Міністерство освіти і науки України
Національний Технічний Університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №3

з дисципліни «Криптографія»

на тему: «Вивчення криптосистеми RSA та алгоритму електронного підпису; ознайомлення з методами генерації параметрів для асиметричних криптосистем»

Виконали:
Студенти групи ФБ-82
Кисіль Денис
Глотов Володимир
Перевірив:
Чорний О.

Київ - 2020

Мета роботи:

Завдання:

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Порядок виконання роботи:

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

- 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 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 Перед початком виконання роботи ми уважно ознайомились з теоретичними відомостями та методичними вказівками до виконання лабораторної роботи;
  Обговорили план виконання лабораторної роботи та визначили варіант згідно вказівок(Варіант 6).

- 2 Реалізували підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв’язуванням лінійних порівнянь. (Також врахували варіант за якого лінійне порівняння має декілька розв’язків.)

- 3 Визначили 5 найчастіших біграм шифротексту варіанту 6 (табл. 1); Та знайшли кандидатів на ключ.

- 4 Для кожного знайденого кандидата на ключ дешифрували текст та зробили перевірку(чи є змістовним текстом російською мовою). Перевірку здійснили шляхом розрахунку індексу відповідності, для кожного з отриманих після дешифрування текстів (індекс відповідності мав бути більшим за 0.054). Для підтвердження коректності обраного методу в табл. 2 наведені деякі значення ключів і індекси відповідності для текстів, що були розшифровані з цими ключами.

Ключ (441 310)

Индекс 0.054227534807633565

Найчастіші біграми ШТ

['ще', 'де', 'хе', 'ле', 'чв']

ШТ

ывлеюгзебщпещхщуйэвиывиюфгувхцубхщыюнюжлепэшфмиьхдощбуднзегдщебоцвшуюгьпц
вэщувкмзеиэбчиюндхщюасдбмонхегщгдэщжезьщемвощфысьмайыегыйяййыэшжеаек

