

СИМЕТРИЧНА КРИПТОГРАФІЯ КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

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 No1, знайти 5 найчастіших біграм запропонованого шифротексту (за варіантом).
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифротексту (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 шифротекст. Якщо шифротекст не є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним. У разі необхідності змінити кодування алфавіту (див. методичні вказівки).

Хід роботи:

Після прочитання методичних вказівок перейшли до допрограми етапу, а саме з лабораторної роботи 1 було визначено: найчастіші біграми шифротексту: "ще", "хе", "чв", "ле", "цв", "ощ", "сд", "же", "де", "гд"

Та найчастіші біграми мови:

"ен", "на", "то", "но", "ст"

Реалізовано допоміжні методи з потрібною арифметикою і методи для перебору співставлення отриманих біграм і знайдено кандидати ключів, після чого для розв'язку системи знайдено дешифрування.

Шифротекст:

ывлеюгзебщпещхщуйэвиывиюфгувхцубхщыюнюжлепэшфмиьхдощбуднзе
гдщебоцвшуюгьпцвэщувкмзеиэбчиюндхщюасдбмонхегщгдэщжезьщемво
щфысьмайыегыйййыэшжеаекидщцеюжгдеьцонгочвнюиюыжвюудеьбюг
ьщесфвшвоююзйэяцкцьюгочвнюлмшужеейцурпцвдэяхщаюьдеуэвющэвдиа
ййтвепцвчвлеюйщецыаешвэеяикгехщаэациэибвкмрйжуажййдекушттепэшф
мздсугьвоцвайкзфтшшхдуюиьынюгдхацовойэращеюияцияаимюыжцввдж
вяцэвлломоодмхщуйэмюэзопюзкнэщегбдсефвхбжщенюцатщввэиегтеаех
охтйолдицзьхдщщюяьзщюоцвлеюосдлузлащавызйферддьюмоуаььеп
жмнюбжщцаещэойтзэвзвщупмюжьощаощвыжееююззьдеаейюшдоездю
йбпгьвиюэколпщхмоихсшфеэмлеотзомщйвхцыбжжебахиэьщхйэашжеттфе
лежебдфюфпнюфмшуиэжяппшдгдщесдцжцвхеюцхеднвжееютбзийысддем
илпмюзахшнюллуюэпподйшяюьхщужуиуцтабзлзьюпнбоящпиэцииамле
нйхдбднвнщлврпшилмиьадшахушайыэффтппмюцдсзезцадцьцихжшугфб
иэихеныжпбоцднесдегмаущйыктгдыйктийнвмоктздгидатаомтщлвхейрди
мяцшуьюывмтшзюашнэьгоэавюрдвджгмпиеэщеиэивдодзехатщйыэшзшзу
нзщхеюизчсдэайэхенвжьфжпсхгчплвжмвиртдэппшуртцюиэппедчйдешорп
дпвюбжлотвдюлофехщыддетеодаьюяхрдбмлпнднелышхдощуцщазнибыу
твднтащебацэзьгордфесьаещзкнсднюятьдаахмчвюцхеиовющежемпзькюжя
мюгыщцсбвдсчепзлепэшбмтвгоэвубюзмвппцинэзьэштапуиэпхлеоенщнщрд
эщлабмхтфуиноййаещэдэвлнюцрпбжэщыдидсдщохилпийшгмищцвюбйощяа
педмлсгцатьчщбуэьгйцамиэавдкюяцрорпбдкьйомьщеаохдяючвейчвэухвх
эерючежюшзюахмрпйзхфйдыжецэзчящктмоодььепюйяйрющююцдиенат
щхщнеэмьхгьощцеюиьвдгивюыжшухехщкдэщжюяцлщлейдуюбпгьюйяй
гдидндидбосдьдиараощаагюывмтвдцзэяхщаайжгпюфпэшяияйхмлпияюц
махщмайвкмшуовывбочвгййобуиэывзджююцгйбасдйэвюэасуяхуцбущуфгтл
пэьвмхшосяхрпдюоцибофебаитвлплхлпэуеюююэлпбийэлпбинюфугьвоцвхе

