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

ЛАБОРАТОРНА РОБОТА №3

з дисципліни «Криптографія»

«Криптоаналіз афінної біграмної підстановки»

Виконали:
студент 3 курсу ФТІ
групи ФБ-81
Романченко Анатолій
Перевірили:
Чорний О.

Київ – 2020

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

Порядок виконання роботи

1. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
2. 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.
3. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму No1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
4. 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).
5. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
6. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Хід роботи

ВАРІАНТ-17

Я обрав 3 найчастіших біграми російскої мови та три найчастіші бграми зашифрованого тексту

From lang: ['ст', 'но', 'то']
From text: ['вк', 'нв', 'ья']

З них я отримав 12 ключів

Keys: [(95, 191), (925, 472), (866, 286), (830, 686), (36, 436), (131, 555), (653, 718), (491, 596), (308, 720), (799, 283), (470, 312), (162, 958)]
Amount: 12

Текст перевіряється на «змістовніть» за допомогою індексу відповідності.
За основу взято значення 0.055, а також допускається абсолютна похибка у 0.005.
Тобто текст змістовний якщо його індекс відповідності $0.05 < I\_C < 0.6$.

Програма знайшла лише один «змістовний текст».

Key: (470, 312)

Conformity index: 0.05508162973456312

Decoded:

борисзаэтовремясвоейслужбыблагодарязаботаманнымихайловнысобственнымвкусамисвойствамсвоегосдержанногохарактерауспелпоставитьсебявсамоевыгодноеположениепослужбеоннаходилсяадъютантомпривесьмаважномлицеимелвесьмаважноепоруч
ениевпруссиюитолькочтовозвратилсяоттудакурьеромонвполнеусвоилсебетупонравившуюсяемувольмюценеписаннуюсубординациюпокоторойпрапорщикмогстоятьбезсравнениявышегенералаипокоторойдляуспеханаслужбебылинужнынеусилиянаслужбе
нетрудынехрабростьнепостоянствоанужнобылотолькоуменьеобращатьсястемикоторыевознаграждаютзаслужбуиончастосамудивлялсясвоимбыстрымуспехамитомукакдругиемоглинепониматьэтоговследствиеэтогооткрытияеговесьобразжизниеговсеотно
шенияспрежнимизнакомымивсеегопланынабудущеесовершенноизменилисьонбылнебогатнопоследниесвоиденьгионупотреблялнаточтобыбытьодетымлучшедругихонскореелишилбысебямногихудовольствийчемпозволилбысебеехатьвдурномэкипажеилип
оказатьсявстароммундиренаулицахпетербургасближалсяониискалзнакомствтолькослюдьмикоторыебыливышеегоипотомумоглибытьемуполезныонлюбилпетербургипрезиралмосквувоспоминаниеодомеростовыхиоегодетскойлюбвикнаташебылоемунепри
ятноионссамогоотездавармиюниразунебылуростовыхвгостинойанныпавловнывкоторойприсутствоватьонсчиталзаважноеповышениепослужбеонтеперьтотчасжепонялсвоюрольипредоставиланнепавловневоспользоватьсятеминтересомкоторыйвнемзаклю
чалсявнимательнонаблюдаякаждоелицоиоцениваявыгодыивозможностисближенияскаждымизнихонселнауказанноеемуместовозлекрасивойэленивслушивалсявобщийразговордядюшканеодобрительнооглянулсянапетюинаташуоннелюбилсоединятьбаловст
воссерьезнымделомохотыздравствуйтедядюшкаимыедемпрокричалпетяздравствуйтетоздравствуйтедасобакнепередавитестрогосказалдядюшканиколенькакакаяпрелестнаясобакатрунилаонузналменясказаланаташапросвоюлюбимуюгончуюсобакутрунила
вопервыхнесобакаавыжлецподумалниколайистроговзглянулнасеструстараясьейдатьпочувствоватьторасстояниекотороедолжнобылоихразделятьвэтуминутунаташапонялаэтовыдядюшканедумайтечтобымыпомешаликомунибудьсказаланаташамыстанемна
своемместеинепошевелимсяихорошееделографинечкасказалдядюшкатолькослошадитонеупадитеприбавилонаточистоеделомаршненачемдержатьсятоостровотрадненскогозаказавиднелсясаженяхвостаидоезжачиеподходиликнемуростоврешивокончательн
осдядюшкойоткудабросатьгончихиуказавнаташеместогдеейстоятьигденикакничегонемоглопобежатьнаправилсявзаезднадоврагомнуплемянничекнаматерогостановишьсясказалдядюшкачурнегладитьпротравитькакпридетсяотвечалростовкарайфюиткрикн
улонотвечаяэтимпризывомнасловадядюшкикарайбылстарыйиуродливыйбурдастыйкобельизвестныйтемчтоонводиночкубиралматероговолкавсесталипоместамстарыйграфзнаяохотничьюгорячностьсынапоторопилсянеопоздатьиещенеуспелидоезжачиепод
ехатькместукакильяандреичвеселыйрумяныйстрясущимисящекаминасвоихвороненькихподкатилпозеленямкоставленномуемулазуираспрaвившубкуинадевохотничьиснарядывлезнасвоюгладкуюсытуюсмирнуюидобруюпоседевшуюкакионвифлянкулошаде
йсдрожкамиотослалиграфильяандреичхотяинеохотникподушенознавшийтвердоохотничьизаконывехалвопушкукустовоткоторыхонстоялразобралповодьяоправилсянаседлеичувствуясебяготовымоглянулсяулыбаясьподленегостоялегокамердинерстаринны
йноотяжелевшийездоксеменчекмарьчекмарьдержалнасворетрехлихихнотакжезажиревшихкакхозяинилошадьволкодавовдвесобакиумныестарыеулеглисьбезсворшаговнастоподальшевопушкестоялдругойстремяннойграфамитькаотчаянныйездокистрастн
