НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені Ігоря СІКОРСЬКОГО»
Фізико-технічний інституту

ЛАБОРАТОРНА РОБОТА №4
з кредитного модуля «Симетрична криптографія»

на тему:
«Побудова генератора псевдовипадкових послідовностей на лінійних регістрах зсуву (генератора Джиффі) та його кореляційний криптоаналіз»
Варіант №6

Виконали:
студенти групи ФІ-03
Гілевський Олександр
Кузьменко Анна

Київ-2023

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 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, опис труднощів, що виникали, та шляхів їх розв'язання
Почали з вивчення методичних вказівок та алгоритму розшифрування афінного шифру. Реалізували необхідні допоміжні функції для обчислення ключа та дешифрування тексту. Зіткнулися з труднощами, пов'язаними з автоматичним розпізнаванням тексту, оскільки отриманий текст мав певні недоліки та помилки.
Знайшли шляхи вирішення проблеми, використовуючи інші підходи до знаходження ключа та аналізу тексту.
У результаті успішно розшифрували текст та отримали змістовний результат.

Знайдені п'ять найчастіших біграм шифротексту
Була використана програма, що була реалізована для комп'ютерного практикуму №1. Результати для нового вхідного тексту (нашого варіанту) такі:
{"ще":46,"хе":44,"чв":42,"ле":40,"цв":38,"ощ":37,"сд":36,"же":36,"де":36,"гд":34,"ню":33,"нв":33,"мю":32,"лп":31…

Результати роботи
Зашифрований текст:
ывлеюгзебщпещхщуйэвиывиюфгувхцубхщыюнюжлепэшфмиьхдощбуднзегдщебоцвшуюгьпцвэщу
вкмзеиэбчиюндхщюасдбмонхегщгдэщжезьщемвощфысьмайыегыйяййыэшжеаекидщщеюжгьдеьц
онгочвнюиюыжвюудеьбюгьщесфвшвоюзйэящкщьюгочвнюлмшужеейцурпцвдэяхщаюьдеуэвющэв
диайятвепцвчвлеюйщецыаешвэеяикгехщаэациэибвкмрйжуажййдекущтепэшфмздсугьвоцвяй
кзфтшшхдуюиьйынюгдхацовойэращеюияциаяимюыжцввджвяцэввлломоодмхщуйэмюэзопюзкнэ
щегбдсефвьхбжщенюцатщввэиегтеаехохтюйлдицзьхдщщщюяьзщюоцвлеюосдлузлзащавызйфе
рддьйомюиаыьепжмнюбжщцаещэзойтзэвзвщупмюжьощшаощвыжееююззьдеаейюшдоездюйбпгьв
июэколпщхмоихсшфеэмлеотзомщйвхцывбжхебахиэьщхйэашжеттфележебдфюфпнюфмшуиэжяпп
шдгдщесдцжцвхеюцхеяднвжееютбзййысддемилпмюзахшнюллююэпподйшяюьхщужиуцтабззлз
ьйопнбоящпиэщииамленйхдбднвнщлврпшилмиьадшахушайыэффтппмюцдсззезщадцьцихжшуфг
биэихеныжпбоцднесдегмаущйыктгдыйктййнвмоктздгидатаомтщлвхеийрдимяцшуьюывмтшзю
ашнэьгоэавюрдвджгмпиээщеиэивдодзехатщйыэшззшзунзщхеюизчсдэайэхенвжьфжпсхгчплв
жмвиртдэппщуртцюиэппедчйдещорпдпвюбжлотвдюлофехщыддетеодаьйояхрдбмллпнднелеыщх
дощуцщазнибыутвднтащебацэзьгордфесьаещзкнсднюятьдаахмчвюцхеиовющежемпзькюжямю
гьщцсбвдсчепзлепэшбмтвгоэвубюзмвппцинэзьэщтапуиэпхлеоенщнщрдэщлабмхтфуиюййаещ