стюцгдтэфйнезатщщавытдщаошумножячаеоеодзтлоййысьсюцсьмашайыь
хлеяюсбфеюоэщуйзлепрдуюкизолюоцубуйюгктнвэииюдэяхщагююцхенеде
фепэлпсайкииящбушзшзунтахаыхдрпдэщчижеьюхибунюзьдесьюцаетщф
еюайвкмжгеэзчхаздхенехднвящжесъвчаеяютвючсьцукммюфпэьххенеещж
пмюфгцвцвзщяшдыээжежуьэфгэзюайычщоднвкгшвиьвчлпэьяххэжмьхиьб
щйыфпжягьматщаефмлесгцадьтцэьакгдйпгцэьдемимозщчртщгдьцэьщщуз
мюнпамвикнсшувлонвиюовкмлебпчвмвзъжемвшзгдяиампнлоппбообхдвых
щнвшуялнюгъзабуохобхдзечадыегжешхдктеаюаирюунедмщуудвайыэанв
фупдэмчвмьщелеяймоюааачвэуопэьжеюэюааеыпхщаэаяхзснгыетепюхиэь
аелецюктпмзшршеьбюекгдъвтщдчиубждгдхьцкнвюиэвднвфузчщдетад
шимжйцумюэщчйощйаэнтцвдешюмюхебавахивлфеионвздоюубтесаыдхщ
нвшуцуюэрдцзщхмвлоцущщайюшдрддебочищцукмжйпиуцфйжпщцоеидф
гшйощемлмжгвдфвюаюообюаюймвшжеэуяххариндщэщгщчикгялнювам
жфуощпйццмюегнещегбдфюфпюйбпгьфпжяиэцвтбнещегбмлещцзаяьд
дьяецыфгсцфжтбшвяцвиоциалещщнвбчрьхаюиючпммьшгяошулобжфгфи
ыжпптбшвиьййраыьнщаоощаэшулопдищщцавяцбуиьэщхдвыбщпееыаебу
хтвдсдоцийыщцыэщзщцймилмлежщощрасгиацэиюшщыйзащеоюиьцвмтш
злебджювшщхщужиюбьяэшулопдхомццвяйощвьявжявщэаадощыщтщкщфй
ыьжеуцщуднвльэяхщабммоппмвппдюлмледшййдужижигежнввииятпнз
етечютдуюбпгьизднвепфйзщиакунэшщфпызайтьхиэианвзшуциорпбдню
цижефвчвйэгцлпнющещыаеямтщтазаощськммочиэилпбоодэаьдааощчвоощо
юшдийрднпщдщнюиадежпиэвиьхсшрдехщуйэтфппрюфпюцпмлпиящцоуг
ыцааюфпэаэвдтщфеоещпхэбоннощиафпжяфпцвчвжьфждэлолвяьчвдоэа
йыжевыоененезаиаразевыбвжйцулмлепешддерьхаюииэяхщагютврюфпэши
ацаыввюсюлоуюуцвшэщйыаегюфпгьднэизящсджпннхезефюфпящчвэвх
лмьдшоюьхиьрьрарежюгыщелекщтьээмюфзнэцвсдмаеюиэисьмюцвэиуб
эфгщдещечйшвюзкоусжээщтеяииюфггцкееюччацапесъзецюмозьхцоуоеу
юмодшййыхетеуиэижецэзчтэгчййыбозэгчййымааейшгюдпнойбпгьищцх
йэзьлевпцвсдчйыутвывяцбехдыиьхзавдсщяобамщсдэанелезатэфйфщиэщн
ежетщгдидчвряоеуюжйжпннтвшивлугцхлехщтапэсбеелеяоодгджюубвюцде
ючщупнлмлеяешайыиалимьящфгмючехйуышзкоусбщмазщбиьхзазьйысьз
ьюауйжекюжмтщкдцъщхйэашщааюцвмабзнэщегеюсюбжовщцапейщцв
юлозьйычвййзаятдпэшхлеяюсбеужищеегдъдэбоодфеаоененетщкервत्वэит
зщанезчудйожецэзчкмючсджэзлрдяюнюиюэзмюсетпыжтащенепхсшыщъвч
внюлоиэяцсбэапепещдйогдыйхедетамайвднвюдэяхщавомоодбпртгъоецупп
иачпковфндхщоедесшсдкюэьдэяцсдцааюцвэщфепэюцзасеяинэшзчуртэщсз
зеысдкюмвежцищемарцзлцвпепемайыщпзъуасыцвэиюэяхщавоцэлеююфпр
деыэвчвтаеуэетеьджюсббамщиаиьмахенщщавысьщцяцодчэтдбщпенегде
аиюуюэзлвиюэзлпмотвярьреэщдепвлпзщщаощсуяхсуяхлпвидшхщпелееецац

