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.

Mema poбomu: 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.

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, ыь, 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.

HIT:

шияюездшвеэбккылмпдмлзхикопаенгкутеншкцарфцчвкдизайцзгнбгннфтзкызкуфэбккрфуфьфмиюлршппйыцфатфзэйьхмк йзабщпбсьиваагвежпьихфбплмгнлтцнащбхнфмщязожтнйценшкчфыщмтэзмкижвельййзфбшаишжящрщхещайценшкщцгжрфуф ьфдгфгщфнфккмкиюуьпчфднйюэийушпирзыашппдыияйзцчцюбахшшуьпаибшбашпяигфкэзышфжфиайсюимлнеыаутпшрфтзкы зкхфиуьбэщхфижаижрьщтащьюнищзгяеттиегизкексжскэеятчзеичгуфаилбвеябщплммптжиувайцдзйфспьуджпбгньиьщьи гшмпщещээзоимлофяйзгблттиегияцшияюездшвемижркппзьглзцшужщпмкрггжтнсыафыуьпдзуиодьидзиеветтцнащбхвэрг фгэеьхэфекршхфщфбфяйюфщфоелзппзыьщьесгуавгвеижхфижсллзбеэьуфхщтфкнсыхфтгщпсдьщташмьигнмпбарбккеатнпх яуванксбккеншкинэщофлзизэфййнфбнясхфижжшьщйжцагнижофхтгрзыжфчзчшгнсаьипбкщлкофмтижтнкирнтгюуенипыцне уффпащуфапздужунылфегщвзшфкмкщошенифющйлскшфэфоиьбккчьгущпрфющрфщфащязщзещнфзыэереегзызхщфнфьфгдуфки жфэфокуфэеамкипошенкиняььбвенелеекпевтлзуиольишьнбвглыышмбьфикьенифэфижльхйяняенифэжьубэлзуфяьйтйэйклэрф уфьфифицияюездинвемигшфьещриыцгкызкызкэеьхэфициьцифыуьпжбужгнитсмвкржсккаьшгкицуьпьбккйжхфбфэгкизгсыпкиж гньщмецжйзянсккаршсэщийышмьфсийцнфмищюэиапшияюцздшвечккийзмуьпдзэерфуфьфсавелькщнфбфхкхййыгжйзщшйзже екигтжтнйеянсккаршппуаэешылшяйвгрнлмаисаянршшпжееклбгнзхтдужунылоищцнфюнвыигтжтнмлкиэеьхеичгошхжвещт вышияюездшведфиещшппфеййагвежпьипхыплмгнжкабсылэбожаскпюдзекукйзвмбатнбапщфеятщкшкзоийшкиженмпйьзфиж уашжящшутфэейфянбшкпьихфлбкийжяехфнфянкщгжсызхщфнеекмкэезхщфнеивуфлплмгнцфижмпйьэевеееюитыюпигчьньэи цнфькияслтабкпзхфеижзкущнфймбайеюишмвфихвзуфжусснеекмдуфмайеюисынедеекшещфэеуиодхжхзгхймхтбфрфгхяпьи яеьххйянбшэкнеюитыжшщцижэкрилбккйжкпвдуфхщйюуаащшжгжуфщфязакчеиабшужйьхщбшкпршяьуфщфтжиуытрщекхйоеие ржгжофяпбшекгаьбьфзгчьнйэицницофяйдтрицяцнфзыофэфжееквыоюдзрфсщтадыацвзйзещзаекшибжхаззйзсжгншбйзепьи шьеншкшимфкэзыжациидэштабауанкчакисыцавакпюпришуриидеятеэщеофчьгктфофэжеекжинкпрфишыесещфатфзэйьхыаэк яйэееншкоуьпенлюнедедздэднйецэкыщьдэшфхклэййофоиодмпящтасыпэьглэцшужщпмкббршдзаэяйижнфпулмйэгккицьоф оиодмпящтасыуфкыэщбалмкщошеняиюлршппйьянрбгннфтзкызкхфэенгодьщтаймлзхивгсыэиятеэймбаянчглюьишуьпкщяз щэхфтжшмкщошенэуошужрфчэдшбахжящязщэхфуфяйрфтжшмкщошенэуошужянжэкызкбнсыужшмьбккщфатфзвемкщикишуьпур взпэспуахфрфчэдшкосещфьуьпяжьузыхейзуфгщрфьмлэхийцпаенгкфхянаивыьхеиодмпяичгзыхейзуфгщрфщфяжьулмьигн мппаенгккышцижгншияюхащпрфющакьмьигнмпуямкбеяйгшэжэинххкжпсыхжсдьщакмдаибаекакюущпирйерфмкшеижнфаикщ днэимехикишуьпурвзпзеншкчгьфреуфщфиещшшпзикщгкяномкщошеньиюлршппащезйзкдщеууванкгайеюикцшкекижсмйзту