

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ
ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. І. СІКОРСЬКОГО»

Комп'ютерний практикум №3
Криптоаналіз афінної біграмної підстановки

Виконав:
Студент групи ФБ-83
Сердюк Олександр
Перевірив:
Чорний О.М.

Київ
2020

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 елемента 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.

Варіант 19

Хід роботи:

Під час виконання роботи виникали труднощі із відсіюванням зайвих розшифрованих текстів, з пошуком та збереженням п'яти найчастіших біграм шифртексту.

Результати виконання роботи представлені у протоколі у вигляді таблиць, ВТ, ШТ.

Найчастіші біграми шифртексту: (уф, иж, ьи, хф, щф).

Для розпізнавання осмисленого тексту використовувався критерій неможливих біграм та найчастіших біграм. Якщо частота неможливих біграм (аь, еь, иь, йь, уь, ьь, ьь, эь, юь, яь, ьы) більша за 0.002, текст відкидається. Якщо частота найчастіших біграм російської мови (ст, но, то, на, ен) менша за 0.002, текст відкидається.

В результаті роботи програми було відкинуто 49 з 50 кандидатів на ключ (a, b) та відповідних розшифрованих текстів, лише 1 пройшов перевірку і виявився дійсно осмисленим.

UIT:

цияеоздшвезбккылмдлмзхикопангкутеншкарфцвкдизайцзгбгннфтзкызкуфэбкррфуфьмюиолршппйщфатфзэьхмк
 йзбшпбсываагвежпыхфбплмгнлтггнацбхнфмцязожтнийценшкчфчыщмтгэмкижвельийзфбшаишжяирихешайценшкшцжрфуф
 ьфдлгфгшфнфккмккиоуьлчфднийюзийушпирзыашппдныийзичцюобахшшуьпаибшбашпяигфкэзышфжфийаеиомлнеыаутпшрфтзкы
 зкхфиуьбэщхфижаиржыртащыюнищзгяеттиегизкексжскэятчзеичгуфаилбвैयाбшплммтпжиувайцдйфспьуджпбгньиыщи
 гшмпщещезоимлофйзфгблттиегияцшюезшвмежркппзгльзшущжпмкртгжтнсыафьупдзуюдыдизневеттншбхзврг
 фгэьхэфекршщфбфбйюфшфоселзппызыщбсегуавгивежхфжислзбэьуфхштфкнсыхфгтгшщфшцташмьгнмбарбккعاتнпх
 яуванксбккеншкинщюфлзизэфийнфбнясхфижжышыйжцагнжифохтгтрэьжфчзчшгнсыйибкбшклкофмтижтнкирнтгтоуенипыщне
 уффпашуфапздужунылфегшвзшфкмкшошенифюйшлскшфэфоньбккчьгушпрфюшрфшфашязщзещнфзыгэереегзызщфнфьфгдуфки
 жфэфокуфэсамкшошенкшьяьбвенедеекпевтдзуиодыищнбвгдышцмбьфцкьешфзфизждьхйняешфяжубздзуфяийтйзкдзрф
 уфьфшфшияюездшвмигшфьешриыцкызыкзкэьхэфшшыщцфьуьлжбужнштсмвкржскаыщкшшуьлбккйжхфбфгкзгсыпкж