идщщеюжгьдеьцонгочвнюиюыжвюудеьбюгьщесфвшвоюзйэящкщьюгочвнюлмшужее
йцурпцвдэяхщаюьдеуэвющэвдиайятвепцвчвлеюйщецыаешвэеяикгехщаэациэибвкмрй
жуажййдекущтепэшфмздсугьвоцвяйкзфтшшхдуюиьйынюгдхацовойэращеюияциаяим
юыжцввджвяцэввлломоодмхщуйэмюэзопюзкнэщегбдсефвьхбжщенюцатщввэиегтеаех
охтюйлдицзьхдщщщюяьзщюоцвлеюосдлузлзащавызйферддьйомюиаыьепжмнюбжщц
аещэзойтзэвзвщупмюжьощшаощвыжееююззьдеаейюшдоездюйбпгьвиюэколпщхмоих
сшфеэмлеотзомщйвхцывбжхебахиэьщхйэашжеттфележебдфюфпнюфмшуиэжяппшд
гдщесдцжцвхеюцхеяднвжееютбзййысддемилпмюзахшнюллююэпподйшяюьхщужиуц
табззлзьйопнбоящпиэщииамленйхдбднвнщлврпшилмиьадшахушайыэффтппмюцдсззе
зщадцьцихжшуфгбиэихеныжпбоцднесдегмаущйыктгдыйктййнвмоктздгидатаомтщлвх
еийрдимяцшуьюывмтшзюашнэьгоэавюрдвджгмпиээщеиэивдодзехатщйыэшззшзунзщ
хеюизчсдэайэхенвжьфжпсхгчплвжмвиртдэппщуртцюиэппедчйдещорпдпвюбжлотвдю
лофехщыддетеодаьйояхрдбмлпнднелеыщхдощуцщазнибыутвднтащебацэзьгордфесьае
щзкнсднюятьдаахмчвюцхеиовющежемпзькюжямюгьщцсбвдсчепзлепэшбмтвгоэвубюз
мвппцинэзьэщтапуиэпхлеоенщнщрдэщлабмхтфуиюййаещэдэвлюцрпбжэщыдидсдщох
илпийшгмищцвюбйощйапедмлесгцатьчщбуэьгйцамиэавдкюяцрорпбдкьйомьщеаохдяю
чвейчвэухвьхэерючежюшзюахмрпяйзхфйдыжецэзчящктмоодььепюйяйрйощоюцдиеи
атщхщнеэмьхгьощщеоюиьвдгивюыжшухехщкдэщжюяцлщлейдюйбпгьюйяйгдидндидб
осдьдиараощаагюывмтвдцэзэяхщаыйжгпюфпэшяияйхмлпияюцмахщмайвкмшуовывбо
чвгййобуиэывзджююцгйбасдйэвюэасуяхуцбущуфтлпэьвмхшоеяхрпдюцибофебаитвлп
хлпэьуеююююэлпбийэлпбинюфугьвоцвхестюцгдтэфйнеэатщщавытдщааошумюжячеае
еоодзтлояййысьюцсьмашайыьхлеяюсбфеюооэщуйзлепрдюйкизолюуцобуйюгктнвэиию
дэяхщагююцхенедефепэлпсаийкиящбушзшзунтахаьыхдрпдэьщчижеьюхибунюзьдесь
юцаетщфеюайвкмжгеэзчхаздхенехдневящжесьвчаеяютвючсьцукммюфпэьхцхенеещжп
мюфгцвцвзщяшдыээжежуйэфгэзюайычщоднвкгшвиьвчлпэьяьхэжмьхиьбщйыфпжягъ
матщаефмлесгцадьтцэьакгдйпгцэьдемимоэщчртщгдьцэьщщузмюнпамвикнсшувлонви
юовкмлебпчвмвзьжемвшзгдяиампнлоппбообхдвыхщнвшуялнюгъэабуохобхдзечадыег
жеыщхдктеаюаирюунедмщуудвайыэанвфупдэмчвмыщелеяймоюааачвэуопэьжеюэюаа
ееыпхщаэаяхзснгыетепюхиэьаелецюктпмзшршеьбюекгдьвтщщдчиубждгдхеьцкнвюиэ
вднвфузчшшдетадшимжйцумюэщчйощйаэмтщвдеьйомюхебавахивлфеионвздоюубтес
аыдхщнвшуцуюэрдцзщхмвлоцущшайюшдрддебочищукмжйпиуцфйжпщцоеидфгшйо
щемлмжгвдфвюаюообюаюьймвшжеэуяххариндщщэщгщчикгялнювамжфуощпйцмю
егнещеегбдфюфпюйбпгьфпжяиэцвтбнещеегбмлещщзеяйьддьяецыфгсцфжтбшвяцвио
щиалещщнвбчрйхаюиючпммышгяошулобжфгфиыжпптбшвиьййраыьнщеаощяэшулоп