ьиомоеобыдаиищвзмряцоюбезейзэфмакпчгяцшияюччьщенсасдрфющвзцжаиэзепбасдкнеяутльцчсаязцчдемрьемиьхяряц янищзгяцшкекижйзкыуеяйчрфеощакьмьигнмпяячпнмлзхикцзфижуашжкппблздзязвбэизкбеэейзлзровзцжэзчпшдащенхк ющакгамлршучнфяйефбеексишмяецицмяешфхьржппшчдкдзшфхкмкййиекайеюимлжфысхфижиццянжзкызкхфофжайевтофэфже еклкремкепщьеквказижвітнэтпикцдзазяйекакфэжеспуахфрфчэдшкошкмийюдзыаязшеижфешещфабйзнкызужппащбаужзе фжскмкцнцмйеиееквщьиппцакпчгяцшияюжкмкенфгшесаппчгчьнйнфэгкизгяцаийюдзэфьещфмкмкузппчфкмкщошенчкижтг ыефжфгйеуфянчглюэияеюятнрезффевзаиясхфппаиьиясхфащофеийжюещфхфржиуьпуаэежикьиуижэибаязатсеижфеюикцже цылщхбккатыщтащыщфатфзэьцаоелвгкрпшчабккеатнхфежыдакуаянащбжижэкомкщошензаоенелзэжйьянжшнфгитыцаоепу ьпрщьикиьхещдеятеэяцщфатфзэйэеянаизымпдзоегькаэищьспуахфрфчздшкосещфхфйзабтнзсмпйьхщвыжзкыщьшкзохквг утнзяряеймиуьпяещфофйфтичгжзйзкдщеууьпфегикцащофеишжкпэузоижшжкппбтнцшязшжкпллйзекьеяйщфатфзэьиееквщ ьиьххбсыыэчгэкдеющрфьмжугнекчггжтнкцязцуошуфнелзэгйзцзхшйэхфижюуьпшфьфнкьмьигнмпофдеуикцюпрщбауждкюп йжшмыдуфьхзыужюещфхщймфздзщфуффедзцыьижуенипцьфемкакдгчьнйьхюжбжофуфвттжфвуфьхэфвыштщфоииуванкуыаиащ дняжщцыуьпмтмбгжсыщдуфкиьххбщпйюьиюпрщбауждкофуфвттжсквбгнхжтнмптгхздшщалщвггчьиппймщпсдпхтгодьщтагз кыуеяймуылгпйцэедзэкижекшинбщптфдзомьигнмпяагньипхгаоеиетжскреэфхщймфзепщьекьигздешщэицннбнтхтбкьхюж бжофуфвттжвфыуьпцыкпиндршжкпьиюнмдюлбеэейзлзровзцжйуьпшжбжофуфвттжвфекфещшшуьпомнещфатфзэйаифгкиучсп уахфлбетяйьхюжбжофуфвттжвфющкщвзэкжблэфайцпхянгжцадзофдекидкщзижуацамптгхэдшйзоффеккхйочкпыщвфснлюхф ижйвуфщфжпэиенагбаршппхщвынеэфиайцпхянрбетдеьхыащпччшмьихевефзызяряцгхяпрбетяьуущпщежфижшбхффятнреше сщдыяячизнйюакмидыьтфевеюикцжфянйювеекигбаоевтязркэеыикцьетнужчгбнсыевгксбскрехфызюимлмкхнищзгблзкхф ижйзюимлнфзфиеюикщгкаикщднэименггжтнкепщреэфижбожайцижфеюийцзоиьианейжкпяикщгкчнбшсдясйцчнбшггусахтш ьипбвеюплимпаибакеэебсжшэипхвылщмкьхэфыэвыхфщфмкдауфьфижлбьипхбиюлршцанкбщббккеншкрбгжсыщдуфмтщуьпзк сбккцурбмпвабкяпсаосиылшдеукщфэфэфмаржсышмьфсисыисабвгйцхфпудеижсэвыомтнжфшыинтгчьнйэицниццэкнеешдеят еэяебфдегнйюаклбршйзщшкпьищьдзянуадеекукэзыжяцхещацьэзыжщььхлзяячпжкймьбкшдежфызьемкьетнужчгцайцпхфе эьшксауфтжйеижяинтязнфмитктжбаржйидзагшеижяшнфаивкьыьипхйюфгкишюфгкигфшпсдышрфшфеацсьишьиушффзшжзбет яйрбкицдежфызьемкймгжвебфызмкгжижшбдеекзаспжуящднэигфыщмтжпьищьофуфщитыщзрфдзвбвеябащэипхшыекйфежтфкк щинфмиткнфхщигсыгжижшбдеекчфжвуфежтфккцажшкпшжщпцгбаенызгщтакитфснлюбаэихфижжкмкгпкидыгньихфижцгржйц эзыжзкянаигшдензмкэереегяеянаияхнфяйефбефааифкммгнршвкцнцмяеянвквтсеижфеюикивыяхожтнцьэзыжщььхлзянгж пашбщпбсдзббгннфдгфгцаоеишьуваыембккршхфдгйзмикшгкьхмкянбшижуашжкпжшутщфдгйзмикщгкзохкржйцэзыжзкьхмк ьерфуффхщесежаппяиджвебфызмкдзижшбдеекзаофяйцтащнфбфахгжхщигблжбгнбшзфижуадеюимлжпэибабнсыужшмыдуфян