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

ЛАБОРАТОРНА РОБОТА №3

«Криптоаналіз афінної біграмної підстановки»

Виконали:
Студенти групи ФБ-04
Музичка-Скрипка Олександра
Кузьмін Гліб
Перевірив:
Чорний О.

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 №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: для того, щоб виконати перше завдання, нашою командою були реалізовані функції inverted_number та linear_equation, що обчислюють обернений елемент за модулем із використанням розширеного алгоритму Евкліда та розв'язують лінійні рівняння відповідно.
Для виконання другого завдання нами була реалізована функція bigram_counter, яка є трохи модифікованою програмою обчислення частот біграм, що була написана в ході виконання комп'ютерного практикуму №1. П'ять найчастіших біграм шифртексту 6 варіанту у порядку спадання: ЩЕ, ХЕ, ЧВ, ЛЕ, ЦВ.
Для виконання третього завдання була реалізована функція possible_keys, яка спочатку перебирає усі можливі варіації пар з найпопулярніших біграм шифртексту та російської мови, після чого за допомогою linear_equation та перевірки на взаємну простоту генерує усі можливі пари ключів та додає у список finding_keys без повторень.
Для виконання четвертого і, водночас, п'ятого завдання наша команда реалізувала функцію result, яка на початку роботи отримує результат з функції possible_keys (тобто усі можливі пари ключів, що зберігаються у змінній finding_keys), та намагається розшифрувати текст кожною парою ключей (розшифровує по одній біграмі за допомогою реалізованої раніше функції inverted_number та додає результат у змінну decrypted_text, доки весь текст не буде розшифрованим). Для відсіювання неправильно розшифрованих текстів і, відповідно, неправильних ключей наша команда взяла формулу пошуку ентропії, що була написана в ході виконання комп'ютерного практикуму №1, та знаходила значення ентропії для кожного з кандидатів на розшифрований текст. Якщо ентропія кандидата не потрапляла у проміжок між 4.4 та 4.5 (під час виконання першої лабораторної роботи ми отримали значення ентропії російської мови, що дорівнює приблизно 4.46, та перевірили це значення у інтернеті), то кандидат відсіювався, і алгоритм розпочинався спочатку вже для наступної пари ключей. На 128 спробі нам вдалося розшифрувати текст, який я приведу трохи нижче.

Зашифрований текст:
ывлеюгзебщпещхщуйэвиывиюфгувхцубхщыюнюжлепэшфмиьхдощбуднзегдщебоцвшуюгьпцвэщувкмзеиэбчиюндхщюасдбмонхегщгдэщжезьщемвощфысьмайыегыййяййыэшжеаеки