дицщццаявяцбуиьэщхдвыбщпееыаебухтвдсдощийыщцыэщзщцймилмлежщощрасгиацэ
июшщыйзащеоюиьцвмтшзлебджювшщхщужиубяэшулопдхомццвяйощвыявжявщэаад
ощыщтщкщфйыьжеуцщуыднвлеьэяхщабммоппмвппдюлмледшяйдужижиженввиищят
пнзетечютдюйбпгьчизднвепфйзщиакунэшщфпызяйтьхиэиианвзшущиорпбдпюцижеф
вчвйэгцлпнющецыаеямтщтаэаощськммочиэилпбоодэаьдааощчвощоюшдийрднпцвдщн
юиадежпиэвиьхсшрдехщуйэтфппрюфпюцпмлпиящцоугьцааюфпэьаэвдтщфеоещпхэб
онноцщиафпжяфпцвчвжьфждэлолвяьчвдодэйайыжевыоененезаиаразевыбвжйцулмлеп
еяшдерйхаюииэяхщагютврюфпэшиацаыввюсюлоюэуцвшэщйыаегюфпгьпднеизящсдж
пннхезефюфпящчвэвьхлммьдшоюьхиьрйрарежюгьщелекщтьээмюфзнэцвсдмааеюиэи
сьмюцвэиубэфгшдещечйшвюзкоусжээщтеяииюфггшкееюччэацапесьзецюмозьхцоуое
уюмодшяййыхетеуиэижецэзчтэгчяййыбозэгчяййымааейшгюдпюйбпгьиищцхйэзьлвепц
всдчйыутвывяцбехдыиьхзавдсщяобамщсдэанелезатэфйфщиээщнежетщгдидчвряоеую
жйжпнтвшивлугцхлехщтапэсбеелеяоодгджюубвюцдеюччщупнлмлеяешайыиалимья
щфгмючехйуышзкоусбщмазщбиьхзазьйысьзьюауйжекюжмтщкдцьщхйэашцаающвма
бзнэщежееюсюбжовщцэапейцщцвюлозьйычвййзаятдпэшьхлеяюсбеужищеегдьдэбоод
фееаоененетщкервтвэитзщанезчудйожецэзчкмючсджэзлрдяюнюиюэзмюсетпыжтаще
непхсшыщьвчвнюлоиэяцсбэапепещдйогдыйхедетамайвднвюдэяхщавомоодбпртгьоецу
ппиачпковфндхщоедесшсдкюэьдэяцсдцааюцвэщфепэюцзасеяинэшзчуртэщсззееысдк
юмвежцищемарцзлцвпепемайыщпзьуасьцвэиюэяхщавоцэлеююфпрдеыэвчвтааеувэете
ьджюсббамщиаиьмахенщщавысьщцяцодчэтдбщпенегдеаиююуэзлвиюэзлпмотвяьреэщ
депвлпзщшаощсуяхсуяхлпвидшхщпелееецацабацыещзщеггдюпшщмцкнвюутючшабщ
ощщщэщжлзьдшфглоиэюаэьубяшбммьшгжюуббуиьппбжхееэщуьхамьхфйсщощвыят
жмючктюцощщпвлхешекюиэзосднефепэчщущхдижппчиртлпчврянюбоодщэзопсеьаох
тгднщхекудээиэибацыещкибохтгдййаююэяхщаяэяхщавонвздадяйтьреошйынщмаонго
юзщатаььтаэазехдвьнйнвэьдюртюцгсдееэюцгющцччщупнлмжмящнюпхмьшияцдеыуп
памрпзьроадздыщчврялежпсбамгдещнвсбэаэщьэяхщаеадежпиээщцьюцмюепаелешгк
итвяцдееюдпэьдюиюложьвиибпейцамиьоецуппбозацыжервщцжиртлпцацытдоехдсвщц
юзмвусщекуяцфгкмрпцвсдчйбщцщлоцвкгвюфттщнгкмжгпййождгдфгнхрйжщиаквбж
хебуктюаоюцдзщшгюйбпгьбпбюфпбвмьщелеяйэщщднесдроюэппамбжронвжешатьэзр
ебциюывэцчврятазшрдюйкизоажхенежетщттххдэтахщшщсьцвэиюэяхщалттвящуэбчи
юндамтщжпунлпэшшвчвйэрпуюиьрйещйыэшдеюйбазеашллыюусзочвцаделекюцииайг
шацвэшвдсдтщеорпиьчврясдщелечпбопнххлпфмшуиэщщсдлоиэледещохиболпжйсдне
гужиоаэвбжронвпйцвгщнюаеегыюфпждвпщюиьаепзкнбатахщьпсефггдяилмепэшэвчв
адздююубиьмюмтчеодеычмдэлпепэьйыямвиртюцсшсднвлптвэиубшштиубзчшгыьгйца