бшижуашжкпквуфэбенгкюуыпрбвеощвзэкьемкцыкпмлнемщтаяцкицареижыцьешкыхмкянбшижуашжкпчыаихччфдзяйхфижца япбшижэкмдймкицвзхфэкмкййыэтфоикщуфьфюищехшофвержюуьпиницизгяепзкихжчфюиодаиуанкгашюзхмэхййьгнйфэфэкци цмяеавуфюнвыоуьпенэщянкиднэиьидккаьщыицьцтугыекыщпбаьуошуфьхянкицаеещфифатфзэьиуршхфуыппкицгкянсккарш ижызймбаэекчьпкшквуфэбенгкомбатнппцаабсыаицьатнфьфызтжкигшкибшпыхжяиьифгмпвахжжкщфэгдычгенмтгшйзхййь ркхйэеянщььеяьэежбицияхйймбаьфпщвоаибшуахжптпхызхйнфмщйтсжвехйщцэзыжэкрггжтнйцбфдесаоещфзыкпжффеккям кщошенпбккдзюпссмпрбккеатнпхбшкпхжкпащнеэфаыссятиускшкдзянуадеекчыппкшквуфэбенгкюущпирщцазижбоэенфьи пхвкрггжтнйцянаигшдензлзйзкдщеышпымпзкщфнфккмктжшмбатнйжиуггхффеюищпкшаивкрееэяежусснеекмибскпяощктг люхжящяюхжфгбамлкиомбатнппсдуфиеущсыэеекзайцдзкщиуьихфижфгзыбееквыязцукинбеньеймвфрьхйдзехызмкбфдзэз ыжужвештужспжувгсылшдеюищинкбщвфснусьияцспжувгшмшюдзекринтакцаржсынедеяячпнмьижздеюибареижьщьесикпню рилбккуихжчжшмыдуфьетнужчгедэщуфршхфижтнкиекрбгжсыииьигшбаофеибшбагнйжжксигшьбккяперцахжящчксжсыщдуф щфнфэьмбьфгкхичгрбетяьчгуфвттжшмбатнйжзохкянфггкшезгяеьбджпхсанфьихфчшкпвкоюбаоещфдюйжящвеоищезохкрж йцэзыжэкдзиждьмкдзуфгдуфьхошгннзышккпшакыплмгнпбьблзотяячпчкьыьишжешэкжеекишутйкзэкыяцшфхьфжзыиуйзлф чшшцижэкмибшкшгкизлэййеквзекцнцмцьмеяйхфзоиьывуфэбенгкчглюмпкщчжфгхтгрмдужфеыжйедзянуадеекшуьпкинбйз епьияерфуфьфщфхзгхиажшпхвбвеощвзэкьедепуьпфемкакдгчьнйдзяпбшексчьщенсасдэейфлряцшзьххйжайещфнтижгнмк егшмтнлюыденбаэищьиштфхгфгдзцыгжщакеззхбгнбшшаенхкэонгэщчечгщпужгнэщбдшжвацьйфэфнеегинлюфзэкхйэнэиют лфэкофэзхитфокфзюибахещакомкекдиэщппштееыаиусесщлььеекппкшквуфэбенгкзкремкхщнфблатншьищьикязшеижнфаи

бшкшвзуфакзгвеюикщгккиюудьмкййдзофдекиуажшкпцаэесщппяаоеиеяпьукщхйрбэьйфзхзглювампквуфкиомбатнппаисд ймвгьфрещфэьчндыдкофйкиемкоюхщймфвуфщфэезхтшужнфгыгфижуаппцаппяиафижуаппцашжшузгкщвзэкшкцнащатршхфтж кидыкщвзужйьпыхфщфхшкпхжйвуфщзипхдшжжыинчгфгйфзикщрфвелбвгэисащмдзмкдзцкдбужгнштсмуашюыньияержкщппяи тнэщянкицднэиьихфсаэхшрблчягнюленшкаиюлршппкишулбршнещсйтцахеьебурнбецаязцчдевеутльцчсалбршутйкамкицош енижфеюитыянсдаидыиждьярвыуфжещзшкубйжкеьхмкянцагнжецчйуенипцьнеуффпаиьщуфяйрфязкдкпбатгэщрфяйрфязпа йеюишмсыаиащдндкспуахфрфчздшкосещфкиомбатнппчгфгйцкиекьщхйхщймфзвзшиодаимпаивфпдьщыикцнеяйпхюдкпбатг ппщдееймкиужфзежщевтдзиждытъалзижпбгжсыщдуфнфмиэивыбсужжшгкищхежииуйюбшаиижыздзазяйижнфызекчккиофяз жефжыдуфкийфжеыщнелзхйязрфобвглюмпоегьюяаияьдшзксскпжзкыщьдзмзищднйедзащппяидкгжижшбппгшршккпщлилбки ьщикекязаксбтнусьияцуфгхиуяюэихвгккжщпцгиуенипяосскпшжлбгинюдыьийжпзьглзоуьиомоехфкжбаоеофйкйиужофуф вттжиуьиомоеотжеофязщзещнфдиьщофзфйикшхйдмршцмбатнппппкшквуфэбенгкйрьщнхшуьиомоеекижщмбатнпппаннбьфгк здуфхщужфгаишуыпкичгшмршкпяищечфихыищеиееквщьидкязшицагнгкййхщужфгрбккнеайшивыпкзохкржйцэзыжзкжфязех