абацыешцщеггдюпшщмцкнвюутючшабщощщэщжлзьдшфглоиэюаэьубяш
бммышгжюуббуиьппбжхееэщуьхамьхфйсщощвьятжмючктюощщпвлхеше
кюиэзосднефепэчщушхдижппчиртлпчврянюбоодщэзопсеьяохтгднщхекудэ
эиэибацыешкибохтгдйаююэяхщаяэяхщавонвздайттьреошйынщмаонгою
зщатаьтаэзехдвьньнвэьдюртюцгсдееэюцгющччщупнлмжмящнюпхмыш
ияцдеууппамрпзьроадздыщчврялежпсбмгдешнвсбэаэщьэяхщаеаедежпиээщ
щьюцмюепаелешгкитвяцдееюдпэьдюиюложьвиибпейцамиьоецуппбозацы
жервщцжиртлпцацытдоехдсвщцюзмвусщекуяцфгкмрпцвсдчйбщцщлоцвкг
вюфттщнгкмжгпййождгдфгнхрйжщиаквбжхебуктюаююцдзщшгюйбпгьбпб
юфпбвмьщелеяйэщщднесдроюэппамбжронвжешатьэзребциюывэчврятаз
щрдюйкизоажхенежетщттххдэтахщщщсцвэиюэяхщалттвящущэбчиондамтщ
жпунлпэшшвчвйэрпуюиьрийешйыэшдеюйбаеашлльюусзочвцаделекюцияа
йгшацвэшвдсдтщеорпиьчврясдщелечпбопнххлпфмшуиэщщсдлоиэледешох
иболпжйсднегужиоаэвжронвпйцвгщнюаеегьюфпждвпщюиьаепзкнбатах
щьпсефггдяилмепэшшэвчвадздююубиьмюмтчеодеычмдэлпепэьйыямвиртюц
сшсднвлптвэиубшштиубзчшгыьгйцаоиэивюрдрячиртлпщешьмоодяюзьжгх
юйэяхщабмчвлеааатюцгсхеэщщднесдюфывепнюсьлоздшшианвщущлмюхеб
уэьрймщшатытьцьеуулмюзэгцлпнюшвчвиьрийешьбюбжщенюиьмахенщтьа
обчйэылщхрдшгматжщешгмаеюцжыгджювитщцразервяцсехдйноцзацыбдд
ебщпезмйэтвоцжестюцгдиавоцвмюцвэуллотвнюжнмющхлеуиььтаэзехд
ющдетазадужиубхошунхрдощнвшардздхылофмгдмащавыщюэздщощоеядз
хвдюэзмочпцвлпиьгоощнвпйсьшузохефпызайтьрехджоодэввифйядшаждгд
фггщнерйюглофцвттщхдвыпелебдеыаеьйнщыщхдгдбмгдхдбщььзецюьхнэс
фибнвиювичврянвзшрйвдзджюлмгчхтзбчишщюаюьтайгшаощюоэшййшоэ
шешьяйгдтидщвоюзйэхесдегжщюаыьзекжгыщенюэьщцфцжшттььжеуцюаю
ьтаэахщчвэвхээщхдупндидвоюзйэсдвчщупнлмтщжпешудежпунтвовднв
юяхмощуепнюдешечйшвчвьхзанэудеьщйжпннтвшиэихешщешьаежецэзчкмо
пияжмрплобчжоцвмозохтйквэипхнэмвижппщцюзэдэтвэипхнэмвзочвжпнн
мвцвщцэардздхытцбойэлмдэяццыцвэшявхжпидидьмаеылочводэжгыюйбауэ
яхщавочвнюжйядтпктаевшэфмюлобылмьмоодпзощпищуээяцыщцщиовюьх
юааьтаэзехдзющцдевдюпиьоецумвбииюмюдэпааюфпбуиьэзээяхщагючвяц
сехдзюэизезэщощвыамьхфйсщощфйзщшнюучаущюимьюжфучугьоддпэьов
лмяхусидгщкухтхеажщедешиюаугшазевытпктепиьсхчвмоюзопщувюывьяч
щдецуыьбщщхйэунищцжфтзелмьщещебджюсбюанвшубюфгеэяхщаыйцачю
эирпмюамлпияцднеунощбпвзвимождгдйидвмюьщегфгыюфпсесакумюфгоа
жгщьвияцжпмохенюятздэаьпзьхегехщыййядужибочвэухвэсюаяйбацыешц
щэабвюатайывдсуыжывдюиэмошушйиадечюмюзэциуцнщхекудэяцепзьхес
тюцсшэщаеиовифйлхнэлвижппикщещежсьмюкмщджгмяппсбхщжвччнюшия
цюужгщдешечмзьмюййнежетщщехдйанюэьюэлвиаэабнппяцнвжегдпмзоб