ыйохотникграфпостариннойпривычкевыпилпередохотойсеребрянуючаркуохотничьейзапеканочкизакусилизапилполубутылкойсвоеголюбимогобордоильяандреичбылнемножкокрасенотвинаиездыглазаегоподернутыевлагойособенноблестелиионукутанны
йвшубкусидянаседлеимелвидребенкакоторогособралигулятьхудойсовтянутымищекамичекмарьустроившисьссвоимиделамипоглядывалнабаринаскоторымонжиллетдушавдушуипонимаяегоприятноерасположениедухаждалприятногоразговораещетретьели
цоподехалоосторожновидноужеонобылоученоиззалесаиостановилосьпозадиграфалицоэтобылстариквседойбородевженскомкапотеивысокомколпакеэтобылшутнастасьяивановнанунастасьяивановнаподмигиваяемушопотомсказалграфтытолькооттопайзве
рятебеданилозадастясамсусамсказалнастасьяивановнашшшшшзашикалграфиобратилсяксеменунатальюильиничнувиделспросилонусеменагдеонаонииспетромильичемотжаровыхбурьяновсталиотвечалсеменулыбаясьтожедамыаохотубольшуюимеютатыудив
ляешьсясеменкаконаездитасказалграфхотьбымужчиневпорукакнедивитьсясмелоловкоаниколашагденадлядовскимверхомчтольвсшопотомспрашивалграфтакточносужонизнаютгдестатьтактонкоездузнаютчтомысданилойдругойраздивудаемсяговорилсеме
нзнаячемугодитьбаринухорошоездитаанаконетокаковакартинуписатькакнамеднисьиззаварзинскихбурьяновпомкнулилисуонипереска кивaтьсталиотуймищастрастьлошадьтысячарублейаседокуценынетдаужтакогомолодцапоискатьпоискатьповторилграфв
идимосожалеячтокончиласьтакскоро речьсеменапоискатьсказалонотворачиваяполышубкиидоставаятабакеркунамедникакотобеднивовсейрегалиивышлитакмихаилтосидорычсеменнедоговорилуслыхавяснораздававшийсявтихомвоздухегонсподвываниемне
болеедвухилитрехгончихоннаклонивголовуприслушалсяимолчапогрозилсябаринунавыводокнатеклипрошепталонпрямоналядовскойповелиграфзабывстеретьулыбкуслицасмотрелпередсобойвдальпоперемычкеиненюхаядержалврукетабакеркувследзалаем
собакпослышалсяголосповолкуподанныйвбасистыйрогданилыстаяприсоединиласькпервымтремсобакамислышнобылокакзаревелисзаливомголосагончихстемособеннымподвываниемкотороеслужилопризнакомгонаповолкудоезжачиеуженепорскалиаулюл
юкалиииззавсехголосоввыступалголосданилытобасистыйтопронзительнотонкийголосданилыказалосьнаполнялвесьлесвыходилиззалесаизвучалдалековполеприслушавшисьнесколькосекундмолчаграфиегостремяннойубедилисьчтогончиеразбилисьнадвест
аиоднабольшаяревевшаяособенногорячосталаудалятьсядругаячастьстаипонесласьвдольполесумимографаиприэтойстаебылослышноулюлюканьеданилыобаэтигонасливалисьпереливалисьнообаудалялисьсеменвздохнулинагнулсячтобоправитьсворкувкото
ройзапуталсямолодойкобельграфтожевздохнулизаметиввсвоейрукетабакеркуоткрылееидосталщепотьназадкрикнулсеменнакобелякоторыйвыступилзаопушкуграфвздрогнулиуронилтабакеркунастасьяивановнаслезисталподниматьеграфисеменсмотрели
нанеговдругкакэточастобываетзвукгонамгновенноприблизилсякакбудтовотвотпереднимисамимибылилающиертысобакиулюлюканьеданилыграфоглянулсяинаправоувидалмитькукоторыйвыкатывавшимисяглазамисмотрелнаграфаиподнявшапкууказывал
емувпереднадругуюсторонуберегизакричалонтакимголосомчтовиднобылочтоэтословодавноужемучительнопросилосьунегонаружуипоскакалвыпустивсобакпонаправлениюкграфуграфисеменвыскакалиизопушкииналевоотсебяувидаливолкакоторыймягко
переваливаясьтихимскокомподскакиваллевееихктойсамойопушкеукоторойонистоялизлобныесобакивизгнулиисорвавшисьсосворпонеслиськволкумимоноглошадейволкприостановилбегнеловкокакбольнойжабойповернулсвоюлобастуюголовуксобакамит
акжемягкопереваливаясьпрыгнулраздругойимотнувполеномхвостомскрылсявопушкувтужеминутуизпротивоположнойопушкисревомпохожимнаплачрастерянновыскочилаоднадругаятретьягончаяивсястаяпонесласьпополюпотомусамомуместугдепролезп