дщщеюжгьдеьцонгочвнюиюыжвюуеьбюгьщесфвшвоюзйэящкщьюгочвнюлмшужеейцурпц
вдэяхщаюьдеуэвющэвдиайятвепцвчвлеюйщецыаешвэеяикгехщаэациэибвкмрйжуажййдек
ущтепэшфмздсугьвоцвяйкзфтшшхдуюиьйынюгдхацовойэращеюияциаяимюыжцввджвяцэ
ввлломоодмхщуйэмюэзопюзкнэщегбдсефвьхбжщенюцатщввэиегтеаехохтюйлдицзьхдщщ
щюяьзщюоцвлеюосдлузлзащавызйферддьйомюиаыьепжмнюбжщцаещэзойтзэвзвщупмюж
ьощшаощвыжееююззьдеаейюшдоездюйбпгьвиюэколпщхмоихсшфеэмлеотзомщйвхцывбж
хебахиэьщхйэашжеттфележебдфюфпнюфмшуиэжяппшдгдщесдцжцвхеюцхеяднвжееютбз
ййысддемилпмюзахшнюлллоюэпподйшяюьхщужиуцтабззлзьйопнбоящпиэщииамленйхдб
днвнщлврпшилмиьадшахушайыэффтппмюцдсззезщадцьцихжшуфгбиэихеныжпбоцднесде
гмаущйыктгдыйктййнвмоктздгидатаомтщлвхеийрдимяцшуьюывмтшзюашнэьгоэавюрдвд
жгмпиээщеиэивдодзехатщйыэшззшзунзщхеюизчсдэайэхенвжьфжпсхгчплвжмвиртдэппщу
ртцюиэппедчйдещорпдпвюбжлотвдюлофехщыддетеодаьйояхрдбмлпнднелеыщхдощуцщаз
нибыутвднтащебацэзьгордфесьаещзкнсднюятьдаахмчвюцхеиовющежемпзькюжямюгьщцс
бвдсчепзлепэшбмтвгоэвубюзмвппцинэзьэщтапуиэпхлеоенщнщрдэщлабмхтфуиюййаещэдэ
влюцрпбжэщыдидсдщохилпийшгмищцвюбйощйапедмлесгцатьчщбуэьгйцамиэавдкюяцро
рпбдкьйомьщеаохдяючвейчвэухвьхэерючежюшзюахмрпяйзхфйдыжецэзчящктмоодььепю
йяйрйощоюцдиеиатщхщнеэмьхгьощщеоюиьвдгивюыжшухехщкдэщжюяцлщлейдюйбпгью
йяйгдидндидбосдьдиараощаагюывмтвдцэззэяхщаыйжгпюфпэшяияйхмлпияюцмахщмайвкм
шуовывбочвгййобуиэывзджююцгйбасдйэвюэасуяхуцбущуфтлпэьвмхшоеяхрпдюцибофеба
итвлпхлпэьуеюююэлпбийэлпбинюфугьвоцвхестюцгдтэфйнеэатщщавытдщааошумюжячеа
еэоодзтлояййысьюцсьмашайыьхлеяюсбфеюоэщуйзлепрдюйкизолюуцобуйюгктнвэииюдэя
хщагююцхенедефепэлпсаийкиящбушзшзунтахаьыхдрпдэьщчижеьюхибунюзьдесьюцаетщ
феюайвкмжгеэзчхаздхенехднвящжесьвчаеяютвючсьцукммюфпэьхцхенеещжпмюфгцвцвз
щяшдыээжежуйэфгэзюайычщоднвкгшвиьвчлпэьяьхэжмьхиьбщйыфпжягьматщаефмлесгца
дьтцэьакгдйпгцэьдемимоэщчртшгдьцэьщщузмюнпамвикнсшувлонвиюовкмлебпчвмвзьже
мвшзгдяиампнлоппбообхдвыхщнвшуялнюгьэабуохобхдзечадыегжеыщхдктеаюаирюунедм
щуудвайыэанвфупдэмчвмьщелеяймоюааачвэуопэьжеюэюааееыпхщаэаяхзснгыетепюхиэьа
елецюктпмзшршеьбюекгдьвтщшдчиубждгдхеьцкнвюиэвднвфузчшщдетадшимжйцумюэщ
чйощйаэмтщвдеьйомюхебавахивлфеионвздоюубтесаыдхщнвшуцуюэрдцзщхмвлоцущцша
йюшдрддебочищукмжйпиуцфйжпщцоеидфгшйощемлмжгвдфвюаюообюаюьймвшжеэуяхх
ариндщщэщгщчикгялнювамжфуощпйццмюегнещеегбдфюфпюйбпгьфпжяиэцвтбнещеегбм
лещщзеяйьддьяецыфгсцфжтбшвяцвиощиалещщнвбчрйхаюиючпммьшгяошулобжфгфиыж