оиэивюрдрячиртлпщещьмоодяюзьжгхюйэяхщабмчвлеааатюцгсхеэщцднесдюфывепн
юсьлоздшшианвщузлмюхебуэьрймщшатьтцьеэуллмюзэгцлпнюшвчвиьрйещеьбюбжщ
енюиьмахенщтьаобчйэылщхрдшгматжщешгмааеюцжьгджювитщразервяцсехдйнощза
цыбддебщпезмйэтвощжестюцгдиавоцвмюцвэуллотвнюжнмющхлеуииьтаэазехдющде
таэадужиубхошунхрдощнвшардздхылофмгдмащавыцюэздщощоеядьзхвдюэзмочпцвлп
иьгоощнвпйсьшузохефпызяйтьрехджоодэввифйядшаждгдфггщнерйюглофцчвтщхдвы
пелебдеыаеьйнщыщхдгдбмгдхдбщььзецюьхнэсфибнвиювичврянвзшрйвдзджюлмгчхтз
бчишщюаюьтайгшаощюоэшййшоэшещяйгдтидщвоюзйэхесдегжщюаыьзекжгыщенюэь
щцфцжштьыьжеуцюаюьтаэахщчвэвьхэеэщхдупндидвоюзйэсдвчщупнлмтщжпежудде
жпунтвовднвюяхмощуепнюдещечйшвчвьхзанэудеьщйжпннтвшиэихещщеьаожецэзчк
мопияжмрплобчжоцвмозохтюйквэипхнэмвижппщцюэдэтвэипхнэмвзочвжпннмвцвщцэ
ардздхытцбойэлмдэяццыцвэшявхжпдидьдмаеылочводэжгьюйбауэяхщавочвнюжйядтп
ктаевшэфмюлоылмьмоодпзощпищуээяцыщзщиовюьхюааьтаэазехдзющцдевдюпиьоец
умвбииюмюдэпааюфпбуиьээээяхщагючвяцсехдзюэизеэщощвыамьхфйсщощфйзщшн
юучаущюимьюжфучугьоддпэьовлмяхусидгщкухтхеажщедещиюаугшазевытпктепиьс
хчвмоюзопщувюывяьчщдецуыьбщщхйэунищцжфтзелммьщебджюсбюанвшубюфгеэя
хщаыйцачюэирпмюамлпияцдneунощбпвзвимождгдяйдвмюьщегфгыюфпсесакумюфго
ажгщьвияцжпмохенюятздэаьпзьхегехщыйяйдужибочвэухвэсюаяйбацыещзщэабвюата
йывдсуыжывдюиэмошушйиадечюмюзэциуцнщхекудэяцепзьхестюцсшэщаеиовифйлхн
элвижппикщежесьмюкмщджгмяппсбхщжвччнюшияцюужгщдеьжечмзьмюййнежетщ
щехдйанюэьюэлвиаэабнппяцнвжегдпмзобднердздшамйдвеавэнщещамхвусеьыьрйчайы
гдчиэижпунудщехехдьжыввмиькдбовшвыэьаееадебпээкоудкюдэяхщаеапехдизопбжще
щечирттвдюлмлеоелжлпчвййщщгдидййтельиюдохжящэаюйбатьцчгдкьвдюжвюубщпз
ьсюцвбжщефебалимьтесьюцсуяхубвдыюэенвздажщеощшшщешежэудеьоезелаллжма
дбщяиэиюайгкукоудеьээяхщабмшузьмасллотвьщдецуьхлпйтаияцгпэзбоцвещяйсдкюц
вюзаихевджюсбеавэнщшвяцзщцюфпбуйэрпхаьллотвюшдеэщбачмжмвддыллкмбжбщ
жпежепиьаэгцуджэяхщагюфтианжщеэвнюэехеяецыойидкмхшоекуяцдэхеажщещщхи
ьнйююфпьхрдяднючвкмшууеошйыунзебвчвййнвсдчхрдщеэаяюубсдкюцвцэзьовывхш
феьэяхщащцбмйэбщкижмюфпмлпвоубкщжещехеэфлошусдеьбюдэчврпшинююцхеии
лмйэзлзайыяецыхесдийрддшлльюуссдэахдоехеаеяюкмтщрдкюхтыжюцядэащдба