эдэвлюцрпбжэщыдидсдщохилпийшгмищцвюбйощйапедмлесгцатьчщбуэьгйцамиэавдкюяцрорп
бдкьйомьщеаохдяючвейчвэухвьхэерючежюшзюахмрпяйзхфйдыжецэзчящктмоодььепюйяйрйо
щоюцдиеиатщхщнеэмьхгьощщеоюиьвдгивюыжшухехщкдэщжюяцлщлейдюйбпгьюйяйгдидндидбо
сдьдиараощаагюывмтвдцэээяхщаыйжгпюфпэшяияйхмлпияюцмахщмайвкмшуовывбочвгййобуи
эывзджююцгйбасдйэвюэасуяхуцбущуфтлпэьвмхшоеяхрпдюцибофебаитвлпхлпэьуеюююэлпби
йэлпбинюфугьвоцвхестюцгдтэфйнеэатщщавытдщааошумюжячеаееоодзтлояййысьюцсьмашай
ыьхлеяюсбфеюоэщуйзлепрдюйкизолюуцобуйюгктнвэииюдэяхщагююцхенедефепэлпсаийкиящ
бушзшзунтахаыыхдрпдэьщчижеьюхибунюзьдесьюцаетщфеюайвкмжгеэзчхаздхенехднвящжес
ьвчаеяютвючсьцукммюфпэьхцхенеещжпмюфгцвцвзщяшдыээжежуйэфгэзюайычщоднвкгшвиьвч
лпэьяьхэжмьхиьбщйыфпжягьматщаефмлесгцадьтцэьакгдйпгцэьдемимоэщчртщгдьцэьщщузм
юнпамвикнсшувлонвиюовкмлебпчвмвзьжемвшзгдяиампнлоппбообхдвыхщнвшуялнюгьэабуох
обхдзечадыегжеыщхдктеаюаирюунедмщуудвайыэанвфупдэмчвмьщелеяймоюааачвэуопэьжею
эюаааееыпхщаэаяхзснгыетепюхиэьаелецюктпмзшршеьбюекгдьвтщщдчиубждгдхеьцкнвюиэвд
нвфузчшщдетадшимжйцумюэщчйощйаэмтщвдеьйомюхебавахивлфеионвздоюубтесаыдхщнвшуц
уюэрдцзщхмвлоцущцшайюшдрддебочищукмжйпиуцфйжпщцоеидфгшйощемлмжгвдфвюаюообюаюь
ймвшжеэуяххариндщщэщгщчикгялнювамжфуощпйццмюегнещеегбдфюфпюйбпгьфпжяиэцвтбнещ
еегбмлещщзеяйьддьяецыфгсцфжтбшвяцвиощиалещщнвбчрйхаюиючпммьшгяошулобжфгфиыжпп
тбшвиьййраыьнщеаощяэшулопдицщццаявяцбуиьэщхдвыбщпееыаебухтвдсдощийыщцыэщзщцйм
илмлежщошрасгиацэиюшщыйзащеоюиьцвмтшзлебджювшщхщужиубяэшулопдхомццвяйощвыявжя
вщэаадощыщтщкщффыьжеуцщуыднвлеьэяхщабммоппмвппдюлмледшяйдужижиженввиищятпнзет
ечютдюйбпгьчизднвепфйзщиакунэшщфпызяйтьхиэиианвзшущиорпбдпюцижефвчвйэгцлпнюще
цыаеямтщтаэаощськммочиэилпбоодэаьдааощчвощоюшдийрднпцвдщнюиадежпиэвиьхсшрдехщ
уйэтфппрюфпюцпмлпиящщоугьцааюфпэьаэвдтщфеоещпхэбонношциафпжяфпцвчвжьфждэлолвяь
чвдодэйайыжевыоененезаиаразевыбвжйцулмлепеяшдерйхаюиияяхщагютврюфпэшиацаыввюс
юлоюэуцвшэщйыаегюфпгьпднеизящсджпннхезефюфпящчвэвьхлммьдшоюьхиьрйрарежюгьщеле
кщтьээмюфзнэцвсдмааеюиэисьмюцвэиубэфгшдещечйшвюзкоусжээщтеяииюфггщкееюччэацап
есьзецюмозьхцоуоеуюмодшяййыхетеуиэижецээчтэгчяййыбозэгчяййымааейшгюдпюйбпгьищ
щхйээьлвепцвсдчйыутвывяцбехдыиьхзавдсщяобамщсдэанелезатэфйфщиээщнежетщгдидчвр
яоеуюжйжпннтвшивлугцхлехщтапэсбеелеяоодгджюубвюцдеюччщупнлмлеяешайыиалимьящфг
мючехйуышзкоусбщмазщбиьхзазьйысьзьюауйжекюжмтщкдцьщхйэащцааюцвмабзнэщежееюсюб
жовщцэапейцщцвюлозьйычвййзаятдпэшьхлеяюсбеужищеегдьдэбоодфееаоененетщкервтвэи
тзщанезчудйожецээчкмючсджэзлрдяюнюиюэзмюсетпыжтащенепхсшыщьвчвнюлоиэяцсбэапеп