пптбшвиьййраыьнщеаощяэшулопдицщццаявяцбуиьэщхдвыбщпееыаебухтвдсдощийыщцы
эщзщцймилмлежщощрасгиацэиюшщыйзащеоюиьцвмтшзлебджювшщхщужиубяэшулопдх
омццвяйощвыявжявщэаадощыщтщкщфйыьжеуцщуыднвлеьэяхщабммоппмвппдюлмледшя
йдужижиженввиищятпнзетечютдюйбпгьчизднвепфйзщиакунэшщфпызяйтьхиэиианвзшущ
иорпбдпюцижефвчвйэгцлппнющецыаеямтщтаэаощськммочиэилпбоодэаьдааощчвощоюшд
ийрднпцвдщнюиадежпиэвиьхсшрдехщуйэтфппрюфпюцпмлпиящцоугьцааюфпэьаэвдтщфе
оещпхэбонноциафпжяфпцвчвжьфждэлолвяьчвдодэйайыжевыоененезаиаразевыбвжйцулм
лепеяшдерйхаюииэяхщагютврюфпэшиацаыввюсюлоюэуцвшэщйыаегюфпгьпднеизящсдж
пннхезефюфпящчвэвьхлммьдшоюьхиьрйрарежюгьщелекщтьээмюфзнэцвсдмааеюиэисьмю
цвэиубэфгшдещечйшвюзкоусжээштеяииюфггшкееюччэацапесьзецюмозьхцоуоеуюмодшя
ййыхетеуиэижецэзчтэгчяййыбозэгчяййымааейшгюдпюйбпгьищщхйэзьлвепцвсдчйыутвыв
яцбехдыиьхзавдсщяобамщсдэанелезатэфйфщиээщнежетщгдидчвряоеуюжйжпннтвшивлуг
цхлехщтапэсбеелеяоодгджюубвюцдеюччщупнлмлеяешайыиалимьящфгмючехйуышзкоусб
щмазщбиьхзазьйысьзьюауйжекюжмтщкдцьщхйэашцааюцвмабзнэщежееюсюбжовщцэапей
цщцвюлозьйычвййзаятдпэшьхлеяюсбеужищеегдьдэбоодфееаоененетщкервтвэитзщанезчу
дйожецэзчкмючсджэзлрдяюнюиюэзмюсетпыжтащенепхсшыщьвчвнюлоиэяцсбэапепещдй
огдыйхедетамайвднвюдэяхщавомоодбпртгьоецуппиачпковфндхщоедесшсдкюэьдэяцсдцаа
юцвэщфепэюцзасеяинэшзчуртэщсззееысдкюмвежцищемарцзлцвпепемайыщпзьуасьцвэию
эяхщавоцэлеююфпрдеыэвчвтааеувэетеьджюсббамщиаиьмахенщщавысьщцяцодчэтдбщпен
егдеаиююуэзлвиюэзлпмотвяьреэщдепвлпзщшаощсуяхсуяхлпвидшхщпелееецацабацыещз

щеггдюпшщмцкнвюутючшабщощщщэщжлзьдшфглоиэюаэьубяшбммьшгжюуббуиьппбжх
ееэщуьхамьхфйсщощвыятжмючктюцощщпвлхешекюиэзосднефепэчщущхдижппчиртлпчв
рянюбоодщэзопсеьаохтгднщхекудээиэибацыещкибохтгдййаююэяхщаяэяхщавонвздадяйть
реошйынщмаонгоюзщатаььтаэазехдвьнйнвэьдюртюцгсдееэюцгющцччщупнлмжмящнюпх
мьшияцдеыуппамрпзьроадздыщчврялежпсбамгдещнвсбэаэщьэяхщаеадежпиээщщьюцмюе
паелешгкитвяцдееюдпэьдюиюложьвиибпейцамиьоецуппбозацыжервщцжиртлпцацытдоех
дсвщцюзмвусщекуяцфгкмрпцвсдчйбщцщлоцвкгвюфттщнгкмжгпййождгдфгнхрйжщиаквб
жхебуктюаоюцдзщшгюйбпгьбпбюфпбвмьщелеяйэщщднесдроюэппамбжронвжешатьэзреб
циюывэцчврятазщрдюйкизоажхенежетщттххдэтахщшщсьцвэиюэяхщалттвящуэбчиюндам
тщжпунлпэшшвчвйэрпуюиьрйещйыэшдеюйбазеашллььоусзочвцаделекюцииайгшацвэшвд
сдтщеорпиьчврясдщелечпбопнххлпфмшуиэщщсдлоиэледещохиболпжйсднегужиоаэвбжро
нвпйцвгщнюаеегыюфпждвпщюиьаепзкнбатахщьпсефггдяилмепэшэвчвадздююубиьмюмтч
еодеычмдэлпепэьйыямвиртюцсшсднвлптвэиубшштиубзчшгыьгйцаоиэивюрдрячиртлпще