ВТ

утробылотихоегородокутанныйтьмоймирнонежилсявпостелипришлолетоиветербыллетнийте
плоедыханиемиранеспешноеиленивоестоитлишьвстатьвысунутьсявокошкоитотчаспо
ймешьвотонаначинаетсянастоящаясвободаижизньвотонопервоеутролетадуглассполди
нгдвенадцатилетотродутолькочтооткрылглазаикаквтеплуюречкупогрузилсявпредрасс
ветнуюбезмятежностьонлежалвсводчатойкомнаткеначетвертомэтажевовсемгородене
былобашнивышеиоттогочтоонпарилтаквысоковвоздухевместесиюньскимветромвнем
рождаласьчудодейственнаясилапоночамкогдавязыдубыикленысливалисьводнобеспоко
йноеморедугласокидывалеговзглядомпронзавшимтьмуточномаякисегоднявотздорово
шепнулонвпередицелоелетонесчетноемножестводнейчутьнеполкалендаряонужевидел
себямногорукимкакбожествошиваизкнижкипропутешествиятолькопоспевайрватьеще
зеленыеяблокиперсикичерныекакночьсливыегоневытащитьизлесуизкустовизречкиак
акприятнобудетпомерзнутьзабравшисьвзаиндевелыйледниккакveселожаритьсявбабуш
кинойкухнезаодностысячьюцыплятапоказаделоразвнеделюемупозволялиночеватьневд
омикепососедствугдеспалиегородителиимладшийбратишкатомаздесьвдедовскойбашне
онвзбегалпотемнойвинтовойлестниценасамыйверхиложилсяспатьвэтойобителикудесн
икасредигромовивиденийаспозаранкукогдадажемолочникещенезвякалбутылкаминаул
ицахонпросыпалсяиприступалкзаветномуволшебствустоявтемнотеуоткрытогоокнаон
набралполнуюгрудьвоздухаиизовсехсилдунулуличныефонаримигомпогаслиточносвеч
киначерномининномпирогедугласдунулещеиещеивнебеначалигаснутьзвездыдугласу
лыбнулсяткнулпальцемтамитамтеперьтутивоттутвпредутреннемтуманеодинзадругим
прорезалисьпрямоугольникивдомахзажигалисьогнидалекодалеконарассветнойземлевд
ругозариласьцелаявереницаоконвсемзевнутьвсемвставатьогромныйдомвнизуожилдед
ушкавынимайзубыизстаканадугласнемногоподождалбабушкаипрабабушкажарьтеолад
ьисквознякпронесповсемкоридорамтеплыйдухжареноготестаивовсехкомнатахвстрепе
нулисьмногочисленныететкидядьядвоюродныебратьяисестрычтосехалисьсюдапогост
итьулицастариковпросыпайсямиссэленлумисполковникфрилеймиссисбентлипокашля
йтевстаньтепроглотитесвоитаблеткипошевеливайтесьмистерджонасзапрягайтелошад
ьвыводитеизсараяфургонпораехатьзастарьемпотусторонуоврагаоткрылисвоидраконь
иглазаугрюмыеособнякискоровнизупоявятсянаэлектрическойзеленоймашинедвестару
хиипокатятпоутреннимулицамприветственномахаякаждойвстречнойсобакемистертри
дденбегитевтрамвайноедепоивскорепоузкимрусламмощеныхулицпоплыветтрамвайрас
сыпаявокругжаркиесиниеискрыджонхафчарливудменвыготовышепнулдугласулицеде
тейготовыспросилонубейсбольныхмячейчтомоклинаросистыхлужайкахупустыхверев
очныхкачелейчтоскучаясвисалисдеревьевмампаптомпроснитесьтихонькопрозвенелиб
удильникигулкопробиличасыназданиисудаточносетьзаброшеннаяегорукойсдеревьеввз