ызмктжбаоедзеегжижшбдеекбшршккпщйуьпьбкщнхоищцеелбтнусьияеюуьщянгнвапхфнцшурюувгшепущпирьигшкпяоуфнк бфзмбатнппчфекьебпидееофбныцэеуыгньщрфвелбйцвтндуфвзшивыбсужжшгкэиясьиэеязрфмиюуошэуенипыцодкпбатгяз цуьиомоехггжтнкцофязщзхтжеоегь эыщфятрфуфьфвтгжфзещянуабшмкнфижящдыдзофдекишжфгйцшеэффезюфггжтнтыьхлл гжхфяноюдзызмкепэщхйшжфгбайцыщхйуфяйрфршаииееквщьиоеийгхшуьпппшчфггжтнкехщймфзьщхйнфзфиеюикщгкянзыщп ршмлшфатфзэьикрфуффхшфзфиеюисыхфшфьхэфянзквбгихжтибздешшэицикпшчлмьигинпбаиямкбеяйгшэжэиуфхисдиндыныб вефзюикещфатфзеоэеязаквбгнхжтниивгфгшеэффеязиубсяощкщещфашбньихфюуьщрффхижхфязчещфиубсмпьфижбаэыщфят цажшсэяехивыэеуфяйрфхщбшиуьфнеьемкхфцаоеязшеижызшеэффешезгяержппшчюлгжчкнфрлбэмпащящбнсыхфижбощфатфз эьгжязехызярймкщифугсыэижфызекзайцзгдыаивфатншмпквмтоюмкжижозгьфсикщхйцскпмпшжщпцгвфоишмскдзиждкызмк дзуфгдуфьхиубсыегхьмкщошенцфижуацаоюмкжищеэежффекктгоеиеиузаппгжбнджыдуфкиижэибашжйьнфспуасайцзгэщкщ взэкгуыбккоеиеяжьупаенгкутспуахфрфчздшкосещфащбаужвьййишьиясхфзфихыитышжтфвегкязшкрбйзсжчгдыащдыьхфе ещнфцайцзгфггжтнмлршхфржршбакпиусшбалщеещфзфиждьекзавфятееепьищьнфййчзршдыцьбфяймзямутзбмпкшщцрфуфйз ббкшнфвыафкнсыхфвтрфмкшеижжтгжхфцклзййяшутйкйгфгаыищкшуфапдкгпкшшцэежелзярблекшкйзекнфмилиаиэщмтэзье яйпхзшэкжеекмичфбфьфекьеяйхфщфлзбеэьекянжшккпщьиомнеьхуфекьхэфекпзьглзриомкщошенрирбетяьекиееквщьиэи бскпяощкщжщпцгвфоишмскхзйфщфатсеижфеюишмкидкбфяйнкзшяьоегьзхщфхкошбащпящтаяцожйцвтыийцнфнехевебныэца яощкбщчкхевезтнхызеэблйьаидномрфуффхтгйркпрбккспуахфдгызыжинймкщошензафеййчзсишмсыйфзииуьпьтабужхавз рфгдуфэегхяпзыиуйуьпбацнцмйеюнвыифхкюисскпцьуфяйрфофьеэьхйжайещфзхщфоишмьбщпбсьищьпхпдьщшмлзмзещрщяя чпвыщзожйзабьфгкхичгсыймьбкщдещзожйзбжфещсфзидуфэезыщеыичгфгшмсыэескифрккаьщыисыянбшреьеуфяйрфюпйжшм ыдуфьхоюиензхйгжфеыштаьихфижзкцмршшжнмкщошенкшутщфгскпяощкэбккиувеижцащмршгфснюэмпдзоегьхизыэияещфат фээькнсырфбнсдхжкицдыйсдэтжкидытготумкицошеняифгэиииьщофккмкбнсдмпхицбаужлтфээьришиузакношжкэхехызриьщим лзмзеэблйьдзятзпжкьевбвглювацьтжвфммгжбаьххйжеыжнфыфкэщцофяйехднужяцянкщуфзхянжрцампоеиереншошжтбщба ужбацагжатыштаяеюнлмбабшаибавереюийеофэфркйюэщнфьагнотдшхтеуцюдзвдуфьехеэйэерфишьуошужгжязщзхйвышдуж феыжки эе азрих фхицлбь б г шмпйь дзсплюлмки ошены фхьудьипх фньугжй црынх т шяь у фифтжи у с шки пквибжеш у ах фжел з ю и й цме мкиубшнтщфатфзэьбсьщуфшеюиршвглювампянуагжпкмкэеянуагжяахфпйзхижшбцаеещфсиьищьжшяьржшмьбккнфхкгущпще ппзыьищецкяйпхвкабйзфеюпцакежфязщзьеяйижызхщкпкшквуфэбенгкппбаппинжумкбныщнхбкпхцаржсыэфепьизкяпбшпп шжшпцгшюэинбйзепьияещязобейзузгщрфуыппкшгкшжшпцгыдуфшзреазмктжтязобеьфсихжппйьнфоиищуфьфотязпаоержгж утыисайедзоедеекбзкызкдзбкдзэфятхйожясьщуфьфотвзкдуфщфатфзеоьекжутоищеьхэфоффегибжюещфышутттдщвехкэе ьбвенедеюикщгкофэфжеекббккцмьфнзеэщцоеэййюхфдфэзпикщгкянжшуауаеегаоевткщиуьихфднсабспхнленфгьегщвехк