ещдйогдыйхедетамайвднвюдэяхщавомоодбпртгьоецуппиачпковфндхщоедесшсдкюэьдэяцсд
цааюцвэщфепэюцзасеяинэшзчуртэщсззееысдкюмвежцищемарцзлцвпепемайыщпзьуасьцвэию
эяхщавоцэлеююфпрдеыэвчвтааеувэетеьджюсббамщиаиьмахенщщавысьщцяцодчэтдбщпенегд
еаиююуээлвиюээлпмотвяьреэщдепвлпзщшаощсуяхсуяхлпвидшхщпелееецацабацыещзщеггдю
пшщмцкнвюутючшабщощщщэщжлзьдшфглоиэюаэьубяшбммьшгжюуббуиьппбжхееэщуьхамьхфйсщ
ощвыятжмючктюцощщпвлхешекюиэзосднефепэчщущхдижппчиртлпчврянюбоодщэзопсеьаохтг
днщхекудээиэибацыещкибохтгдййаююэяхщаяэяхщавонвздадяйтьреошйынщмаонгоюзщатаьь
таэазехдвьнйнвэьдюртюцгсдееэюцгющцччщупнлмжмящнюпхмьшияцдеыуппамрпзьроадздыщч
врялежпсбамгдещнвсбэаэщьэяхщаеадежпиээщщьюцмюепаелешгкитвяцдееюдпэьдюиюложьви
ибпейцамиьоецуппбозацыжервщцжиртлпцацытдоехдсвщцюзмвусщекуяцфгкмрпцвсдчйбщцщл
оцвкгвюфттщнгкмжгпййождгдфгнхрйжщиаквбжхебуктюаоюцдзщшгюйбпгьбпбюфпбвмьщелеяй
эщщднесдроюэппамбжронвжешатьээребциюывэцчврятазщрдюйкизоажхенежетщттххдэтахщш
щсьцвэиюэяхщалттвящуэбчиюндамтщжпунлпэшшвчвйэрпуюиьрйещйыэшдеюйбазеашллькюусзо
чвцаделекюцииайгшацвэшвдсдтщеорпиьчврясдщелечпбопнххлпфмшуиэщщсдлоиэледещохиб
олпжйсднегужиоаэвбжронвпйцвгщнюаеегыюфпждвпщюиьаепзкнбатахщьпсефггдяилмепэшэв
чвадздююубиьмюмтчеодеычмдэлпепэьйыямвиртюцсшсднвлптвэиубшштиубзчшгыьгйцаоиэив
юрдрячиртлпщещьмоодяюзьжгхюйэяхщабмчвлеааатюцгсхеэщщднесдюфывепнюсьлоздшшианв
щузлмюхебуэьрймщшатьтцьеэуллмюззгцлпнюшвчвиьрйещеьбюбжщенюиьмахенщтьаобчйэылщ
хрдшгматжщешгмааеюцжьгджювитщразервяцсехдйнощзацыбддебщпезмйэтвощжестюцгдиаво
цвмюцвэуллотвнюжнмющхлеуииьтаэазехдющдетаэадужиубхошунхрдощнвшардздхылофмгдм
ащавыцюээздщощоеядьзхвдюэзмочпцвлпиьгоощнвпйсьшузохефпызяйтьрехджоодэввифйядша
ждгдфггщнерйюглофцчвтщхдвыпелебдеыаеьйнщыщхдгдбмгдхдбщььзецюьхнэсфибнвиювичвр
янвзшрйвдзджюлмгчхтзбчишщюаюьтайгшаощюоэшййшоэшещяйгдтидщвоюзйэхесдегжщюаыьзе
кжгьщенюэьщцфцжштыыьжеуцюаюьтаэахщчвэвьхэеэщхдупндидвоюзйэсдвчщупнлмтщжпежудд
ежпунтвовднвюяхмощуепнюдещечйшвчвьхзанэудеьщйжпннтвшиэихещщеьаожецэзчкмопияжм
рплобчжоцвмозохтюйквэипхнэмвижппщцюэдэтвэипхнэмвзочвжпннмвцвщцэардздхытцбойэл
мдэяццыцвэшявхжпдидьдмаеылочводэжгьюйбауэяхщавочвнюжйядтпктаевшэфмюлоылмьмоод
пзощпищуээяцыщзщиовюьхюааьтаэазехдзющцдевдюпиьоецумвбииюмюдэпааюфпбуиьээээяхщ
агючвяцсехдзюэизеэщощвыамьхфйсщощфйзщшнюучаущюимьюжфучугьоддпэьовлмяхусидгщку
хтхеажщедещиюаугшазевытпктепиьсхчвмоюзопщувюывяьчщдецуыьбщщхйэунищцжфтзелммьщ
ебджюсбюанвшубюфгеэяхщаыйцачюэирпмюамлпияцднеунощбпвзвимождгдяйдвмюьщегфгыюфп
сесакумюфгоажгщьвияцжпмохенюятздэаьпзьхегехщыйяйдужибочвэухвэсюаяйбацыещзщэаб