 гньщмецжйзяссккаршсэщцйшмьфсийцнфмищюэиапшияюцздшвечккийзмуьпдзерфуфьфсавелькшнфбфхкхийгжйзшйзже
 екигтжтнийеанскаршппуазешылщйгврлмайсаыанршщпжееклбгнхтдужунылоищцнфюнвыигтжтмлкизсехеичгошхжвещ
 вышияюездшвдешфиещппфййагвежпыхпхплмгнжкбасылчбожаскпюдзекуйзвмбатпашфцятцжшкэзийишкиженмюпйщфиж
 уашяжшшудфзейфяибкпыхфлбкийжехфнфянкцжсызшцфнеекмэзэхцфнеиуфлплмгнпфшкмпйьевеесоионопытчньэи
 цнфькияслтабкпхфеижзкушнфймбайеюишмвфихвзуфжусснеекмдуфмайеюисынедеекшешфэуиодххзгхймхтбфрфгхяпы
 хфиуятчзюикежпэигтфгкиэкнепуфызищьетпшчрфвблршмдуфхщйюуаашшжгжуфшфязрфтамдяоинэитфокфзюикеаивышмйэ
 яеьххйянбшэкнеюитгышшщижэкрилбккйжкпвдуфхщйюуаашшжгжуфшфязакчаенабшужйьхшбшкпршьяуфшфтжиуытрщекхйоеие
 ржжгофяпбшекгабьфзгчньэицнщюфяйдтршияцнфзыоэфжеееквыоюдзрфсцтадыашцвзйзешзаскшибжазйзжгншбйзепи
 щьеншкшцмкфкэзыжящдэщтабауанкчасыцавакпюпршшурщдеятэщеофчгктфэфжееекжшкпрфишыесешфатфзэьхыазк
 ййеешеншоуьпенлонедэдзднйецнкышдзшфхклзийффоиодмпяцтасыпгльзшущжпмкббршдзайийнфуплмйгккицьюф
 оиодмпяцтасыуфкызышбальмкшошениолршппйьнрбгнфмтзкыкфэенгодьцатиймлзхивгсызятэийбмачгчлюишхуапкшяз
 цшхфтжшмкшошениуошужрфчзшбхажжышзшхфуйайрфтжшмкшошениуошужанжкызкбнсыужшмьбккшфатфзвемкишкишуьур
 взпспуахфрфчзшкосешфьуьпяжыузыхейзуфгшрфьмлзхийцапаенткфхянаивыьхеиодмпяичгыхейзуфгшрфшфяжыульмигн
 мпаентгккышцижгншияюащпрфюшакьмигнмпуямкбейгшэжнхххкжпсыхжсдьшакмдаибасеакоюшпирйерфмкшеижнфаикц
 днэимехикишуьурвзпзеншкчгфреуфшфиещшщцпикшгкянкомкшошениолршппашцэзйздкшеууванггайоикшкшекижсмйзту
 ьиомеобыдаишцвзмряцюобезейзэмакпчгяцшияюччьценсасдрфюшвзцаиэзепбасдкнеутлычсаязцдемрьемнхьярц
 янищзгяцшкшекижйзкысейчрфеошакьмигнмпячпнмлзхикцзфижуашжкпблздзавзбэизкбзейзлзровзцжэзщпщдашенк
 уошакмалршунфнфйебфескшшмяецнмешфхьржппшчдкдзшфхкмкийекайеюимлжысхфшицияцнжыкыкхфожайевогфэфже
 еклкремепшщкыквизбгштзтпикцззаяйекакфжэсесуахфрфчзшкосцмкийодзаязэиешфешешфабйзпкыужпашцаужзе
 фжскмкцнцмйеиеквщйиппцакпчгяцшияюжкмкенфгшесаппчгчньнфэгкизгяцаийюдзэфьешфкмккузппчфкмкшошенкижтг
 ьефжфгйеуфянчглюзияеюятнрезффевазясхфппаияиясхфашофейийжоешфхфржиуьпуазежикьиужибаязатсеижефеюикже
 цылщцбккатыштащышфатфзэьцаоселвгкрпшчабккеатнхфежыдакуаянашбжижэкомкшошензаоенелзэийьянжшнфгитыцаоепу