робежалволквследзагончимирасступилиськустыорешникаипоказаласьбураяпочерневшаяотпотулошадьданилынадлиннойспинееекомочкомвалясьвпередсиделданилабезшапкисседымивстрепаннымиволосаминадкраснымпотнымлицомулюлюлюулюлюкрич
алонкогдаонувидалграфавглазахегосверкнуламолнияжкрикнулонгрозясьподнятымарапникомнаграфапроливолкатоохотникиикакбынеудостоиваясконфуженногоиспуганногографадальнейшимразговоромонсовсейзлобойприготовленнойнаграфаударилпов
валившимсямокрымбокамбурогомеринаипонессязагончимиграфкакнаказанныйстоялоглядываясьистараясьулыбкойвызватьвсеменесожалениексвоемуположениюносеменауженебылоонвобездпокустамзаскакивалволкаотзасекисдвухсторонтакжепереск
ивализверяборзятникиноволкпошелкустамииниодинохотникнеперехватилегониколайростовмеждутемстоялнасвоемместеожидаязверяпоприближениюиотдалениюгонапозвукамголосовизвестныхемусобакпоприближениюотдалениюивозвышениюголосовд
оезжачихончувствовалточтосовершалосьвостровеонзналчтовостровебылиприбылыемолодыеиматерыестарыеволкионзналчтогончиеразбилисьнадвестаичтогденибудьтравилиичточтонибудьслучилосьнеблагополучноеонвсякуюсекундунасвоюсторонужда
лзверяонделалтысячиразличныхпредположенийотомкакискакойстороныпобежитзверьикаконбудеттравитьегонадеждасменяласьотчаяниемнесколькоразонобращалсякбогусмольбоюотомчтобыволквышелнанегоонмолилсястемстрастнымисовестливымчув
ствомскоторыммолятсялюдивминутысильноговолнениязависящегоотничтожнойпричинынучтотебестоитговорилонбогусделатьэтодляменязнаючтотывеликичтогрехтебяпроситьобэтомнорадибогасделайчтобынаменявылезматерыйичтобыкарайнаглазахдя
дюшкикоторыйвоноттудасмотритвлепилсяемумертвойхваткойвгорлотысячуразвэтиполчасаупорнымнапряженнымибеспокойнымвзглядомокидывалростовопушкулесовсдвумяредкимидубаминадосиновымподседомиоврагсизмытымкраемишапкудядюшкич
утьвидневшегосяиззакустанаправонетнебудетэтогосчастьядумалростовачтобыстоилонебудетмневсегдаивкартахинавойненевовсемнесчастьеаустерлицидолоховярконобыстросменяясьмелькаливегововоображениитолькоодинразбывжизнизатравитьматерогово
лкабольшеянежелаюдумалоннапрягаяслухизрениеоглядываясьналевоиопятьнаправоиприслушиваяськмалейшимоттенкамзвуковгонаонвзглянулопятьнаправоиувидалчтопопустынномуполюнавстречукнемубежалочтотонетэтонеможетбытьподумалростовт
яжеловздыхаякаквздыхаетчеловекприсовершенииитогочтобылодолгоожидаемоимсовершилосьвеличайшеесчастьеитакпростобезшумабезблескабезознаменованияростовневерилсвоимглазамисомнениеэтопродолжалосьболеесекундыволкбежалвпередипере
прыгнултяжелорытвинукотораябыланаегодорогеэтобылстарыйзверьседоюспинойиснаеденнымкрасноватымбрюхомонбежалнеторопливоочевидноубежденныйчтониктоневидитегоростовнедышаоглянулсянасобаконилежалистоялиневидяволкаиничегонеп
онимаястарыйкарайзавернувголовуиоскаливжелтыезубысердитоотыскиваяблохущелкалиминазаднихляжкахулюлюлюшопотомоттопыриваягубыпроговорилростовсобакидрогнувжелезкамивскочилинастороживушикарайпочесалсвоюляжкуивсталнастор
оживушиислегкамотнулхвостомнакоторомвиселивойлокишерстипускатьнепускатьговорилсамсебениколайвтовремякакволкподвигалсякнемуотделяясьотлесавдругвсяфизиономияволкаизмениласьонвздрогнулувидавещевероятноникогданевиданныеимчел
овеческиеглазаустремленныенанегоислегкаповоротивкохотникуголовуостановилсяназадиливпередэвсравновпередвиднокакбудтосказалонсамсебеипустилсявпередуженеоглядываясьмягкимредкимвольнымнорешительнымскокомулюлюнесвоимголосомза
