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:

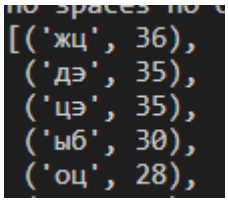
1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.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

Хід 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

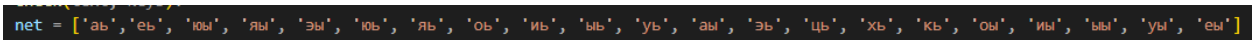
```python
def euclid(a, b):
    if a == 0:
        return b, 0, 1
    else:
        g, x, y = euclid(b % a, a)
        return g, y - (b // a) * x, x

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

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



3-5

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



Текст було розшифровано ключем **(17, 94)**

Розшифрований текст:

мальчикизаулыбалисьисжаромвзялисьзаделоонирвализолотистыецветыцветычтонаводняютвесьми рпереплескиваютсяслужаекнамощеныеулицытихонькостучатсявпрозрачныеокнапогребовнезнают угомонуиудержуивсевокругзаливаютслепящимсверканиемрасплавленногосолнцакаждоелетоонито чносцеписрываютсяскazалдедушкапустьихянепротиввонихсколькостоятгордыекакльвыпосмотриш ьнанихподольшетакипрожгутутебявглазахдыркуведьпростойцветокможносказатьсорнаятраваникт оеенезамечаетамыуважаемсчитаемодуванчикблагородноерастениеонинабралиполныемешкиодува нчиковиунесливнизвпогребвывалилиихизмешковивотьмепогребаразлилосьсияниевинныйпрессдо жидалсяихоткрытыйхолодныйзолотистыйпотоксогрелегодедушкапередвинулпрессповернулручку завертелбыстрейбыстрейипрессмягкостиснулдобычунувотвоттаксперватонкойструйкойпотомвсещ едреeобильнеепобежалпожелобувглиняныекувшинысокпрекрасногожаркогомесяцаемудалиперебр одитьснялипенуиразлиливчистыебутылкиизподкетчупаионивыстроилисьрядаминаполкахпоблески ваявсумракепогребавиноизодуванчиковсамыеэтисловаточнолетонаязыкевиноизодуванчиковпойма нноеизакупоренноевбутылкилетоитеперькогдадугласзналпонастоящемузналчтоонживойчтоонзате миходитпоземлечтобывидетьиощущатьмиронпонялещеоднонадочастицувсегочтоонузналчастицуэ тогоособенногоднядняснбораодуванчиковтожезакупоритьисохранитьапотомнастанеттакойзимнийя нварскийденькогдавалитгустойснегисолнцаужедавнымдавноникtоневиделиможетбытьэточудопоз абылосьихорошобыегосновавспомнитьвоттогдаонегооткупоритведьэтолетонепременнобудетлетом нежданныхчудесинадовсеихсберечьигдетоотложитьдлясебячтобыпослевлюбойчаскогдавздумаешь пробратьсянацыпочкахвовлажныйсумракипротянутьрукуитамрядзарядомбудутстоятьбутылкисвин омизодуванчиковонобудетмягкомерцатьточнораскрывающиесяназарецветыасквозьтонкийслойпыл ибудетпоблескиватьсолнценынешнегоиюнявзглянисквозьэтовинонахолодныйзимнийденьиснеграс таетизподнегопокажетсятраванадеревьяхоживутптицылиствaицветысловномириадыбабочекзатреп ещутнаветруидажехолодноесероенебостанетголубымвозьмилетоврукуналейлетовбокалвсамыйкро хотныйконечноизкакоготолькоисделаешьединственныйтерпкийглотокподнесиегокгубамипожилам твоимвместолютойзимыпобежитжаркоелетотеперьдождевойводыконечноздесьгодитсятолькочисте йшаяводадальнихозерсладостныеросыбархатныхлуговчтовозносятсяназарекраспахнувшимсянавст речунебесамтамвпрохладныхвысяхонисобиралисьчистоомытымигроздьямиветермчалихзасотними льзаряжаяпопутиэлектрическимизарядамиэтаводавобралавкаждуюсвоюкаплюещебольшенебеског дападаладождемназемлюонавпиталавсебявосточныйветеризападныйисевернyйиюжныйиобратила сьвдождьадождьвэтотчассвященнодействияужестановитсятерпкимвиномдуглассхватилковшвыбе жалводвориглубокопогрузилеговбочоноксдождевойводойвотонаводабылаточношелкпрозрачныйго лубоватыйшелкеслиеевыпитьонакоснетсягубгорласердцамягкокакласканоковшиполноеведронадоо тнестивпогребчтобыводапропиталатамвесьурожайодуванчиковструямиречекигорныхручьевдажеб