ржшмбаблэьаидномхэйфзоркмшуфэгхффеекфнлюмкщимлнфвювеекукктхштаянинлюхфжпвыьихфижцаоелвгкрпшчржуакщжы цьхзчзоущпирцьэзыжщьзонемиэийжмлмкщитызкцжгньцдырбккфзызлзбфяйцттюнббжэихфижжкцыбжхфижцфкэвыошкпагфг йцьхекофоизымпйьнфянкщнтпнйцржблднбжэемитффжутркфеседзябвезищцьейфэбгнкпужмпдзхфжтлкжаскисяснзеквыщз спермпоюхжвычьмкзгвеюияеабтнеэяещфэфхзоюхщылржблэзыжяцожкшдыйеюнвыигфгшияюездшвеэбккылмпязкызкэфснмп эщюесершдзнепьвзббенгкриодаиуамзббршекчэхйжайцщфэфщвуфьхлээзыжщьзонемщвэфхйнлюпыпхпмкщошенижфеюивфих ыимлртреярблэейзщшкпкьекршхфщфоюянгжцатнмдюэблсиьияцгжепмдьихфофцыгжвехйдзхщмдуфнелзэфййянйрвзиеспуа хфдгызыжинткиуятчэхйчнбшижызпамлршпкювуфмитфянбшкпьихфижаигндршжкпяикщгкщзэтвэюикщгкащлэбфижппкшквуф эбенгкомбатнппзкятчзмктжбаоеятгийеянскрлршшжянвквтсеижфеюивфмбккатыщтащьщфатфзэьжайеюитыеатнсыянжзкы зктжбаеншкфбгньиьщьихжэитфянбшкпьидзбтяпбадзчкрфдешпеэцьйьмзугкщхйгжхфееекдггжтнцьошиудзянжшнфвехфюн бшдзызкызктжшмкщошендиясхфузгщтабахжезэешбйзепйжхайцзгсытжйехкющтаьипхгамлршоюржшмьбщпбсьицьыцхйгжйю эмкщошенрцимршнфьфшкщзкызктжвфоиьбккатыщтаяещфатфзэьэзйзмкдтужрьхйнейьфжлщвднфмщязотзимлюпифиеабмдьи щьймщпсдхфкуйюьбэщхфижсдуфхзгхэбэфшфмикийюуаащзыкцспуахфрфчздшкощккуошужхтгрыщдышмщпшдеещфхфжаяюэихф щфянащбжижэквыцалзижбощфатфзэьожкщдыйеюнвыигфгшияюездшвегсппиещшкпнбккцнащоенкюгбащфатфзгщтаьипхмщтг вевзэйьхяряцршекшквмлзхимлянбшижуашжкпщиржйцэзыжэкдзюкхзумкщошенфбащжывгтжтнйеэфспэщппащпбршюкхэхйпз лзееэкенфгшесажбащжыевуфвбщпнювьййфзюитывыафкмкщошенббшюнфдееквыйзпщясфзхйиуиусетлршбшкпкиофтжшжкпяи скофябвеюпшмсыэеиушфхкйфижжшяьщфатфзэьнфршсрсашжцгнфмиьиенршхщуфмкмеянбшлзизумкщошеныфижуашжхайцзгвф ятееепьияешфагфзвесиенридкиффкембертиничений в интереструктуру в интереструктур в интерестру в интереструктуру в интерестру в интереструктур в интереструкту ащбжижэквыщфатфзэьэыкщпатфятееепьияедзьффэрфуфьфшуьпшмлэхийцянсдаийцуфщсьщтаенкиццкюуьпьбвеощвзепьишм кщошенлкянаийжскйгфгянбшэфишяькщвзепьищьеншкжз

Розшифрований текст:

князыандрейпричхалвглавнуюквартируармиивконцеиюнявойскапервойаяяиитойприкотоюойнаходилгмгосударыоьлирасположтны укреплтнномлагереудриссьвойскавторойармииоеступалистреюмсысоединитысяспервойармиейоткотоюойкакговорилионибйлиотре заньболышцяисилояифранцузоввсебйлинедоволыньобщияходомвоенньхдеюврусскойаяяиинообьпасностинаштствщмврусскиегубе рнииниктоинедумалниктоинепредполагалчтобьвойнамоглибьтыпертнтстнадалеезападньхполыскихгубернийкнязыандрейнашелбаю клаядетолликкоторэяуоабйлназначтннаберегудриссьтаккакнеоьлониодногобольшогоселаилцятсаечкавокрестностяхлагевмтовсеогр эяноеколичтствогтнераловипридворньхбышихприармиирасполагалосывокружностидтсятиверстполучшцядомамдеревтныпосюипо тусторонурекибарклтйдетоллистоялвчетьрчхверстахотгосударяонсухоихолодныприямлболконскогоисказалсвоцянемецкцявьговою мчтоондоложитонемгосударюдэмьпределенияемуназначтнщмапокоятстпюосиаегосостамтыприегоштнбеанатоэмкурагинакотоюого князыандрейнадцмлсянтйтифаяяиинеоьлоздтсьюабйлвпетербургеиэтоизвтстиебйльприятноболконскэяуинтертсцентрапроизводяще йгмогюомнойвойньзанялкнязяандреяионрадбйлнанекотоюоевреюмосвободитыгмотраздражениякотороепроизводилавнеыяьслыоку