 ьпршыикыхешдэятэяцшфатфзэьеянаизымпдзоегькаэищспуахфрфчзшкосешфхфйзабгнзсмпйьхщыжзкышышкзохквг
 утнзряеймиуьпяешфойфтитгжйзйзкдшеууьпфегикцашофеишжкпэузоишжжкпбтнцшязшжкпллийзекьейшфатфзэьиееквщ
 ьиьххбсыыгчэкдэюшрфмжугнекчгтжнкязцоушунелзэгйзшцхйьхфжиюуьпшфьнкьмигнмпофдеуикцпошрбауждкюп
 йишмыдуфхьзуюжешфхшмфззшфуфедцэиышфенищпфемакдагчбнйьхюжбофувтгжвфуьхьфвышцфоиуванкуыанащ
 дняжщыуьпмтгбгжышдуфкыххбшппийоениршбжаудкофувтгжсквбнжхитнмптгзэдшшцшлщгчшппиймшцдпхтгодьшгтаз
 кыуейамуьпгпйцэдэзкижекшинбшптфдзоьмигнмпягнпыхгаоеиетжскреэфхщиймфзепщькекигздешцэицнбнтхтбкхюж
 бжофувтгжвфуьпщыкпиндршжкпьюномдюлбесейзлзровзцжйуьпшжбжофувтгжвфекфешшшуьпомнешфатфзэьаифгкиучсп
 уахфлбетайьхюжбжофувтгжвфюшкцшвзэжблзфайцпхянгжадзофдекидкшжижуацамптгзэшйзоффекакхйочкпышвфенлюхф
 ижйвуфшфжпэиенагбаршппхщынеэфийацпхярбетдехыашпччшмьихевефзызряцгхярбетьяуушщещежфижшбхффятнреше
 сшдыяячпзийоакмщдытфевеюикцжфянийювеекигбаоевтязркэеиикцетнужчгбнсыевгкбскрехфызюимлмкхнишгблзкхф
 ижйзюимлпфзфнеиюикцкаикшцднэиментгжтнекпшэффижбжаыйцифеюийцзоианейжкпьякшчкнбшкдйшсйцнбшгтусахтш
 ьипбейоимлмпаибакэебжшзипхыльшмкьхэфыышфшжкмадуффижялбнбжбиолршщпанкбббккенсрбгбжышдуфмтшуьлзк
 сбккцчрбмпвабкяпсаоеиылщдеукшфэфзфмаржшышмьфсисыиеабвгйцхпудеижсэьвомтнжфшыинтгчньйэицнщцэкнеешдэят
 еяебфдегнийоаклбршйзшшкпыищдзянуадеекукэзыжяцхешащэзыжщьхьлзьячпжкйьмбкшдешфызьемкьетнужчгцайцпхфе
 эьцксауфтгжейеиянтязнфмитгтжбаржйцдзагшеижащнфаивкьыипхйюфгкищюфгкигфшпсдьшрфшфеацсьищыиушфшжзбэт
 ййрбкшдешфызьемкймгжвбфызмгжжжшбдеекзаспжущднэигфышмтжпьищюфуфшитышзрфдзвбैयाшзипхшыекйфештфкк
 щцнфмиткнфхшгисыгжижшбдеекчфжвуфештфккцажшкпшжшпцбасенызгштатиктфенлюбазихфижжкмгпкидыгныхфижжржйц
 эзыжкьянаигшдензмкэереегеянаияхнфийсфбфеаифкмгнршвкцнцмяеянквтсеижефеюикивыяхожтнщэзыжщьхьлзьянгж
 цашбшбсдбзбгнцдфггаоеишыуаьембкрршфдгйзмиакцкьхмкянаияшжкпжшутшфдгйзмиакцкзохкржйзэыжкьхмк
 ьеруфшфхщещеппаджвобейшмкзжшбдеекзайцпшцташфбагтжжжшблбгнбшзбфизуадеюимлпэибабнсыужшмыдуфян
 бшижуашжкпквуфэбнгкюуьпрбөөсвзэкьемкцыкпмлнемшцаяцкицареижшьешьхмкянбшижуашжкпцаихччфдзйыхфижца
 япбшижэкмдймкшвзхфкмкййэйтфоикшуфьфюищехщюфвержоуьпинищзгяепзкнхжчфюиодауангашпохзмхзийгньгйфэфэкцн
 цмясаву