вюатайывдсуыжывдюиэмошушйиадечюмюзэциуцнщхекудэяцепзьхестюцсшэщаеиовифйлхнэлв
ижппикщежесьмюкмщджгмяппсбхщжвччнюшияцюужгщдеьжечмзьмюййнежетщщехдйанюэьюэлви
аэабнппяцнвжегдпмзобднердздшамйдвеавэнщещамхвусеьыьрйчайыгдчиэижпунудщехехдьж
ыввмиькдбовшвыэьаееадебпээкоудкюдэяхщаеапехдизопбжщещечирттвдюлмлеоелжлпчвййщ
щгдидййтельиюдохжящэаюйбатьцчгдкьвдюжвюубщпзьсюцвбжщефебалимьтесьюцсуяхубвдыю
эенвздажщеощшшщешежэудеьоезелаллжмадбщяиэиюайгкукоудеьээяхщабмшузьмасллотвьщд
ецуьхлпйтаияцгпэзбоцвещяйсдкюцвюзаихевджюсбеавэнщшвяцзщцюфпбуйэрпхаьллотвюшде
эщбачмжмвддыллкмбжбщжпежепиьаэгцуджэяхщагюфтианжщеэвнюэехеяецыойидкмхшоекуяцд
эхеажщещещхиьнйююфпьхрдяднючвкмшууеошйыунзебвчвййнвсдчхрдщеэаяюубсдкюцвцэзьов
ывхшфеьэяхщащщбмйэбщкижмюфпмлпвоубкщжещехеэфлошусдеьбюдэчврпшинююцхеиилмйэзлз
айыяецыхесдийрддшллььюуссдэахдоехеаеяюкмтщрдкюхтыжюцядэащдба