щьмоодяюзьжгхюйэяхщабмчвлеааатюцгсхеэщщднесдюфывепнюсьлоздшшианвщузлмюхе
буэьрймщшатьтцьеэуллмюзэгцлпнюшвчвиьрйещеьбюбжщенюиьмахенщтьаобчйэылщхрд
шгматжщешгмааеюцжьгджювитщразервяцсехдйнощзацыбддебщпезмйэтвощжестюцгдиав
оцвмюцвэулллотвнюжнмющхлеуииьтаэазехдющдетаэадужиубхошунхрдощнвшардздхыло
фмгдмащавыцюэздщощоеядьзхвдюэзмочпцвлпиьгоощнвпйсьшузохефпызяйтьрехджоодэв
вифйядшаждгдфггщнерйюглофцчвтщхдвыпелебдеыаеьйнщыщхдгдбмгдхдбщььзецюьхнэс
фибнвиювичврянвзшрйвдзджюлмгчхтзбчишщюаюьтайгшаощюоэшййшоэшещяйгдтидщво
юзйэхесдегжщюаыьзекжгьщенюэьщцфцжштьыьжеуцюаюьтаэахщчвэвьхэеэщхдупндидво
юзйэсдвчщупнлмтщжпежуддежпунтвовднвюяхмощуепнюдещечйшвчвьхзанэудеьщйжпнн
твшиэихещщеьаожецэзчкмопияжмрплобчжоцвмозохтюйквэипхнэмвижппщцюэдэтвэипхн
эмвзочвжпннмвцвщцэардздхытцбойэлмдэяццыцвэшявхжпдидьдмаеылочводэжгьюйбауэях
щавочвнюжйядтпктаевшэфмюлоылмьмоодпзощпищуээяцышзщиовюьхюааьтаэазехдзющц
девдюпиьоецумвбииюмюдэпааюфпбуиьэээяхщагючвяцсехдзюэизеэщощвыамьхфйсщощ
фйзщшнюучаущюимьюжфучугьоддпэьовлмяхусидгщкухтхеажщедещиюаугшазевытпктеп
иьсхчвмоюзопщувюывяьчщдецуыьбщщхйэунищцжфтзелммьщебджюсбюанвшубюфгеэях
щаыйцачюэирпмюамлпияцднеунощбпвзвимождгдяйдвмюьщегфгыюфпсесакумюфгоажгщ
ьвияцжпмохенюятздэаьпзьхегехщыйяйдужибочвэухвэсюаяйбацыещзщэабвюатайывдсуыж
ыывдюиэмошушйиадечюмюзэциуцнщхекудэяцепзьхестюцсшэщаеиовифйлхнэлвижппикще
жесьмюкмщджгмяппсбхщжвччнюшияцюужгщдеьжечмзьмюййнежетщщехдйанюэьюэлвиа
эабнппяцнвжегдпмзобднердздшамйдвеавэнщещамхвусеьыьрйчайыгдчиэижпунудщехехдь
жыввмиькдбовшвыэьаееадебпээкоудкюдэяхщаеапехдизопбжщещечирттвдюлмлеоелжлпч
вййщщгдидййтельиюдохжящэаюйбатьцчгдкьвдюжвюубщпзьсюцвбжщефебалимьтесьюцс
уяхубвдыюэенвздажщеощшшщешежэудеьоезелаллжмадбщяиэиюайгкукоудеьээяхщабмшу
зьмасллотвьщдецуьхлпйтаияцгпэзбоцвещяйсдкюцвюзаихевджюсбеавэнщшвяцзщцюфпбу
йэрпхаьллотвюшдеэщбачмжмвддыллкмбжбщжпежепиьаэгцуджэяхщагюфтианжщеэвнюэе
хеяецыойидкмхшоекуяцдэхеажщещещхиьнйююфпьхрдяднючвкмшууеошйыунзебвчвййнв
сдчхрдщеэаяюубсдкюцвцэзьовывхшфеьэяхщащщбмйэбщкижмюфпмлпвоубкщжещехеэфл
ошусдеьбюдэчврпшинююцхеиилмйэзлзайыяецыхесдийрддшлльюуссдэахдоехеаеяюкмтщр
дкюхтыжюцядэащдба

Знайдений ключ та розшифрований текст:
[441, 310]
утробылотихоегородокутанныйтьмоймирнонежилсявпостелипришлолетоиветербыллетни
йтеплоедыханиемиранеспешноеиленивоестоитлишьвстатьвысунутьсявокошкоитотчаспой
мешьвотонаначинаетсянастоящаясвободаижизньвотонопервоеутролетадуглассполдингдве
надцатилетотродутолькочтооткрылглазаикаквтеплуюречкупогрузилсявпредрассветнуюбез