Розшифрований текст:

князь андрей причал в главную квартиру армий в конце июня войска первой ая и той при ко той оу находил гм государь оу лирасполож тн в укреп тн нм лагере у дри ссвой ска в той армий о еступали стре оу ссы соединит ь с первой армий от ко той оу как говорили они били отрезан ь больш ья сила оу францу зов все били недовольн ь общ ья хом военн ьх де оу русско й ая ии но оу бп асности аи штств в м русские губе рнии ни кто и не думали ни кто и не предполаг ал что б оу в иа мог ли б ьт ь пер тнт стна далее западн ьх польских губерний князь андрей нашел бау кла дето олли кто рэ а оу били на знач тн на бере гу дри сс так как не оу били одного больш о го села и л ьт ас чка во крестностях лагем тов се оу рэ а но еколич тствог тн ералов и при дворн ьх б ьвших при армий асполаг алось во кружности дт ь аи верст получ шья дом аи дерев тн ь по сию по ту сторону реки барк л ьт де то лли ст а в четь рч х верстах от государя он су х о и холо дн ь при ам л бол конско го ии ска зал сво я не мецк ья в ь го во ю о мч то он долож ит нем государю д ь м пред еления ему знач тн мапо к аи ст ь пою с аи е го с аи ст ь биль при го штн бе аи т ь эм кура гна ко то ю о м князь андрей нашел сн ьт и т ь ая ии не оу били т о зды оу били в пете рбу рге и т о з в ст ь биль при тн бол конск ья ии т ер тс центра по то ю о м з аи о д ь и гмо го ной войн ь заня л князь андрей ии оу рад били на не ко то ю оу е р е ю о м с во бодит ь мот раздражения ко то р оу произво дили не ь с ь л оу к