кричалниколайисамасобоюстремглавпонесласьегодобраялошадьподгоруперескакиваячерезводомоиныпоперечьволкуиещебыстреeобогнавеепонеслисьсобакиниколайнеслыхалсвоегокриканечувствовалтогочтоонскачетневидалнисобакниместапокотором
уонскачетонвиделтольковолкакоторыйусиливсвойбегскакалнепеременяянаправленияполощинепервяпоказаласьвблизизверячернопегаяширокозадаямилкаисталаприближатьсякзверюближеближевотонаприспелакнемуноволкчутьпокосилсянанееивместот
огочтобынаддатькаконаэтовсегдаделаламилкавдругподнявхвостсталаупиратьсянапередниеногиулюлюлюлюкричалниколайкрасныйлюбимвыскочилиззамилкистремительнобросилсянаволкаисхватилегозагачиляжкизаднихногновтужсекундуиспуганнопере
скочилнадругуюсторонуволкприселщелкнулзубамииопятьподнялсяипоскакалвпередпровожаемыйнааршинрасстояниявсемисобакаминеприближавшимисякнемууйдетнетэтоневозможнодумалниколайпродолжаякричатьохрипнувшимголосомкарайулюлюк
ричалонотыскиваяглазамистарогокобеляединственнуюсвоюнадеждукарайизвсехсвоихстарыхсилвытянувшисьсколькомогглядянаволкатяжелоскакалвсторонуотзверянаперерезему нопобыстротескокаволкаимедленностискокасобакибыловидночторасчетка
раябылошибоченниколайуженедалековпередисебявиделтотлесдокоторогодобежавволкуйдетнаверноевпередипоказалисьсобакииохотникскакавшийпочтинавстречуещебыланадежданезнакомыйниколаюмуругиймолодойдлинныйкобельчужойсворыстремит
ельноподлетелспередиkволкуипочтиопрокинулеговолкбыстрокакнельзябылоожидатьотнегоприподнялсяибросилсякмуругомукобелющелкнулзубамииокровавленныйсраспоротымбокомкобельпронзительнозавизжавткнулсяголовойвземлюкараюшкаотецп
лакалниколайстарыйкобельссвоимимотавшимисяналяжкахклокамиблагодаряпроисшедшейостановкепереpезываядорогуволкубылужевпятишагахотнегокакбудтопочувствовавопасностьволкпокосилсянакараяещедальшеспрятавполенохвостмеждуногинад
далскокунотутниколайвиделтолькочточтотосделалосьскараемонмгновенноочутилсянаволкеиснимвместеповалилсякубаремвводомоинукотораябылапереднимитаминутакогданиколайувидалвводомоинекопошащихсясволкомсобакизподкоторыхвиднеласьсе
даяшерстьволкаеговытянувшаясязадняяногаисприжатымиушамииспуганнаяизадыхающаясяголовакарайдержалнаташасбросилассебяплатоккоторыйбылнакинутнанейзабежалавпереддядюшкииподперширукивбокисделаладвижениеплечамиисталагдекакко
гдавсосалавсебяизтогорусскоговоздухакоторымонадышалаэтаграфинечкавоспитаннаяэмигранткойфранцуженкойэтотдухоткудавзялаонаэтиприемыкоторыедавнобыдолжныбыливытеснитьнодухиприемыэтибылитесамыенеподражаемыенеизучаемыерусс
киекоторыхиждалотнеедядюшкакактолькоонасталаулыбнуласьторжественногордоихитровеселопервыйстрахкоторыйохватилбылониколаяивсехприсутствующихстрахчтоонанетосделаетпрошелиониужелюбовалисьеюонасделалатосамоеитакточнотакпо
лноточноэтосделалачтоанисьяфедоровнакотораятотчасподалаейнеобходимыйдляееделаплатоксквозьсмехпрослезиласьглядянаэтутоненькуюграциознуютакуючужуюейвшелкуивбархатевоспитаннуюграфинюкотораяумелапонятьвсточтобылоиванисьеиво
тцеанисьиивтеткеивматериивовсякомрусскомчеловекенуграфинечкачистоеделомаршрадостносмеясьсказалдядюшкаокончивпляскуайдаплемянницавоттолькобымуженькатебемолодцавыбратьчистоеделомаршужвыбрансказалулыбаясьниколайосказалуди
вленнодядюшкаглядявопросительнонанаташунаташассчастливойулыбкойутвердительнокивнулаголовойещекакойсказалаонанокактолькоонасказалаэтодругойновыйстроймыслейичувствподнялсявнейчтозначилаулыбканиколаякогдаонсказалужвыбранрад