мятежностьонлежалвсводчатойкомнаткеначетвертомэтажевовсемгороденебылобашнивыш
еиоттогочтоонпарилтаквысоковвоздухевместесиюньскимветромвнемрождаласьчудодейст
веннаясилапоночамкогдавязыдубыикленысливалисьводнобеспокойноеморедугласокидыва

леговзглядомпронзавшимтьмуточномаякисегоднявотздоровошепнулонвпередицелоелетон
есчетноемножестводнейчутьнеполкалендаряонужевиделсебямногорукимкакбожествошив
аизкнижкипропутешествиятолькопоспевайрватьещезеленыеяблокиперсикичерныекакночь
сливыегоневытащитьизлесуизкустовизречкиакакприятнобудетпомерзнутьзабравшисьвзаи
ндевелыйледниккаквеселожаритьсявбабушкинойкухнезаодностысячьюцыплятапоказадело
развнеделюемупозволялиночеватьневдомикепососедствугдеспалиегородителииимладшийб
ратишкатомаздесьвдедовскойбашнеонвзбегалпотемнойвинтовойлестниценасамыйверхило
жилсяспатьвэтойобителикудесникасредигромовивиденийаспозаранкукогдадажемолочник
ещенезвякалбутылкаминаулицахонпросыпалсяиприступалкзаветномуволшебствустоявтем
нотеуоткрытогоокнаоннабралполнуюгрудьвоздухаиизовсехсилдунулуличныефонаримиго
мпогаслиточносвечкиначерномименинномпирогедугласдунулещеиещеивнебеначалигасну
тьзвездыдугласулыбнулсяткнулпальцемтамитамтеперьтутивоттутвпредутреннемтуманеод
инзадругимпрорезалисьпрямоугольникивдомахзажигалисьогнидалекодалеконарассветной
землевдругозариласьцелаявереницаоконвсемзевнутьвсемвставатьогромныйдомвнизуожил
дедушкавынимайзубыизстаканадугласнемногоподождалбабушкаипрабабушкажарьтеолад
ьисквознякпронесповсемкоридорамтеплыйдухжареноготестаивовсехкомнатахвстрепенули
сьмногочисленныететкидядьядвоюродныебратьяисестрычтосехалисьсюдапогоститьулица
стариковпросыпайсямиссэленлумисполковникфрилеймиссисбентлипокашляйтевстаньтепр
оглотитесвоитаблеткипошевеливайтесьмистерджонасзапрягайтелошадьвыводитеизсарояф
ургонпораехатьзастарьемпотусторонуоврагаоткрылисвоидраконьиглазаугрюмыеособняки
скоровнизупоявятсянаэлектрическойзеленоймашинедвестарухиипокатятпоутреннимулица
мприветственномахаякаждойвстречнойсобакемистертридденбегитевтрамвайноедепоивско
репоузкимрусламмощеныхулицпоплыветтрамвайрассыпаявокругжаркиесиниеискрыджон
хафчарливудменвыготовышепнулдугласулицедетейготовыспросилонубейсбольныхмячейч
томоклинаросистыхлужайкахупустыхверевочныхкачелейчтоскучаясвисалисдеревьевмамп
аптомпроснитесьтихонькопрозвенелибудильникигулкопробиличасызданиисудаточносе
тьзаброшеннаяегорукойсдеревьеввзметнулисьптицыизапелидирижируясвоиморкестромду
гласповелительнопротянулрукуквостокуивзошлосолнцедугласскрестилрукинагрудииулыб