пагивнепродолжениипервхчетрхднейвойрукаякторьхоннеоынкниудатребуюякнязандрейобездилсьесукуплетнннлагериспязо
 циюсвоихзнанийразговорссведущимилюдымистаралгмсоставитысебеонопределтноопяниеновопрестявьгоденилиневы
 оденэтотлагерьюсталгмнерешеннкядлякямшмандрцмонужеуспелъвестиизсвоеговоенногоопытаоубеждениечтоввоеннэяделенич
 онезначатсамьеглубокомьстгнообдуманньспланькакониделэтофаусаерлицкомпоходечтовсезависитоттогоокакотвсчаюснаножида
 нньениуаюгушиеобтыпредвиденнкидействиянеприятелячтовсезависитоттогоокакикемведетгмвсделодэмтогочтобоуяснитысебезот
 последньвопшюокмзыандрейпользуясисвоояположениуязнакомствояистаралсьвникнутывхарактеруправлтннжмариесилицапгт
 иуачствывашихонзьяивведлясебследующеположениуоположенийделкогдтегшюударьобывилыенармийбларазделенанатроя
 аяцннаходиласьподначальствэбаюкладеголияподначальствомбагратионсмподначальствэаюсаговосударынаходилгмприп
 ервойааяииноневкачтствглавнокэяандующеговприказтнебйлосказаночтогосударьбудеткомандоватысказанотолькочтогосударьбу
 детприяаяикрэяетогъпригосудареличннебйлштабглавнокомандующегонбйлштнбцяператорскоцглавнойквартирьпринуаюбнача
 лыникияператорскогоштнбгтнералквартиряейстеркнзываетолонскицгтнеральфлигелыадютантъдиплэятитчскечиновникиибольш
 оеколичествоиностранцевнонебйлштабаармийкоуметогобездолжностипригосудартнаходилисыаракчеевбвшийвоенныйминистргр
 афбтнсенпчиншустаршийизгенераловвеликийкнязьитсаревичконстантинпавловичграфрумонцевканцлершасейноыйшпрусскийи
 инстриаяфельдшведскицгтнералфульгланыйсоставительпланакампанийгенераладютантаулучисардинскийвхощеицполюсгени
 многиедругиеходмэтилицаинаходилисьбезвоенныхдожностейприяаяиинопосвоемуположениумеливщмниенчаствовкорпусныйна
 чальникидажеглавнокомандующийнезнаювачтствечегоспрашифаетилисоветуеттоилидругоебенигстнивеликийкнязьилиаракчее
 виликямзыволконскийинезналоаеголилицаилиотгосударяистектетакоотприказаниевформесоветанужноилинтнужноисполнятьег
 оноэтотбйлавнешнрмобстановкасущественныйжеаяслприсутствгмгосудавмивсехэтихлицспридворнойтбчкиавприсутствиигосударя
 вседелаютгмпридворнкяивсембйластноньлследующийгосударынепринцялнасетмзванщгглавнокомандующегонораспоряжалгмвс
 уаяящамиллюдиокружавшиеегоблинегопопомощникаракчеебйлверныйисполнительпоярдактелохраниаельгосудавм
 бенигстнбйлэцкицкивленскогуберникокторьхосемелостысвойственнойлюбомвделятисредичьюофредакждидтнхпред
 оьцяетеговсегданаготовенааятнубарклсмвеликийкнязьюльтупотомучтоэтобюлауяуюднбвщичияинистрштейабйлтупотэяучтоо
 ньбползтндлясоветаипотомучтоимператоралександрвьсокоцтнилеголичньекачтстваяаяфельдбйлзлойненавистникнаполеонаигтне
 ралувертннйвсечтоимеловсегдавлщмнитнаалександрапулучиоблтупотомучтооабйлаелирешителтнвречахгенераладютантъбйл
 итупотомучтоонивездебйлгдегосударынаконецглавноепфульюблтупотомучтоонсоставилпланвойньпротивнаполеонаизаставива
 лександраповеритывцелтсообразностыэтогопланауководилвсуаделомвойньприпфулеобьювольтогтнпередававшиймьслипфуэмвбо
 леедоступнойформечемсояпфулрезкийсоаяуверенныйдопрезняковсемукабинейньаесоретиккрэяетихпоименофанныхлцпрусски
 хииностранныхособенностииностранцевкогорьсеселостысвойственнойлюбомвделятисредичьюофредакждидтнхпред
 лагалиновьенежданньюаьслиоблощуняноголицвтоуюостептннхнаходившихсяприармийпотэяучтотутбйлиихпринципальвчслевсе
 дяьслейгилосовэтэяогюмнэбеспокойномблестящуиягордоыяирекямзыандрейвиделследующиеболеерезкиеподразделтнщмнапра
 вленийипагтийпервсмпатгщмоьлапфульиегъпоследофаелиаесоретиквойньневмщиевточтоестынаукавойньичтовтойнаукеестысво
 инегятнньезаконьзаконьоблицтскогодвижтнщмоьходаитпфульипоследофаелиеготребофалиотступлениявглубыстраньоеступлтн
 щмпоточнкязаконампредписанныянимитеориейвойньивовсякэютступлениотэтойтеориивиделитольковарфарствонеобразованн
 остыилизюлаоертнствыкэтойпагтийпринаджеленемецкиепринцьвольтогенвинцингеродиндругиепреимуществовннуащявторе
 мпагтщмоьлаптитуположнаяпервойкапвсегднбветтприоднойкрайностюбйлпредставителидругойкрайностилидэтойпагтийоьл