днердздшамйдвеавэнщещамхвусеььрьчайыгдчиэжпунудщехехдьжывм
иькдбовшвыэьаееадебпээкоудкюдэяхщаеапехдизопбжщещечирттвдюлмleo
елжлпчвййщцгдидйительиюдохжящцаюйбатыцгдкьвдюжвюубщпзьсюцвб
жщфебалимьтесьюцсуяхубвдыюенвздажщеошшщещежэудеьоезелаллж
мадбщяиэиюайгкукоудеьэяхщабмшузьмасллотвыщдецуьхлпйтаияцгпээбо
цвешяйсдкюцвюзаихевджюсбеавэншшвяцзщцюфпбуйэрпхаьллотвюшдеэщ
бачмжмвддылкмбжбщжпечеписьаэгцуджэяхщагюфтианжщевнюэехеяцы
ойидкмхшоекуяцдэхеажщещещихьнийююфпьхрдяднючвкмшууеошйыунзеб
вчвййнвсдчхрдщезаяюубсдкюцвцэзьовывхшфьэяхщащбмйэбщкижмюф
пмлпвоубкщжещехеэфлошусдебюдэчврпшинююцхеиилмйэзлзайыяецыхе
сдийрддшлльюуссдэахдоехеаеяюкмтщрдкюхтыжюцядэащдба

Повідомлення:

утробылотихоегородакутанныйтмоймирнонежилсявпостелипришлолетои
ветербыллетнийтеплоедыханиемиранеспешноеиленивоестоитлишьвстатьв
ысунутьсявокошкоитотчаспоймешьвотонаначинаетсянастоящаясвободаиж
изньвотонпервоеутролетадуглассполдингдвенадцатилетотродутолькочтоо
ткрылглазаикаквтеплуюречкупогрузилсывпредрассветнуюобезмятежностью
нлежалвсводчатойкомнаткеначетвертомэтажевовсемгороденебылобашни
ышеиоттогочтоонпарилтаквысоковвоздухевместесиюньскимветромвнемро
ждаласьчудодейственнаясилапоночамкогдавзядыдубыикленысливалисьводн
обеспокойноеморедугласокидывалеговзглядомпронзавшимтьмуточномаяк
исегоднйавотздоровошепнулонвпередичелоелетонесчетноемножестводнейч
утьнеполкалендаряонужевиделсебямногорукикакбожествоишваизкнижки
пропутешествиятолькопоспевайрватьещезеленыеяблокиперсикичерныекак
ночьсливыегоневытащитьизлесаизкустовизречкиакакприятнобудетпомерз
нутьзабравшисьвзаиндевелыйледниккаквеселожаритьсявбабушкинойкухне
заодностысячьюцпятапоказаделоразвнеделюемупозволялиночеватьневд
омикепососедствугдеспалиегородителиимладшийбратишкатомаздесьвдедо
вскойбашнеонвзбегалпотемнойвинтовойлестниценасамыйверхиложилсся
атьвэтойобителикудесникасредигромовивиденийаспозаранкукогдадажемо
лочкикешценезвякалбутылкаминаулицахонпросьпалсяипреступалкзаветном
уволшебствустоявтемнотеуоткрытогоокнаоннабралполнуюгрудьвоздухаии
зовсехсилдунулучныефонаримигомпогаслиточносвечкиначерномименин
номпирогедугласдунулещеиещевнебеначалигаснутьзвездьдугласулыбнул
сяткнулпальцемтамитамтеперьтутивоттутвпредутреннемтуманеодинзадруг
импрорезалисьпрямоугольникивдомахзажигалисьогнидалекодалеконарассв
етнойземлевдругозариласьцелаявереницаоконвсемзевнутьвсемвставатьогр
омныйдомвнизуожилдедушкавынимайзубыизстаканадугласнемногопожд

албабушкаипрабабушкажарьтеоладысквознякпронесовсемкоридорамтеп
лыйдухжареноготестаивовсехкомнатахвстрепенулисьмногочисленные
идядядвоюродныебратьяисестрычтосехалисьсюдапогоститьулицастарико
впросыпайсямиссэленлумисполковникфрилеймиссисбентлипокашляйтевст
аньтепроглотитесвоитаблеткипошевеливайтесьмистерджонасзапрягайте
лошадьвыводитеизсараяфургонпораехатьзастарьемпотусторонуоврагаоткрыл
исвоидраконьиглазаугрюмыеособнякискоровнизупоявятсянаэлектрической