нулсякакнастоящийволшебниквоттотодумалонтолькояприказаливсеповскакаливсезабегал
иотличноебудетлетоионнапоследокогляделгородищелкнулемупальцамираспахнулисьдвер
идомовлюдивышлинаулицулетотысячадевятьсотдвадцатьвосьмогогоданачалосьвтоутропр
оходяполужайкедугласнаткнулсянапаутинуневидимаянитькоснуласьеголбаинеслышнолоп
нулаиотэтогопустячногослучаяоннасторожилсяденьбудетнетакойкаквсенетакойещеипото
мучтобываютднисотканныеизоднихзапаховсловновесьмирможновтянутьносомкаквоздухв
дохнутьивыдохнутьтакобяснялдугласуиегодесятилетнемубратутомуотецкогдавезихвмаши
незагородавдругиедниговорилещеотецможноуслышатькаждыйгромикаждыйшорохвселен
нойиныеднихорошопробоватьнавкусаиныенаощупьабываютитакиекогдаестьвсесразувотна
примерсегодняпахнеттакбудтоводнуночьтамзахолмаминевестьоткудавзялсяогромныйфру
ктовыйсадивседосамогогоризонтатакиблагоухаетввоздухепахнетдождемнонанебениоблач
катогоиглядиктотоневедомыйзахохочетвлесунопокатамтишинадугласвовсеглазасмотрелна
плывущиемимополянетнисадомнепахнетнидождемдаиоткудабыразнияблоньнетнитучикто
тамможетхохотатьвлесуавсетакидугласвздрогнулденьэтоткакойтоособенныймашинаостан
овиласьвсамомсердцетихоголесаануребятанебаловатьсяониподталкивалидругдругалоктям
ихорошопапамальчикивылезлиизмашинызахватилисиниежестяныеведраисойдяспустынно
йпроселочнойдорогипогрузилисьвзапахиземливлажнойотнедавнегодождяищитепчелсказа
лотецонивсегдавьютсявозлевиноградакакмальчишкивозлекухнидугласдугласвстрепенулся
опятьвитаешьвоблакахсказалотецспустисьназемлюпойдемснамихорошопапаионигуськомп
обрелиполесувпередиотецрослыйиплечистыйзанимдугласапоследнимсеменилкоротышкат
омподнялисьнаневысокийхолмипосмотреливдальвонтамуказалпальцемотецтамобитаютог
ромныеполетнемутихиеветрыинезримыеплывутвзеленыхглубинахточнопризрачныекитыд
угласглянулвтусторонуничегонеувиделипочувствовалсебяобманутымотецкакидедушкавеч
ноговоритзагадкамииивсетакидугласзатаилдыханиеиприслушалсячтотодолжнослучитьсяп

одумалоняужзнаюавотпапоротникназываетсявенеринволосотецнетороплівошагалвпередс
инееведропозвякивалоунеговрукеаэточувствуетеионковырнулземлюноскомбашмакамилли
онылеткопилсяэтотперегнойосеньзаосеньюпадалилистьяпоказемлянесталатакоймягкойухт
ыяступаюкакиндеецсказалтомсовсемнеслышнодугласпотрогалземлюнониченогонеощутилон
всевремянастороженноприслушивалсямыокруженыдумалончтотослучитсяночтооностанов
илсявыходижегдетытамчтотытакоемысленнокричалонтомиотецшлидальшепотихойподатл