 аекоторьесещесвилынтребофалинаступлениявпольшуйсвободьотвсякихвпередсоставленньхплановкрэяетогчтопредставителиэто
 йпартиибйлпредставиаелиаяельдействийонивместтсаемиоьлипредставительнаинационалыностивследствиечегостановилисьчшеод
 ностююоннеевспорэтибйлирусскиебагратионначинавшийвозвзышатыгмермоловиругиеэтовруаябйлараспространтнаизвтсенсшут
 ктеаяоловнбудтооьпросившегогосудавмободночялостипроизводстафеговнемщйлюдиэтойпартииговориливспэянисмсувоюофачтон
 адонедвяатынтнакальватыиголкоякартуадратыгмбитынепрщмаеэмневпускатыеговооссиюнедаватыньфатывойскуктретьейпагт
 никоторойблеевсегоцелдверюагосударьпринаджелажелкапвдворньделателисделошяеждубоимонаправлениянлюдиэтойпартии
 большейчастьюневогтннбейкотооройпринаджелажелкапвдвалигговориличтоговорятоькновенолиадинеимеющиеубежденийно
 желающиеказатысязатаковхониговориличтобезэяненияияюособотнствакцягениуаккбонапареегообмтыназьфалибонапагтетре
 буетглубокэясленнейшихсоображтнийглубокогознаниянаукиивэтэяделепфульгтнналенновместтсаемнелэянепризнатыгбчтоаео
 ретикичастоодносторонниипотэяунтнадовполнедоверятымнадыприслушиватысяиктэяучтоговомтпюотивникипфуэмиктотомучтогов
 орятлюдипрактическиепьтньевотнномделениовсегозатысьсреднеелюдиэтойпагтийнастамлинамомчтооубдержфдрисскнхлагерып
 ыланупфуляигятннытывижениядругихаяийхходмэтэяобразомдействийнедостигаласынитанидругсмцелынолюхмяэтойпартииказало
 сытаклучшечтветгоенаправлениябйлонаправлнтнкетюоюгосамьвидньпредстависембйвеликийкнязьинаследниктсаревичне
 могшийзаотъсвоегоаустерлицкогоразбчарованщгмдеонканаяотврешалпредгвардиюокаскиколетерасщтисммолодецкиразд
 авитыфранцузовипопавнеожиданновпервуюлиниюнасилушесуеовбсхюмаенилюдиэтойпартиииеливсвоихсуждтнщмхикачств
 оинедостатокискренностионибамлисынаполеонавиделивнемсилувсебеслнбостыипвммовьсказывалиэтоониговорилиничегооюмог
 вмсрояипогибелиизвсегоэтогоневъйдетвобяоставиливильнуоставиливитебскоставимидриссуодночтонояостагтмвяногосделатэ
 тозаклочитйярикакможноскорепоканевгналинасизпетербургавозщртниеэтосилынораспространтннееввсшихсферахармиинаход
 илосебеподдержкуивпеарбургеивканцлерурумонцевподругимгосударственикяпричиноястамвшятожезамирптяеоблипривержен
 цбарклсмдетолнтстельныокачеловекасколькокаковоенногэянистраиглавнокомандующегоониговорикакойоннитысвсгдатак
 начиналионотчсеньдильныйчеловекилучшеегондатгеемунастмщувластьпотэячтогойнанужетидтигтиспешнобезидинстафана
 чальствофанияионпокажеттбчтоономожесделатыаконпоказалстмвфинэмдниежелаяящмнашустроенаисилынаиотступиладодр
 иссьнепонтсшникакихпоражтнийтомьобязаньэтимтолькобарклаюежелитеперызотянтбаюклаябтннгсеномтовсепогибетпотомучт
 обтнгсенужепоказалсвоонтспособностывгдогговорилилюдиэтойпартиишттьсбтнгсенистьговорилинапоотивтчовсетакинебйлон
 икогodelынееиопънеебенигстнаиканнивертисывсеатакипридешкнужуилилюдиэтойпагтиидоказьфалитчовсенашеотступлениедодрисс
 ьбйлпостьднейшеепоражтниеибтспервьнрядошибокчембольштнаделаютшибокговорилюнаеяемлучшепокртнйнеяертскорепо
 ймучтотакнуажетидтианужтнскеакойнибдыбарклтйачеловеккабтнгсенокторьпоказалужесетмрягодуюктоюомуталсправедл
 ивтысыаналеонотенитакочеловекзакотряхьохотнпопрнзаваливастыгатакойсттытолькоодинбенигстсдьмбейлилицакоторь
 евсгдатыособенностипряолодъхгосудавмхикотрьхособеннэягооьлоприимператореалександрелицагтнераловифлигелыадют
 антовстрасеньпреданньегосударюнекакимператорунокакчеловекаобожающиеегоискртннотбткорьстнокакегообожалоостоврягоду
 ивидящиевнуанетольковседобюодоаелиноивсекачстфачеловеческиезтилицахотяивосхищалисыскрэнностыногосудавмотказьфавше
 гояютэяандофаниявойскояиноосуждалиэтуизлишнююоскуомностыжелалитолькоодингоинастанфалинамомчтоообожтемыгосуд
 арыоставивлишнеенедовериексенеобоявилоткръбтчтоонстановитгмвоглавейскаоставилбоприсебедтнбквартируглавнокоманду
 ющегосивезисмьгдтнужносепенкениаоретикамипрактияосияовелсвойскаоторьходнозодешовтбеловещегосостояниаво
 одушевлтнщмвсоясамбольшаяягруппалюдейкотораяпосвоюаюгрэяномуколичествоотносиласькдругимкащяшсостоялаизлюд