зеленоймашинедвестарухиипокатятпоутреннимулицамприветственнамаха
каждойвстречнойсобакемистертридденбегитевтрамвайноедепоивскорепоуз
кимрусламмоценыхулицпоплыветтрамвайрассыпаявокругжаркиесиниеиск
рыджонхафчарливудменвыготышепнулдугласулицедетейготовыспросило
нубейсбольныхмячейчтомоклинаросистыхлужайкахупустыхверевочныхка
челейчтоскучаясвисалисдеревьевмаппатомпроснитесьтихонькопрозвенел
ибудильникигулкопробиличасыназданииисудачносетьзаброшеннаягорук
ойсдеревьеввзметнулисьптицыизапелидирижируясвоиморкестромдугласпо
вельительнопротянулрукуквостокуйвзошлосолнцедугласскрестилрукинагру
диулыбнулсякакнастоящийволшебниквоттотодумалонтолькояприказаливс
еповскакаливсезабегалиотличноебудетлетоиионнапоследокогляделгородище
лкнулемупальцамираспахнулисьдверидомовлюдивышлинаулицулетотысяч
адевятьсотдвадцатьвосемьмогоданачалосьвтроутропроходяполужайкедуглас
наткнулсянапаутинуневидимаянитькоснуласьеголбаинеслышнолопнулаиот
этогопустячногослучаяоннасторожилсяденьбудетнетакойкаквсенетакойеще
ипотомучтобываютдниотканьеизоднихзапаховсловновесьмирможновтян
утьносомкаквоздухвдохнутьивыдохнутьтакобяснялдугласуиегодесятилетне
мубратутомуотецкогдавезихвмашинезагородавдругиедниговорилещеотецм
ожноуслышатькаждыйгромикаждыйшорохвселеннойиныедниххорошопроб
оватьнавкусайныенаощупьабываюттакиекогдаестьвсесразуотнапримерсе
годняпахнеттакбудтоводнуюночьтамзахолмаминевестьоткудавзялсяогромны
йфруктовыйсадивседосамогогоризонтатакиблагоухаетввоздухепашнетдожд
емнонанебениоблачкатогоиглядиктотоневедомыйзахохочетвлесунопокатам
тишинадугласвовсеглазасмотрелнаплывущиемимополянетнисадомапахне
тнидождемдаиоткудабыразниаблоньнетнитучиктотамможетхотатьвлесуа
всетакидугласвздрогнулденьэтоткакойтоособенныймашинаостановиласьвс
аомсердцетихоголесаануребятанебаловатьсяониподталкивалидругдругал
октямихорошопамальчикивылезлиизмашинызахватилисиниежестяныеве
драисойдяспустыннойпроселочнойдорогипогрузилисьвзапахиземливлажн
ойотнедавнегодождяищитепчелсказалотецони всегдавьютсявозлевинограда
какмальчишкивлезлекухнидугасдугласвстрепенулсяопятьвитаешьвоблакахс
казалотецпустисьназемлюпойдемснамиорошопапаионигуськомпобрелипо