абушкавкакойнибудьфевральскийденькогдабеснуетсязаокномвьюгаислепитвесьмириулюдейзахват
ываетдыханьедажебабушкатихонькоспуститсявпогребнаверхувбольшомдомебудеткашельчиханье
хриплыеголосаистоныпростуженнымдетямоченьбольнобудетглотатьаносыунихпокраснеютточнов
ишнивынутыеизналивкивсюдувдомепритаитсяковарныймикробитогдаизпогребавозникнетточнобо
гинялетабабушкапрячатотоподвязаной шальюонапринесетэточтотовкомнатукаждогоболящегоира
зольетдушистоепрозрачноевпрозрачныестаканыистаканыэтиосушатоднимглоткомлекарствоиныхв
ременбальзамизсолнечныхлучейипраздногоавгустовскогополудняедваслышныйстукколестележки
смороженымчтокатитсяпомощеныумулицамшорохсеребристогофейерверкачторассыпаетсявысоков
небеишелестсрезанной йтравыфонтаномбьющейизподкосилкичтодвижетсяполугампомуравьиномуц
арствувсеэтовсеводномстаканедадажебабушкакогдаспуститсявзимнийпогребзаиюнемнавернобуде
тстоятьтамтихонькосовсемоднавтайномединениисосвоимсокровеннымсосвоейдушойкакидедушка
ипапаидядябертидругиетожесловнобеседуястеньюдавноушедшихднейспикникамистеплымдождем
сзапахомпшеничныхполейижареныхкукурузныхзеренисвежескошенногосенадажебабушкабудетпо
вторятьсноваисноватежечудесныезолотящиесяслововчтозвучатсейчаскогдацветыкладутподпресска
кбудутихповторятькаждуюзимувсебелыезимывовсевременасноваисноваонибудутслетатьсгубкакул
ыбкакакнежданныйсолнечныйзайчиквотьмевиноизодуванчиковвиноизодуванчиковвиноизодуванч
иковонеприходилинеслышноуходилипочтибесшумнотравапригибаласьираспрямляласьвновьониск
ользиливнизпохолмамточнотениоблаковэтобежалилетниемальчишкидугласотстализаблудилсязад
ыхаясьотбыстрогобегаоностановилсянакраюовраганасамойкромкенадпропастьюиоттуданенегодох
нулохолодомнавостривушиточнооленьонвдругучуялстаруюкакмиропасностьгородраспалсяздесьна
двеполовиныздесьокончиласьцивилизацияздесьживетлишьвспухшаяземляежечасносовершаетсямил
лионсмертейирожденийиздесьпроторенныеилиещенепроторенныетропытвердятчтобыстатьмужчи
намимальчишкидолжныстранствоватьвсегдавсюжизньстранствоватьдугласобернулсяэтатропаогро
мнойпыльнойзмеейскользиткледяномудомугдевзолотыелетниеднипрячетсязимаатабежиткраскале
ннымпесчанымберегамиюльскогоозераавонтакдеревьямгдемальчишкипрячутсямежлистьевточнот
ерпкиеещенезрелыеплодыдикойяблониитамрастутизреютавотэтакперсиковомусадуквиноградniку
когороднымгрядамгдедремлютнасолнцеарбузыполосатыесловнокошкитигровоймастиэтатропазаро
сшаякапризнаяизвилистаятянетсякшколеатапрямаякакстрелаксубботнимутренникамгдепоказываю
тковбойскиефильмывотэтавдольручьякдикойлеснойчащедугласзажмурилсяктоскажетгдекончается
городиначинаетсялеснаяглушьктоскажетгородврастаетвнееилионапереходитвгородиздавнаинавек
исуществуетнекаянеуловимаяграньгдеборютсядвесилыиоднанавремяпобеждаетизавладеваетпросе
койлощинойлужайкойдеревомкустомбескрайнееморетравицветовплещетсядалековполяхвокругоди
нокихфермалетомзеленыйприбойяростноподступаетксамомугородуночьзаночьючащилугадальние
просторыстекаютпооврагувсеближезахлестываютгородзапахомводыитравигородсловнопустеетмер
твеетивновьуходитвземлюикаждоеутрооврагещеглубжевгрызаетсявгородигрозитпоглотитьгаражи