метнулисьптицыизапелидирижируясвоиморкестромдугласповелительнопротянулруку
квостокуивзошлосолнцедугласскрестилрукинагрудииулыбнулсякакнастоящийволшеб
никвоттотодумалонтолькояприказаливсеповскакаливсезабегалиотличноебудетлетоио
ннапоследокогляделгородищелкнулемупальцамираспахнулисьдверидомовлюдивышли
наулицулетотысячадевятьсотдвадцатьвосьмогогоданачалосьвтоутропроходяполужайк
едугласнаткнулсянапаутинуневидимаянитькоснуласьеголбаинеслышнолопнулаиотэто
гопустячногослучаяоннасторожилсяденьбудетнетакойкаквсенетакойещеипотомучтоб
ываютднисотканныеизоднихзапаховсловновесьмирможновтянутьносомкаквоздухвдох
нутьивыдохнутьтакобяснялдугласуиегодесятилетнемубратутомуотецкогдавезихвмаш
инезагородавдругиедниговорилещеотецможноуслышатькаждыйгромикаждыйшорохв
селеннойиныеднихорошопробоватьнавкусаиныенаощупьабываютитакиекогдаестьвсес
разувотнапримерсегодняпахнеттакбудтоводнуночьтамзахолмаминевестьоткудавзялся
огромныйфруктовыйсадивседосамогогоризонтатакиблагоухаетввоздухепахнетдождем
нонанебениоблачкатогоиглядиктотоневедомыйзахохочетвлесунопокатамтишинадугла
свовсеглазасмотрелнаплывущиемимополянетнисадомнепахнетнидождемдаиоткудабы
разнияблоньнетнитучиктотамможетхохотатьвлесуавсетакидугласвздрогнулденьэтотк
акойтоособенныймашинаостановиласьвсамомсердцетихоголесаануребятанебаловатьс
яониподталкивалидругдругалоктямихорошопапамальчикивылезлиизмашинызахватил
исиниежестяныеведраисойдяспустынноипроселочнойдорогипогрузилисьвзапахиземли
влажнойотнедавнегодождяищитепчелсказалотецонивсегдавьютсявозлевиноградакакм
альчишкивозлекухнидугласдугласвстрепенулсяопятьвитаешьвоблакахсказалотецспус
тисьназемлюпойдемснамихорошопапаионигуськомпобрелиполесувпередиотецрослый
иплечистыйзанимдугласапоследнимсеменилкоротышкатомподнялисьнаневысокийхол
мипосмотреливдальвонтамуказалпальцемотецтамобитаютогромныеполетнемутихиеве
трыинезримыеплывутвзеленыхглубинахточнопризрачныекитыдугласглянулвтусторон
уничегонеувиделипочувствовалсебяобманутымотецкакидедушкавечноговоритзагадка
миивсетакидугласзатаилдыханиеиприслушалсячтотодолжнослучитьсяподумалоняуж
знаюавотпапоротникназываетсявенеринволосотецнеторопливошагалвпередсинееведр
опозвякивалоунеговрукеаэточувствуетеионковырнулземлюноскомбашмакамиллионы
леткопилсяэтотперегнойосеньзаосеньюпадалилистьяпоказемлянесталатакоймягкойух
тыяступаюкакиндеецсказалтомсовсемнеслышнодугласпотрогалземлюноничегонеощу
тилонвсевремянастороженноприслушивалсямыокруженыдумалончтотослучитсяночт
ооностановилсявыходижегдетытамчтотытакоемысленнокричалонтомиотецшлидальш
епотихойподатливойземленасветенеткружеватоньшенегромкосказалотеципоказалрук
ойвверхгделиствадеревьеввплеталасьвнебоилиможетбытьнебовплеталосьвлиствувсер
авноулыбнулсяотецвсеэтокружевазеленыеиголубыевсмотритесьхорошенькоиувидите
лесплететихсловногудящийстанокотецстоялуверennопохозяйскиирассказывалимвсяк
уювсячинулегкоисвободноневыбираясловчастоонисамсмеялсясвоимрассказамиотэтог
оонитеклиещесвободнеехорошоприслучаепослушатьтишинуговорилонпотомучтотогд
аудаетсяуслышатькакноситсяввоздухепыльцаполевыхцветовавоздухтакигудитпчелам
идадатакигудитавотслышитетамзадеревьямиводопадомльетсяптичьещебетаньевотсей
часдумалдугласвотоноужеблизкоаяещеневижусовсемблизкорядомдикийвиноградсказ
алотецнамповезлосмотритеканенадоахнулпросебядугласнотомиотецнаклонилисьипог
рузилирукившуршащийкустчарырассеялисьтопугающееигрозноечтоподкрадывалосьб
лизилосьготовобылоринутьсяипотрястиегодушуисчезлоопустошенныйрастерянныйду
гласупалнаколенипальцыегоушлиглубоковзеленуютеньивынырнулиобагренныеалымс
окомсловноонвзрезаллесножомисунулрукивоткрытуюранумальчикизавтракатьведрач
утьнедоверхунаполненыдикимвиноградомилеснойземляникойвокруггудятпчелыэтово
всенепчелыацелыймиртихонькомурлычетсвоюпесенкуговоритотецаонисидятназамше
ломстволеупавшегодереважуютсандвичиипытаютсяслушатьлескакслушаетонотецчут
ьпосмеиваясьискосапоглядываетнадугласахотелбылочтотосказатьнопромолчалоткуси
лещекусоксандвичаизадумалсяхлебсветчинойвлесунеточтодомавкуссовсемдругойверн
оостреечтолимятойотдаетсмолойаужаппетиткакразыгрываетсядугласпересталжевать
ипотрогалязыкомхлебиветчинунетнетобыкновенныйсандвичтомкивнулпродолжаяжев
атьяпонимаюпавведьужепочтислучилосьдумаетдугласнезнаючтоэтоноонобольшущее
прямогромадноечтотоегоспугнулогдежеонотеперьопятьушловтоткустнетгдетозамной
нетнетздесьтутрядомдугласисподтишкапощупалсвойживотоноещевернетсянадотольк
онемножкоподождатьбольнонебудетяужзнаюнезатемонокомнепридетнозачемжезачем
а

Висновки:

Під час виконання лабораторної роботи на прикладі розкриття моноалфавітної підстановки ми набули навичок частотного аналізу та опанували прийоми роботи в модулярній арифметиці. А саме, в

ході виконання цієї лабораторної роботи ми навчились дешифрувати текст отриманий в результаті шифрування за допомогою афінної підстановки біграм відкритого тексту; реалізували підпрограми для обчислення оберненого елемента та розв’язання лінійних порівнянь; реалізували автоматичний розпізнавач російської мови.