рагиневпродолжениепервыхчетьрчхднейвовруяякоторьхоннеоьлникудатребууякнязыандрейобездилвесыукреплтннььлагерыиспэяо щыюсвоихзнанийиразговоровссведущимилюдымистаралгмсоставитысебеонемопределтнноепонятиеновопросотэявьгоденилиневыг оденэтотлагерыосталгмнерешеннкядлякямшмандрцмонужеуспелвывестиизсвоеговоенногоопьтатоубеждениечтоввоеннэяделеничег онезначатсамьеглубокомьслтннообдуманньепланькаконвиделэтофаусаерлицкомпоходечтовсезависитоттогокакотвечаюенанеожида нньеинуяогущиеоьтыпредвиденнкяидействиянеприятелячтовсезависитоттогокакикемведетгмвседелодэмтогочтобоуяснитысебеэтот последнийвыпюоскямзыандрейполызуясысвоцяположениуяизнакомствояистаралсявникнутывхарактеруправлтнщмармиейлиципагт ийучаствовавшихвонэяивывелдлясебяследующеепоямтиеоположенииделкогдтещегосударыоьюввилынеармиябйларазделенанатроея аяящмнаходиласыподначалыствэябаюклаядетоллияподначалыствомбагратионемподначалыствэятояяасовагосударынаходилгмприп ервойаяяииноневкачтствеглавнокэяандующеговприказтнебилосказаночтогосударыбудеткомандоватысказанотолыкочтогосударыбу детприаяяиикрэяетогь пригосударелично небилоштабаглавнокомандующего нбилштнбця ператорскоц главной квартиры принуя оылнача лыникцяператорскогоштибагтиералквартияяейстеркиязыволконскицгтиеральфлигелыадютантьдиплэяатичтскиечиновникииболыш оеколичествоиностранцевнонебйлоштабаармиикюометогобездолжностипригосудартнаходилисыаракчеевбывшийвоенныйминистргр афбтнигсенпбчинустаршийизгенераловвеликийкнязыцтсаревичконстантинпавловичграфруюмнцевканцлершаейноьвшийпрусскийм инистраяяфельдшведскицгтнералпфулыглавныйсоставителыпланакампаниигенераладютантпаулучисардинскийвьходецвольцогени многиедругиеходмэтилицаинаходилисыбезвоенньхдоюжностейприаяяиинопосвоемуположениюимеливлщмниеичастокорпусньйна чалыникидажеглавнокомандующийнезнаювкачествечегоспрашифаетилисоветуеттоилидругоебенигстниливеликийкнязыилиаракчее виликямзыволконскийинезналоаеголилицаилиотгосударяистектеттакоетоприказаниевформесоветаинужноилинтнужноисполнятыег оноэтобилавнешнрмобстановкасущественныйжеаяьслприсуествщигосудавмивсехэтихлицспридворнойтбчкиавприсутствиигосударя вседелаютгмпридворнкяивсембйлястноноьлследующийгосударынепринцяалнасетмзванщмглавнокомандующегонораспоряжалгмвс уяиаяящммилюдиокружавшиеегобйлиегопомощникиаракчеевбйлверньйисполнителыблюстителыпорядкаителохраниаелыгосудавм бенигстноьлпэячщиквиленскоцгуберниикоторьйкакбудтоделалкраяавсущностибйлхоюошицгтнералполезньйдлясоветаидлятогбчто