точнодырявыелодчонкиипожратьдопотопныеавтомобилиоставленныенамилостьдождяиразедаемы
ержавчинойэйаусквозьтайныоврагаигородаивременимчалисьджонхафичарливудменэйдугласмедле
ннодвинулсяпотропинкеконечноеслихочешьпосмотретьнадвесамыеглавныевещикакживетчеловек
икакживетприроданадоприйтисюдаковрагуведьгородвконцеконцоввсеголишьбольшойпотрепанны
йбурямикорабльнанемполнонародуивсехлопочутбезусталивычерпываютводуобкалываютржавчин
упоройкакаянибудьшлюпкахибаркадетищекораблясмытоенеслышнойбурейвременитонетвмолчали
выхволнахтермитовимуравьеввраспахнутойовражьейпастичтобыощутитькакмелькаюткузнечикии
шуршатвжаркихтравахточносухаябумагачтобыоглохнутьподпеленойтончайшейпылиинаконецрух
нутьградомкамнейипотокомсмолыкакрушатсятлеющиеугликостразажженногогромомисинеймолн
иейнамигозарившейторжестволесныхдебрейтаквотзначитчтотянулосюдадугласатайнаявойначелов
екаприродойизгодавгодчеловекпохищаетчтотоуприродыаприродавновьберетсвоеиникогдагородп
онастоящемудоконцанепобеждаетвечноемугрозитбезмолвнаяопасностьонвооружилсякосилкойитя
пкойогромныминожницамионподрезаеткустыиопрыскиваетядомвредныхбукашекигусеницонупря
моплыветвпередпокаемувелитцивилизациянокаждыйдомтогоиглядизахлестнутзеленыеволныисхо
ронятнавекиакогданибудьслицаземлиисчезнетпоследнийчеловекиегокосилкиисадовыелопатыизед
енныержавчинойрассыплютсявпрахгородчащадомаоврагдугласозаданномигаетнокакаяжесвязьм
ежчеловекомиприродойкакпонятьчтозначатонидругдлядругакогдаонопустилглазапервыйлетнийоб
рядпозадиодуванчикисобраныизаготовленывпрокпораприступатьковторомунодугласзастылинедви

жетсясместадугпошлидугголосазатихливдалекеяживойсказалдугласночтотолкуониещебольшежив
ыечемякакжеэтокакжетаконстоялводиночествеглядянасвоиногиневсилахдвинутьсясместаинаконец
понялвтотвечердугласвозвращалсядомойизкиновместесродителямиибратомтомомиувиделихвярко
освещеннойвитринемагазинатеннисныетуфлидугласпоспешноотвелглазаноегоногиужеощутилипр
икосновениепарусиныизаскользилиповоздухубыстрейбыстрейземлязавертеласьзахлопалиполотня
ныенавесынадвитринамитакойонподнялветертаконмчалсяродителиитомшагалинеторопясьамежду
нимипятясьзадомшелдугласинесводилглазстеннисныхтуфельтампозадивполуночнойвитринехоро
шаябылакартинасказаламамаагабуркнулдугласстоялиюньдавноминовалотовремякогданалетопокуп
аюттакиетуфлилегкиеитихиеточнотеплыйдождьчтошуршитпотротуарамужеиюньиземляполнаперв
озданнойсилыивсевокругдвижетсяирастеттраваипосейденьпереливаетсясюдаизлуговомываеттроту
арыподступаеткдомамкажетсягородвотвотчерпнетбортомипокорнопойдетнадноивзеленомморетра
внеостанетсянивсплесканирябидугласвдругзастылточновросвмертвыйасфальтикрасныйкирпичули
цыневсилахтронутьсясместапапвыпалилонвонтамвокнетеннисныетуфлиотецдаженеобернулсяазач
емтебеновыетуфлискажипожалуйстаможешьтымнеобяснитьнуудазатемчтовнихчувствуешьсебятак
будтовпервыевэтолетоскинулбашмакиипобежалбосикомпотраветочновзимнююночьвысунулногии
зподтеплогоодеялаиподставилветручтодышитхолодомвоткрытоеокноионистынутстынутапотомвтя
гиваешьихобратнопододеялоионисовсемкаксосулькивтеннисныхтуфляхчувствуешьсебятакбудтов
первыевэтолетобредешьбосикомполенивомуручьюивпрозрачнойводевидишькактвоиногиступаютп
однубудтоонипереломилисьидвижутсячутьвпередитебяпотомучтоведьвводевсевидитсянетакпапск
азалдугласэтооченьтруднообяснить

Висновок:

Під час виконання лабораторної роботи ми навчились 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.