Розшифрований текст:

утробылотихоегородокутанныйтьмоймирнонежилсявпостелипришлолетоиветербыллетний
теплоедыханиемиранеспешноеиленивоестоитлишьвстатьвысунутьсявокошкоитотчаспойм
ешьвотонаначинаетсянастоящаясвободаижизньвотонопервоеутролетадуглассполдингдв
енадцатилетотродутолькочтооткрылглазаикаквтеплуюречкупогрузилсявпредрассветну
юбезмятежностьонлежалвсводчатойкомнаткеначетвертомэтажевовсемгороденебылобашн
ивышеиоттогочтоонпарилтаквысоковвоздухевместесиюньскимветромвнемрождалась чудо
действеннаясилапоночамкогдавязыдубыикленысливалисьводнобеспокойноеморедугласо
кидывалеговзглядомпронзавшимтьмуточномаякисегоднявотздоровошепнулонвпередицел
оелетонесчетноемножестводнейчутьнеполкалендаряонужевиделсебямногорукимкакбоже
ствошиваизкнижкипропутешествиятолькопоспевайрватьещезеленыеяблокиперсикичерны
екакночьсливыегоневытащитьизлесуизкустовизречкиакакприятнобудетпомерзнутьзабр
авшисьвзаиндевелыйледниккаквеселожарить сявбабушкинойкухнезаодностысячьюцыплят
апоказаделоразвнеделюемупозволялиночевать невдомикепососедствугдеспалиегородит
елиимладшийбратишкатомаздесьвдедовскойбашнеонвзбегалпотемнойвинтовойлестницен
асамыйверхиложилсяспатьвэтойобителикудесникасредигромовивиденийаспозаранкуког
дадажемолочникещенезвякалбутылкаминаулицахонпросыпалсяиприступалкзаветномувол
шебствустоявтемнотеуоткрытогоокнаоннабралполнуюгрудьвоздухаиизовсехсилдунулул
ичныефонаримигомпогаслиточносвечкиначерномименинномпирогедугласдунулещеиещеив
небеначалигаснутьзвездыдугласулыбнулсяткнулпальцемтамитамтеперьтутиваттутвпре
дутреннемтуманеодинзадругимпрорезалисьпрямоугольникивдомахзажигалисьогнидалек
одалеконарассветнойземлевдругозариласьцелаявереницаоконвсемзевнутьвсемвстават
ьогромныйдомвнизуожилдедушкавынимайзубыизстаканадугласнемногоподождалбабушкаи
прабабушкажарьтеоладьисквознякпронесповсемкоридорамтеплыйдухжареноготестаивов
сехкомнатахвстрепенулисьмногочисленныететкидядьядвоюродныебратьяисестрычтосех
алисьсюдапогоститьулицастариковпросыпайсямиссэленлумисполковникфрилеймиссисбе
нтлипокашляйтевстаньтепроглотитесвоитаблеткипошевеливайтесьмистерджонасзапряг
айтелошадьвыводитеизсараяфургонпораехатьзастарьемпотусторонуоврагаоткрылисвои
драконьиглазаугрюмыеособнякискоровнизупоявятсянаэлектрическойзеленоймашинедве
старухиипокатятпоутреннимулицамприветственномахаякаждойвстречнойсобакемистерт
ридденбегитевтрамвайноедепоивскорепоузкимрусламмощеныхулицпоплыветтрамвайрасс
ыпаявокругжаркиесинииеискрыджонхафчарливудменвыготовышепнулдугласулицедетейгот
овыспросилонубейсбольныхмячейчтомоклинаросистыхлужайкахупустыхверевочныхкачел
ейчтоскучаясвисалисдеревьевмампаптомпроснитесьтихонькопрозвенелибудильникигул
копробиличасыназданииисудаточносетьзаброшеннаяегорукойсдеревьеввзметнулисьптиц
ыизапелидирижируясвоиморкестромдугласповелительнопротянулрукуквостокуивзошлос
олнцедугласскрестилрукинагрудииулыбнулсякакнастоящийволшебникводтотодумалонто
лькояприказаливсеповскакаливсезабегалиотличноебудетлетоионнапоследокогляделго
родищелкнулемупальцамираспахнулись дверидомовлюдивышлинаулицулетотысячадевятьс
отдвадцатьвосьмогогоданачалосьвтоутропроходяполужайкедугласнаткнулсянапаутину
невидимаянитькоснуласьеголбаинеслышнолопнулаиотэтогопустячногослучаяоннасторо
жилсяденьбудетнетакойкаквсенетакойещеипотомучтобываютднисотканныеизоднихзапах
овсловновесьмирможновтянутьносомкаквоздухвдохнутьивыдохнутьтакобяснялдугласуи
егодесятилетнемубратутомуотецкогдавезихвмашинезагородавдругиедниговорилещеоте
цможноуслышатькаждыйгромикаждыйшорохвселеннойиныеднихорошопробоватьнавкусаины
енаощупьабываютитакиекогдаестьвсесразувотнапримерсегодняпахнеттакбудтоводнуно
чьтамзахолмаминевестьоткудавзялсяогромныйфруктовыйсадивседосамогогоризонтатак
иблагоухаетввоздухепахнетдождемнонанебениоблачкатогоиглядиктотоневедомыйзахох
очетвлесунопокатамтишинадугласвовсеглазасмотрелнаплывущиемимополянетнисадомне
пахнетнидождемдаиоткудабыразнияблоньнетнитучиктотамможетхохотатьвлесуавсетаки
дугласвздрогнулденьэтоткакойтоособенныймашинаостановиласьвсамомсердцетихоголе