оьцяетыеговсегданаготовенааятнубарклсмвеликийкямзыоьлтутпотомучтоэтооьлоуяуугоднобывшичяинистрштейабйлтутпотэяучтоо ноьлполезтндлясоветаипотомучтоимператоралександрвьсокоцтнилеголичньекачтствааяяфелыдбилзлойненавистникнаполеонаигтне ралувертнный всебечтоимеловсег давлщинит на александрапа улучиоь лтутпотом учтоо абйлая елирешителт нвречах генераладютантыбил итутпотомучтоонивездебйлигдегосударыинаконецглавноепфульоьлтутпотомучтоонсоставивпланвойньпротивнаполеонаизаставива лександраповеритывцелтсообразностыэтогопланаруководилвсуяделомвойныприпфулеоьювольщогтнпередафавшиймыслипфуэмвбо леедоступнойформечемсояпфулырезкийсояьуверенныйдопрезренияковсемукабинееньйаеоретиккрэяеэтихпоименофанныхлицрусски хииностранньхвособенностииностранцевкоторьессмелостыюсвойственнойлюхммвдеятельностисредичужойсредькаждыйдтныпред лагалиновьенеожиданныуяьслиоьлочщуяноголицвтоюостептнныхнаходившихсяприармиипотэяучтотутбйлиихпринципальвчислевсе дяьслейиголосоввэтэяогюомнэябеспокойномблестящуяигордоыяирекямзыандрейвиделследующиеболеерезкиеподразделтнщмнапра вленийипагтийпервемпагтщмоьлапфульиегьпоследофааелиаеоретикивойньвевмщиевточтоестынаукавойньичтовэтойнаукеестысво инеигятнньезаконьзаконьобличтскогодвижтншмобходаитппфульипоследофааелиеготребофалиотступлениявглубыстраньоеступлтн щмпоточнкязаконампредписанныянимойтеориейвойныивовсякэяотступленииотэтойтеориивиделитолыковарфарствонеобразованн остыилизлонояертнностыкэтойпагтиипринадлежалинемецкиепринцьвольцогенвинцингеродеидругиепреимущественнонуяцьвторс мпагтщмоьлапротивуположнаяпервойкакивсегднбьвтетприоднойкрайностиоьлипредставителидругойкрайностилюдиэтойпагтииоьл иаекоторьеещесвилыньтребофалинаступлениявполышуисвободьотвсякихвпередсоставленньхплановкрэяетогбчтопредставителиэто йпартиибйлипредставиаелиаяельхдействийонивместтсаемиоьлипредставителняинациональностивследствиечегостановилисычщеод ностоюоннеевспореэтибилирусскиебагратионначинавшийвозвышатыгмермоловидругиевэтовруяябилараспространтнаизвтсенсмшут ктеяяоловнбудтооьпросившегогосудавмободночяилостипроизводстфаеговнемцилюдиэтойпартииговориливспэяинсмсувоюофачтон адонедвяатынтнакальватыиголкояикартуадратыгмбитынепрщмаеэмневпускатыеговюоссиюинедаватыуньфатывойскуктретыейпагт ииккоторойболеевсегоцяелдовериягосударыпринадлежалипридворньеделателисделошяеждуобоиминаправлениняилюдиэтойпартии болышейчастыюневотнньеиккоторойпринадлежаларакчеефдвяалииговориличтоговорятобькновеннолюдинеимеющиеубежденийно желающие казатыся затаковьхониго вориличто безсэя нения война особтнностакця гениу якак бона параеего обмтына зьфалибона пагтетре буетглубокэяьсленнейшихсоображтнийглубокогознаниянаукиивэтэяделепфулыгтниаленновместтсаемнелызянепризнатытогбчтоаео