онэтомуилинерадонкакбудтодумаетчтомойболконскийнеодобрилбынепонялбыэтойнашейрадостинетонбывсепонялгдеонтеперьподумаланаташаилицоеевдругсталосерьезноноэтопродолжалосьтолькоодинусекундунедуматьнесметьдуматьобэтомсказалаонасе
беиулыбаясьподселаопятькдядюшкепросяегосыгратьещечтонибудьдядюшкасыгралещепеснюивальспотомпомолчавпрокашлялсяизапелсвоюлюбимуюохотническуюпеснюкаксовечерапорошавыпадалахорошадядюшкапелтаккакпоетнародстемполнымиинаи
внымубеждениемчтовпеснеевсезначениезаключаетсятольковсловахчтонапевсамсобойприходитичтоотдельногонапеванебываетачтонапевтактолькодляскладуотэтогоэтотбессознательныйнапевкакбываетнапевптицыудядюшкибылнеобыкновеннохорошн
аташабылаввосторгеотпениядядюшкионарешилачтонебудетбольшеучитьсянаарфеабудетигратьтольконагитареонапопросилаудядюшкигитаруитотчасжеподобралааккордыкпесневдесятомчасузанаташейипетейприехалилинейкадрожкиитроеверховыхпосл
анныхотыскиватьихграфиграфинянезналигдеониикрепкобеспокоилиськаксказалпосланныйпетюсснеслииположиликакмертвоетеловлинейкунаташасниколаемселивдрожкидядюшкаукутывалнаташуипрощалсяснейссовершенноновойнежностьюонпешкомп
роводилихдомостакоторыйнадобылообехатьвбродивелелсфонарямиехатьвпередохотникампрощайплемянницадорогаякрикнулизтемнотыегоголоснетоткоторыйзналпрежденаташаатоткоторыйпелкаксовечерапорошавдеревнекоторуюпроезжалибыликрас
ныеогонькиивеселопахлодымомчтозапрелестьэтотдядюшкасказаланаташакогдаонивыехалинабольшуюдорогудасказалниколайтебенехолоднонетмнеотличноотличномнетакхорошоснедоумениемдажесказаланаташаонидолгомолчалиночьбылатемнаяисырая
лошадиневидныбылитолькослышнобылокаконишлепалипоневиднойгрязичтоделалосьвэтойдетскойвосприимчивойдушетакжадноловившейиусвоившейвсеразнообразнейшиевпечатленияжизникакэтовсеукладывалосьвнейноонабылаоченьсчастливаужепо
дезжаякдомуонавдругзапеламотивпесникаксовечерапорошамотивкоторыйоналовилавсюдорогуинаконецпоймалапоймаласказалниколайтыобчемдумалтеперьниколенькаспросиланаташаонилюбилиэтоспрашиватьдругдругаясказалниколайвспоминаявотви
дишьлисначалаядумалчторугайкрасныйкобельпохожнадядюшкуичтоежелибыонбылчеловектоондядюшкувсебыещедержалусебяежелинезаскачкутакзаладывсебыдержалкаконладендядюшканеправдалинуатыяпостойпостойдаядумаласначалачтовотмыедемид
умаемчтомыедемдомойамыбогзнаеткудаедемвэтойтемнотеивдругприедемиувидимчтомыневотрадномавволшебномцарствеапотомещедумаланетничегобольшезнаювернопронегодумаласказалниколайулыбаяськазалосьнаташапозвукуегоголосанетотвечал
анаташахотядействительноонавместестемдумалаипрокнязяандреяипротокакбыемупонравилсядядюшкааещевсповторяявсюдорогуповторяюкаканисьюшкахорошовыступалахорошосказаланаташаиниколайуслыхалеезвонкийбеспричинныйсчастливыйсме
хзнаешьвдругсказалаонаязнаючтоникогдауженебудутаксчастливаспокойнакактеперьвотвздорглупостивраньесказалниколайиподумалчтозапрелестьэтамоянаташатакогодругогодругаменянетинебудетзачемейвыходитьзамужвсебыснейездилиэкаяпрелест
ьэтотниколайдумаланаташааещеогоньвгостинойсказалаонаказываянаокнадомакрасивоблестевшиевмокройбархатнойтемнотеночиграфильяандреичвышелизпредводителейпотомучтоэтадолжностьбыласопряженаслишкомбольшимирасходаминоделаегов
снепоправлялисьчастонаташаиниколайвиделитайныебеспокойныепереговорыродителейислышалитолкиопродажебогатогородовогоростовскогодомаиподмосковнойбезпредводительстваненужнобылоиметьтакогобольшогоприемаиотрадненскаяжизньвелас
ьтишечемвпрежниегодыноогромныйдомифлигелявсетакибылиполнынародомзастолвсетакжесадилосьбольшечеловеквсеэтобылисвоиобжившиесявдомелюдипочтичленысемействаилитакиекоторыеказалосьнеобходимодолжныбылижитьвдомеграфатаковыбы