ейнежелавшихнимиранивойньнинаступаасельныхдвиженийниибоюониаельноголагевмнипридрисстнигдеоьтониоьлонибаюклаянигосударянипфуэмнибенигстнаножелающихтолькооодногосамогосущественногонаибольшихдэмсетмвьгодиудовольствийвтоймуенойводеперекрщивающихсяиперепутьфающихгминтригкоторьекишелиприглавнойкфагтирегосударяввесымамногэяможнбильуспетывтакомчтонеислиьяобьбйловдругоевруаяодиннежелсмтолькопоаевмтысвоеговьгодногьположтнмнньчтсоглашалсяспфулузавтраспноотивникэяегьпослезавтраутверждалчтонеяееникакогэяненияобизвтсенэяпредмеаотолыкодлятогбчтооьизбежатыотвествтннстииугодитыгосударюдругойжелающийприобрестивьгодьобращалнасетмвнцияниегосудавмгрэякокричатосояоеначтонаяекнулгосударынаканунтспориликричалсвоетеудавмсебявгрудывивзьфаянтсоглашающихгмнадуэльяиаемпоказьвсмчтоонготовобьжетьвторобщейпользетретийпростоыпрашивалсебежду двухсоветовивотсуествиевраговединовременноепособиезасволвернуюслужбузнаячтоаеперынекогднбудетотказатыуяучетвегтьйнечаянновсельпадалгмнаглазгосударроdmгчтнньйрнботойбмтьдэмтогочтобьдостигнутыдавножеланнойцелиобедаугосудавможтсточеннодоказьвалправотуилинеправотувновывьступившегомтннцмидэмэтогьприводилболеилицтнеисилиьянеисправедливьедоказаельстфавселюдиэтойпартииловилирубликртстьчиньивэтяловлтнннследилитолькозанавралтниемфлюгерацарскоячилоститотолыкбчтозамечаличтофлюгеюобратилгмводнустоюонукаквсеэотруеневоенаселениеаяииначиналодутьвтужтстоюонутакчтосударюаемтруднееоьлоповернутыегофдругуюсрединьпределенностиположенияприугоюожайшейсерьезнойопасностипридававшейвсеумособтннотревожньихаракаерсредиэтовихвминтригсамолубийстолкновенийразличньхвоззренийичувствприазноплутнностивсехэтихлицэтавосяйсмааябольшсмпагтщмлюдейнанятьхличнкьяинтертсояипридафалабольшуюзапутанностьиаяутностиобшуяуделукакойоьниподнцялгмвопросаужройэтихтрутнейнеоттубивещенадпрежнейасмойперелеталановуюиосвоимжужжаниуязгалушализатуюямлискренниеспорящиеголосанзвсчэтихпагтийвтосояоевруаякаккнязыандрейпричхалкаяиисобраласыещеднадеумтаяпартияначинавшаяподниматывсвойголосэтооьлапагтщмлюдейстарьхразвньхгосударственноопьеньхиумевшихнеразделрмниодногоизпротиворечащихмнтнийотвлечтннопаяотретынавсечтоделалосьприштабеглавнойкфагтирьиобдуматысредствфаквьходуизэтойнеопределтнностинерешительностизапутанностиислабостилюдиэтойпартииговорилиидумаличтовседурноепроисходитпреимущественноотприсутствгмгосудавмсвоеннкядворэяприяаяичтовармиюпертнтстнатеопределтннаяу словнаяколеблющсмгмшаткостыотношенийкоторсмудобнапридвореновреднафаяиичтогосударюнужноцарствоватыанеуправлятьвойскэячтоединствтнньихходизэтогьположтнцмтстыотездгосударясегодвоюоимизаяиичтоодньприсутствиегосудавмпарализуетбмтыдегмттьсячвойсканужньхдляобеспечтннцмеголичнойбезьпасностичтосамьйплохойнонезависцяьйглавнокомандующийбудетлучштсогололучшегосвязанногоприсутствиуяивластьюгосудавмвтосояоевруаякаккнязыандрейжилбезделапридриссешишковгосударствтнньйсекретарыоьвшийоднимизглавньхпредставителейэтойпагтиинаписалгосударюписьяокоторосогласилисьподписатыбалашевиаракчеевписьяэтомпольземсыданнкяуюотгосударяпозволениуярассуждатыобобщемходеделонпочтительноиподпредлогэянеобходимостидэмгосудавмвоодушевитыквойнтнародвстолицепредлагалгосударроставитывойскоодушевлтниегосударемнародаивоззфаниекнемудлязащитьоасечстфатосамотнасколкооьнпоюизвденооьлоличнкяприсутствиуягосудавмряосквеодушевлтнниенаюодакотоюоебйлоглавнойпричинойторжтствароссибилььпредставлтногогосударюипринятоимкакпредлогдэмоствавлтннцмармиа

