядругакогдаонопустилглазапервыйлетнийоб рядпозадиодуванчикисобранныизаготовленывпрокпораприступатьквторомунодугласастылинедви

жетсясместадугпошлидугголосазатихливдалекеяживойсказалдугласночтотолкуниещебольшежив
ычемеякакжеэтокакжетаконстоялводиночествеглядянасвоиногиневсилахдвинутьсясместаинаконец
понялвтотвечердугласвозвращалсядомойизкиновместесродителямиибратомтомомиувиделихвярко
освещеннойвитринемагазинатеннисныетуфлидугласпоспешноотвелглазаноегоногиужеощутилипр
икосновениепарусиныизаскользилиповоздухубыстрейбыстрейземлязавертеласьзахлопалиполотня
ныенавесынадвитринамитаконподнялветертаконмчалсяродителиитомшагалинеторопясьажежду
нимипятысязадомшелдугласинесводилглазстенисныхтуфельтампозадивполночнойвитринехоро
шаябылакартинасказаламамаагабуркнулдугласстоялионьдавноминовалотовремякогдааналетопокуп
аюттакиетуфлилегкиеитихиеточныйтеплыйдождьчтошуршитпотротуарамужеиюньземляполнаперв
озданнойсилыивсевокругдвижетсяирастетттраваипосейденьпереливаетсясюдаизлугомывайтроту
арыподступаеткдомамкажетсягородвотвотчерпнетбортомипокорнопойдетнадноивзеленомморетра
внеостанетсянивсплесканирябидугласвдругзастылточновросвмертвыйасфальтикрасныйкирпичули
цыневсилахтронутьсясместапапвыпалионвонтамвокнетеннисныетуфлиотецдажеповернулсяазач
емтебеновыетуфлиискажипожалуйстаможешьтымнеобъяснитьнуудазатемчтовнихчувствуешьсебятак
будтовпервыевэтолетоскинулбашмакиипобежалбосикомпотраветочновзимнююночьвысунулноги
зподтеплогоодеялаиподставилветручтодышитхолодомвоткрытоеокноониистынутстынутапотомтя
гиваешьихобратнопододеялоониисовсемкаксосулькивтеннисныхтуфляхчувствуешьсебятакбудтов
первыевэтолетобредешьбосикомполенивомуручьюивпрозрачнойводевидишькактвоиногиступаютп
однубудтоонипереломилисьидвижутсячутьвпередтебяпотомучтоведьвводевсевидитсянетакпапск
азалдугласэтооченьтруднообъяснить

Висновок:

Під час виконання лабораторної роботи ми навчилися використовувати методи частотного аналізу, використовуючи моноалфавітну підстановку як приклад. Також ми освоїли прийоми роботи з модулярною арифметикою. Здійснюючи частотний аналіз, ми виявили п'ять найчастіших біграм у зашифрованому тексті та визначили кандидатів на ключ шляхом аналізу частотних біграм мови та шифртексту. Застосовуючи розпізнавач російської мови, ми успішно визначили вірний ключ і здійснили розшифрування смислового тексту.