ивойземленасветенеткружеватоньшенегромкосказалотеципоказалрукойввержгделиствадер
евьеввплеталасьвнебоилиможетбытьнебовплеталосьвлиствувсеравноулыбнулсяотецвсеэто
кружевазеленыеиголубыевсмотритесьхорошенькоиувидителесплететихсловногудящийста
нокотецстоялуверennопохозяйскиирассказывалимвсякуювсячинулегкоисвободноневыбир
аясловчастоонисамсмеялсясвоимрассказамиотэтогоонитеклиещесвободнеехорошоприслуч
аепослушатьтишинуговорилонпотомучтотогдаудаетсяуслышатькакноситсяввоздухепыльц
аполевыхцветовавоздухтакигудитпчеламидадатакигудитавотслышитетамзадеревьямиводо
падомльетсяптичьещебетаньевотсейчасдумалдугласвотоноужеблизкоаяещеневижусовсем
близкорядомдикийвиноградсказалотецнамповезлосмотритеканенадоахнулпросебядугласн
отомиотецнаклонилисьипогрузилирукившуршащийкустчарырассеялисьтопугающееигроз
ноечтоподкрадывалосьблизилосьготовобылоринутьсяипотрястиегодушуисчезлоопустоше
нныйрастерянныйдугласупалнаколенипальцыегоушлиглубоковзеленуютеньивынырнулио
багренныеалымсокомсловноонвзрезаллесножомисунулрукивоткрытуюранумальчикизавтр
акатьведрачутьнедоверхунаполненыдикимвиноградомилеснойземляникойвокруггудятпче
лыэтововсенепчелыацелыймиртихонькомурлычетсвоюпесенкуговоритотецаонисидятназа
мшеломстволеупавшегодереважуютсандвичиипытаютсяслушатьлескакслушаетонотецчуть
посмеиваясьискосапоглядываетнадугласахотелбылочтотосказатьнопромолчалоткусилеще
кусоксандвичаизадумалсяхлебсветчинойвлесунеточтодомавкуссовсемдругойверноостреч
толимятойотдаетсмолойаужаппетиткакразыгрываетсядугласпересталжеватьипотрогалязы
комхлебиветчинунетнетобыкновенныйсандвичтомкивнулпродолжаяжеватьяпонимаюпапв
едьужепочтислучилосьдумаетдугласнезнаючтоэтоноонобольшущеепрямогромадноечтото
егоспугнулогдежеонотеперьопятьушловтоткустнетгдетозамнойнетнетздесьтутрядомдугла
сисподтишкапощупалсвойживотоноещевернетсянадотольконемножкоподождатьбольноне
будетяужзнаюнезатемонокомнепридетнозачемжезачема

У ході виконання лабораторної роботи було виявлено, що у початковому алфавіті потрібно поміняти місцями літери «Ы» та «Ь», щоб отримати коректний результат.

Висновки: під час виконання лабораторної роботи нами була досліджена афінна біграмна підстановка. Нам вдалося розробити алгоритм, який розшифровує цей шифр, з чого можна зробити висновки, що афінна біграмна підстановка не відповідає сучасним вимогам криптостійкості. Також нами були отримані навички частотного аналізу на прикладі розкриття моноалфавітної підстановки та опановані прийоми роботи в модулярній арифметиці