лидиммлермузыкантсженойиогельтанцовальныйучительссемействомстарушкабарышнябеловажившаявдомеищемногиедругиеучителяпетибывшаягувернанткабарышеньипростолюдикоторымлучшеиливыгоднеебыложитьуграфачемдоманебылотакогобол
ьшогоприездакакпрежденоходжизнивелсятотжебезкоторогонемоглиграфсграфинейпредставитьсебежизнитажебылаещеувеличеннаяниколаемохотатежелошадейикучеровнаконюшнетежедорогиеподаркивименинныиторжественныенавесьуездобедытежегр
афскиевистыибостонызакоторымионраспускаявсемнавидкартыдавалсебякаждыйденьнасотниобыгрыватьсоседямсмотревшимнаправосоставлятьпартиюграфаильиандреичакакнасамуювыгоднуюарендуграфкаквогромныхтенетахходилвсвоихделахстараясь
неверитьтомучтоонзапуталсяискаждымшагомвсеболееиболеезапутываясьичувствуясебяневсилахниразорватьсетиопутавшиеегониосторожнотерпеливопринятьсяраспутыватьихграфинялюбящимсердцемчувствовалачтодетиееразоряютсячтографневиноват
чтооннеможетбытьнетакимкакимонестьчтоонсамстрадаетхотяискрываетэтоотсознаниясвоегоидетскогоразоренияиискаласредствпомочьделусееженскойточкизренияпредставлялосьтолькоодносредствоженитьбаниколаянабогатойневестеоначувствовалач
тоэтобылапоследняянадеждаичтоеслиниколайоткажетсяотпартиикоторуюонанашлаемунадобудетнавсегдапроститьсясвозможностьюпоправитьделапартияэтабылажюликарагинадочьпрекрасныхдобродетельныхматериотцасдетстваизвестнаяростовымимит
еперьбогатаяневестапослучаюсмертипоследнегоизеебратьевграфиняписалапрямоккарагинойвмосквупредлагаяейбракеедочерисвоимсыномиполучилаотнееблагоприятныйответкарагинаотвечалачтоонасосвоейсторонысогласначтовсебудетзависетьотсклонн
остиеедочерикарагинаприглашаланиколаяприехатьвмосквунесколькоразсослезаминаглазахграфиняговориласынучтотеперькогдаобедочериеепристроеныееединственноежеланиесостоитвтомчтобывидетьегоженатымонаговорилачтолеглабывгробспокойно
йежелибыэтобылопотомговорилачтоунееестьпрекраснаядевушканапримететеивыпытывалаегомнениеоженитьбевдругихразговорахонахвалилажюлиисоветоваланиколаюсездитьвмосквунапраздникиповеселитьсяниколайдогадывалсякчемуклонилисьразгово
рыегоматериводинизтакихразговоровонавызвалаеенаполнуюоткровенностьонавысказалаемучтовсянадеждапоправленияделоснованатеперьнаегоженитьбенакарагинойчтожеслибыялюбилдевушкубезсостояниянеужеливыпотребовалибычтобыяпожертвовалчу
вствомичестьюдлясостоянияспросилонуматеринепониманиежестокостисвоеговопросаинежелаяпоказатьсвоеблагородствонотыменянепонялсказаламатьнезнаякакоправдатьсятыменянепонялниколенькаяжелаютвоегосчастьяприбавилаонаипочувствова
лачтоонаговоритнеправдучтоонапуталасьоназаплакаламаменянеплачьтеатолькоскажитемнечтовыэтогохотитеивызнаетечтоявсюжизньсвоюотдамдлятогочтобывыбылиспокойныисказалниколайявсемпожертвуюдлявасдажесвоимчувствомнографиня
етакхотелапоставитьвопросонанехотелажертвыотсвоегосынаонасамабыхотелажертвоватьемунеттыменянепонялнебудемговоритьсказалаонаутираяслезыдаможетбытьялюбилбеднуюдевушкусказалсамсебениколайчтожмнепожертвоватьчувствомичест
[illegible]

Висновки

В ході лабораторної роботи я набув навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанув прийомами роботи в модулярній арифметиці.

Мною було обрано декілька найчастіших біграм шифротексту та декілька найчастіших біграм російської мови. Вибравши пару з кожної множини, я утворював модулярні рівності, розв'язком яких був теоретичний ключ.

Змістовність тексту перевірялась за допомогою індекса відповідності російского тексту, що показало дуже точний результат.