саануребятанебаловатьсяониподталкивалидругдругалоктямихорошопапамальчикивылез
лиизмашинызахватилисиниежестяныеведраисойдяспустынноймроселочнойдорогипогрузи
лисьвзапахиземливлажнойотнедавнегодождяищитепчелсказалотецонивсегдавьютсявозл
евиноградакакмальчишкивозлекухнидугласдугласвстрепенулсяопятьвитаешьвоблакахс
казалотецспустисьназемлюпойдемснамихорошопапаионигуськомпобрелиполесувпередио
тецрослыйиплечистыйзанимдугласапоследнимсеменилкоротышкатомподнялисьнаневысок
ийхолмипосмотреливдальвонтамуказалпальцемотецтамобитаютогромныеполетнемутихие
ветрыинезримыеплывутвзеленыхглубинахточнопризрачныекитыдугласглянулвтусторону
ничегонеувиделипочувствовалсебяобманутымотецкакидедушкавечноговоритзагадкамии
ивсетакидугласзатаилдыханиеиприслушалсячтотодолжнослучитьсяподумалоняужзнаюав
отпапоротникназываетсявенеринволосотецнетороплivошагалвпередсинееведропозвяки
валоунеговрукеаэточувствуетеионковырнулземлюноскомбашмакамиллионылеткопилсяэт
отперегнойосеньзаосеньюпадалилистьяпоказемлянесталатакоймягкойухтыяступаюкаки
ндеецсказалтомсовсемнеслышнодугласпотрогалземлюноничегонеощутилонвсевремянаст
ороженноприслушивалсямыокруженыдумалончтотослучитсяночтооностановилсявыходиже
гдетытамчтотытакоемысленнокричалонтомиотецшлидальшепотихойподатливойземленасв
етенеткружеватоньшенегромкосказалотеципоказалрукойвверхгделиствадеревьеввплет
алась внебоилиможетбытьнебовплеталосьвлиствувсеравноулыбнулсяотецвсеэтокружева
зеленыеиголубыевсмотритесьхорошенькоиувидителесплететихсловногудящийстанокоте
цстоялуверennопохозяйскиирассказывалимвсякуювсячинулегкоисвободноневыбираясло
вчастоонисамсмеялсясвоимрассказамиотэтогоонитеклиещесвободнеехорошоприслучаеп
ослушатьтишинуговорилонпотомучтотогдаудаетсяуслышатькакноситсяввоздухепыльцап
олевыхцветовавоздухтакигудитпчеламидадатакигудитавотслышитетамзадеревьямиводо
падомльетсяптичьещебетаньевотсейчасдумалдугласвотоноужеблизкоаященевижусовсе
мблизкорядомдикийвиноградсказалотецнамповезлосмотритеканенадоахнулпросебядугл
аснотомиотецнаклонилисьипогрузилирукившуршащийкустчарырассеялисьтопугающееигр
озноечтоподкрадывалосьблизилосьготовобылоринутьсяипотрястиегодушуисчезлоопуст
ошенныйрастерянныйдугласупалнаколенипальцыегоушлиглубоковзеленуютеньивынырнул
иобагренныеалымсокомсловноонвзрезаллесножомисунулрукиваоткрытуюранумальчикизав
тракатьведрачутьнедоверхунаполненыдикимвиноградомилеснойземляникойвокруггудят
пчелыэтововсенепчелыацелыймиртихонькомурлычетсвоюпесенкуговоритотецаонисидятн
азамшеломстволеупавшегодереважуютсандвичиипытаютсяслушатьлескакслушаетонотецч
утьпосмеиваясьискосапоглядываетнадугласахотелбылочтотосказатьнопромолчалоткус
илещекусоксандвичаизадумалсяхлебсветчинойвлесунеточтодомавкуссовсемдругойверн
оостреечтолимятойотдаетсмолойаужаппетиткакразыгрываетсядугласпересталжеватьип
отрогалязыкомхлебиветчинунетнетобыкновенныйсандвичтомкивнулпродолжаяжеватьяпо
нимаюпапведьужепочтислучилосьдумаетдугласнезнаючтоэтоноонобольшущеепрямогрома
дноечтотоегоспугнулогдежеонотеперьопятьушловтоткустнетгдетозамнойнетнетздесьт
утрядомдугласисподтишкапощупалсвойживотоноещевернетсянадотольконемножкоподожд
атьбольнонебудетяужзнаюнезатемонокомнепридетнозачемжезачема