лесу впереди тец рослый и плечистый, а за ним дугласа, последним семенил коротышка, тот поднялся на невысокий холм и посмотрел в даль, вон там указал пальцем, отец там обитают огромные полетные мухи и ветры и незримые плывут в зеленых глубинах точно призрачные киты, дуглас глянул в ту сторону, ничего не увидел, и почувствовал себя обманутым, отец как дедушка вечно говорит загадками и и в сетаки дуглас затаил дыхание и прислушался, что то должно случиться, подумал, а ну ж знаю, а вот папоротник называется венерин волос, отец неторопливо шагнул вперед, синее ведро позвякивало у него в руке, а это чувствуете и он ковырнул землю, оноском башмаками, миллионы лет копился этот перегной, осень за осень, юпадали листья, пока земля не стала такой мягкой, ух ты, а ступая, как индеец, сказал, том совсем не слышно, дуглас потрогал землю, он ничего не ощутил, он все время настороженно прислушивался, мы окружены, думал, он что то случится, а что он установил, а выходи же, где ты там, что ты такое, мысленно кричал, он томи, отец шли дальше, по тихой податливой земле, на свет не так кружеват, он шенегром, коска, сказал, отец, пока зал рукой в верх, где листва, деревья ввплеталась в небо, или может быть, небо в плетало, сь в листву, в сера, ну, улыбнулся, отец все это кружева, зеленые иголки, в в с м о т р и т ь с ь х о р о ш е н ь к о и у в и д и т е л ь с п л е т е т и х с л о в н о г у д я щ и й с т а н о к о т ь с т о я л у в е р н о п о х о з ь i с k и и р а с с к а з ы в а л и м в с ь я к у ю в с ь я ч и н у л ь г о i с в о б о д н о н е в ы б и р а я с л o v ч a c t o o n i c a m c m e я л ь c ь c в o i m p o c c a з a m и o t 3 t o г o o n и t e k л и e щ e c в o б o d н e e x o p o ш o п p и c л y ч a e п o c л y ш a т ь t и ш и н y г o в o p и л o n п o t o м y ч t o t o г д a д a e т ь c ь y c л ы ш a т ь k a k н o c и т ь c ь в в o з д y x e п ы л ь ц a п o л e в ы x ц в e t o в a в o з d y x t a k и г y д и т п ч e л a m и d a d a t a k и г y d и т a в o t c л ы ш и т e t a m з a д e p e в ь я m и в o d o п a d o m л ь e т ь c ь п т и ч ь e щ e б e т a н ь e в o t c e i ч a c д y м a л d y г л a c в o t o н o y ж e б л и з k o a я e щ e н e в и ж y c o в c e m б л и з k o p я d o m д и k и й в и н o г p a d c a з a л o t e ц n a m п o в e з л o c m o t p и t e k a n e n a d o a x н y л п p o c e б ь a d y г л a c n o t o m и o t e c n a k л o n и л и c ь i п o г p y з и л и p y k и в ш y p ш a щ и й k y c t ч a p ы p a c c e я л и c ь t o п y г a ю щ e e i г p o з н o e ч t o п o d k p a d ы в a л o c ь б л и з и л o c ь г o t o в o б ы л o r и н y т ь c ь i п o t p ь a c t и e г o d y ш y и c ч e з л o o п y c t o ш e n н ы й p a c t e p ь a n н ы й d y г л a c y п a л n a k o л e n и п a л ь c ы e g o y ш л и г л y б o k o в з e л e н y ю t e n ь b ы n y p н y л и o б a g p e n n ы e a л ы m c o k o m c л o v н o o n v з p e z a л л e c н o ж o m и c y н y л p y k и в o t k p ы т y o p a n y m a л ь ч и k и z a в t p a k a т ь в e d p a ч y т ь n e d o в e p x y n a п o л n e n ы d и k и m в и н o г p a d o m и л e c н o й з e m л ь n и k o й v o k p y г г y d ь t п ч e л ы 3 t o v o в c e n e п ч e л ы a c e л ы й m и p t и x o н ь k o m y p л ы ч e t c в o ю п e c e n k y g o v o p и t o t e c a o n и c i d ь t n a z a m ш e л o m c t o л e y п a в ш e г o d e p e в a ж y o t c a n d в и ч и i п ы т a ю т ь c ь c л y ш a т ь л e c k a c л y ш a e t o n o t e c t y т ь п o c м e и в a я c ь i c k o c a п o г л ь a д ы в a e t n a d y г л a c a x o t e л b ы л o ч t o t o c a з a т ь n o п p o m o л ч a л o t k y c и л e щ e k y c o k c a n d в и ч a i z a d y м a л c ь x л e б c в e t ч и н o й v л e c y n e t o ч t o d o m a v k y c c o в c e m d p y г o й в e p н o o c t p e e ч t o л и m ь a t o y t d a e t c m o л o y a y ж a п e t и t k a k p a з ы г p ы в a e т ь c ь a d y г л a c п e p e c t a л ж e в a т ь i п o t p o г a л ь z ы k o m x л e б и v e t ч и n y n e t n e t o b ы k н o в e n н ы й c a n d в и ч t o m k и v н y л п p o d o л ж a я ж e в a т ь y п o n и m a ю п a п e d ь y ж e п o ч t и c л y ч и л o c ь d y м a e t d y г л a c n e з н a ю ч t o 3 t o н o o n o б o л ь ш y щ e e n p ь a m o g p o m a d n o e ч t o t o e g o c п y г н y л o g d e ж e o n o t e п e p ь o п ь a т ь y ш л o v t o t k y

стнетгдетозамнойнетнетздесьутрядомдугласисподтишкапощупалсвойжив
отоноещевернетсянадотольконемножкоподобждатьбольнонебудетяужзнаюи
езатемонокомнепридетнозачемжезачема

Значення ключа (441, 310)

Висновок:

У лабораторній роботі реалізовано підпрограми для обчислення оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язання лінійних конгруенцій, які далі були використані для знаходження кандидатів на ключ (a,b) шифру афінної біграмної підстановки, і, власне, програма для розшифрування тексту.