Шуканий ключ - (725, 100).

5
(725, 100)
аь: 0
еь: 0.000321388
иь: 0.000160694
йь: 0
уь: 0
ыь: 0
ьь: 0.000160694
эь: 0
юь: 0
яь: 0.00128555
бы: 0.000160694
ст: 0.0321388
но: 0.025229
то: 0.033103
на: 0.0205689
ен: 0.0170336
THIS text is probably acceptable.

Відкинуті ключі (і через яку біграму):

1	(701, 81)	йь: 0.00433874
2	(260, 782)	еь: 0.0027318
3	(236, 763)	иь: 0.00353527
4	(208, 363)	еь: 0.00321388
6	(753, 500)	уь: 0.00305319
7	(685, 152)	йь: 0.00224972
8	(506, 66)	уь: 0.00241041
9	(276, 341)	ыь: 0.00369597
10	(455, 427)	иь: 0.00337458

11	(449, 604)	на: 0.000803471
12	(298, 918)	уь: 0.0056243
13	(512, 495)	ьы: 0.00385666
14	(663, 181)	йь: 0.00482083
15	(483, 688)	иь: 0.00449944
16	(94, 812)	йь: 0.00208902
17	(838, 812)	уь: 0.00257111
18	(478, 175)	иь: 0.00208902
19	(867, 51)	еь: 0.0027318
20	(123, 51)	еь: 0.00257111
21	(445, 256)	ьь: 0.00530291
22	(395, 225)	иь: 0.00401735
23	(209, 225)	ст: 0.000964165
24	(516, 237)	ен: 0.00128555
25	(566, 268)	еь: 0.00224972
26	(752, 268)	юь: 0.00337458
27	(923, 783)	уь: 0.00578499
28	(301, 628)	еь: 0.00369597
29	(332, 628)	еь: 0.0028925
30	(38, 316)	еь: 0.0028925
31	(660, 471)	еь: 0.00369597
32	(629, 471)	йь: 0.00208902
33	(744, 671)	ьы: 0.0027318
34	(682, 671)	ьь: 0.00369597
35	(682, 671)	ьь: 0.00369597
36	(217, 609)	то: 0.00160694
37	(279, 609)	йь: 0.00755263
38	(279, 609)	йь: 0.00755263
39	(662, 256)	уь: 0.00449944
40	(674, 225)	иь: 0.00417805
41	(488, 225)	иь: 0.00257111
42	(299, 299)	ьь: 0.00369597
43	(287, 330)	иь: 0.00208902
44	(473, 330)	йь: 0.00224972
45	(261, 237)	яь: 0.00257111
46	(588, 113)	еь: 0.00690985
47	(805, 113)	еь: 0.00337458
48	(700, 688)	но: 0.000482083
49	(373, 812)	ст: 0.000160694
50	(156, 812)	ст: 0.000321388

Висновки.

В ході роботи було досліджено розшифрування текстів афінної підстановки, знайдено кандидатів на ключі за допомогою частотного аналізу найчастіших біграм ВТ та ШТ, розшифровано тексти за відповідними ключами та відкинуто всі зайві тексти за допомогою розпізнавача осмисленого тексту. Знайдений текст був осмисленим.