Ключ: (441, 310)

Опис розпізнавача

Програма працює на основі аналізу індексу співставлення, який є метрикою схожості символів у тексті. Індекс співставлення обчислюється для розшифрованого тексту і порівнюється з нормованим значенням для кожної мови.

Основні кроки програми:

1. Задається зашифрований текст txt.
2. Визначається список символів алфавіту ALPH, які використовуються для розшифрування.
3. Функція calc_index обчислює індекс співставлення для розшифрованого тексту. Для цього проходиться по кожному символу зі списку ALPH і підраховує кількість його появ у тексті. За допомогою цих значень обчислюється індекс співставлення k за певною формулою.
4. Існує список ключів keys, які будуть використовуватись для розшифрування тексту.

5. Програма проходиться по кожному ключу зі списку keys і розшифровує текст за допомогою функції dec_text. Отриманий розшифрований текст зберігається у змінній decoded_text.
6. Перевіряється, чи є розшифрований текст порожнім. Якщо так, програма переходить до наступного ключа.
7. Обчислюється індекс співставлення для розшифрованого тексту decoded_text за допомогою функції calc_index.
8. Розраховується різниця між обчисленим індексом співставлення та нормованим значенням norm_I.
9. Якщо різниця менша за певне порогове значення, вважається, що мова розшифрованого тексту співпадає зі знайденою мовою, і виводиться розшифрований текст та відповідний ключ. Виконання програми завершується.
10. Якщо жоден з розшифрованих текстів не відповідає умовам, програма продовжує своє виконання до кінця без виведення результатів.

Висновок

В ході виконання цієї лабораторної роботи ми успішно набули навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки. Цей прийом аналізу допоміг нам відновити змістовний текст з зашифрованого повідомлення, використовуючи частотну структуру мови та статистику появи окремих символів.

Також, ми опанували прийоми роботи в модулярній арифметиці, зокрема знаходження оберненого елемента за модулем та розв'язування лінійних порівнянь за модулем. Ці навички дозволили нам виконувати обчислення з використанням арифметичних операцій над числами у модульному просторі, що є важливим у криптографії.

Отримані навички частотного аналізу та роботи в модулярній арифметиці допоможуть нам у подальших криптографічних дослідженнях та розв'язанні задач забезпечення безпеки даних. Ми освоїли необхідні інструменти та методи для аналізу та розкриття шифрів, що робить нас більш компетентними в галузі криптографії.