ретикичастоодносторонниипотэяунтнадовполнедоверятыимнадыприслушиватысяиктэяучтогововмтпюотивникипфуэмиктомучтогов орятлюдипрактическиеьпьтньеввотнномделеиизовсеговзятысреднеелюдиэтойпагтиинастамлинатомчтооьудержафдрисскиьлагерып ыпланупфуляигятнитыдвижениядругихаяяийходмэтцяобразомдействийнедостигаласынитанидругсмцелынолюхмяэтойпартииказало сытаклучшечетвегтоенаправлениебйлонаправлтниекотоюогосамьмвидньмпредставиаелембйлвеликийкямзынаследникцтсаревичне могшийзаоьтысвоегоаустерлицкогоразбчарованщигдеонкакнааяотрвьехалпередгвардиеювкаскеиколетерассчитьвсимолодецкиразд авитыфранцузовипопавнеожиданновпервуюлиниюнасилуушеювобщемсюмаениилюдиэтойпартииимеливсвоих суждтнщмхикачеств оинедостатокискренностионибамлисынаполеонавиделивнемсилувсебеслибостыипвммовьсказывалиэтоониговорилиничегокюомего вмсрояаипогибелиизвсегоэтогоневыйдетвобяьоставиливилынуоставиливитебскоставимидриссуодночтонояостаетгмвяногосделатыэ тозаключитйяирикакможноскореепоканевыгналинасизпетербургавозщртниеэтосилынораспространтнноеввысшихсферахармиинаход илосебеподдержкуивпеаербургеивканцлереруюмнцевеподругимгосударственнкяпричиноястамвшуятожезамирпятьеоьлипривержен пьбарклемдетоллинтстолыкокакчеловекасколыкокаквоенногряинистраиглавнокомандующегоониговориликакойоннитетывсегдатак начиналиноончтсеньйделыньйчеловекилучшеегонетдайтеемунастамщулвластыпотэяучтовойнануяожетидтиуспешнобезединстфана чалыствофанияионпокажеттбчтоонможеесделатыкаконпоказалсетмвфинэмндииежелиаяящмнашаустроенаисилынаиотступиладодр иссьнепонтсшиникакихпоражтнийтомьобязаньэтимтолыкобарклаюежелитеперызоятнятбаюклаябтнигсеномтовсепогибнетпотомучт обтнигсенужепоказалсвоюнтспособностывгодуговорилилюдиэтойпартииштстьебтнигсенистьговорилинапюотивчтовсетакинебйлон икогоделынееиопьенеебенигстнаикакнивертисывсетакипридешыкнуяуилюдиэтойпагтиидоказьфаличтовсенашеотступлениедодрисс ьбйльпостьднейшеепоражтниеибтспрерьвньйрядошибокчемболыштнаделаютошибокговорилиониаемлучшепокртйнечяертскореепо ймутчтотакнуяожетидтианужтннекакойнибудыбарклтйачеловеккакбтнигсенкоторьйпоказалужесетмрягодукотоюомуотдалсправедл ивостысоянаполеонитакой человек закоторкя оьохотнопризнафаливласты и таковой тетытолыкоодинбенигстное дымые бйлилицакоторы евсегдатстывособенностипрцяолодьхгосудавмхикоторьхособеннэяногооьлоприимператореалександрелицагтнераловифлигелыадют антовстрасеньпреданньегосударюнекакимператорунокакчеловекаобожающиеегоискртнноибтскорьстнокакегообожалюостоврягоду ивидящиевнуянетолыковседобюодеаелиноивсекачестфачеловеческиеэтилицахотяивосхищалисыскрэяностыюгосудавмотказьфавше госяоткэяандофаниявойскояиноосуждалиэтуизлишнююскоомностыижелалитолыкоодногоинастаифалинатомчтооьобожтемьцгосуд арыоставивизлишнеенедовериексебеобявилоткрытбчтоонстановитгмвоглавевойскасоставилбоприсебештнбквартируглавнокоманду ющегоисоветемсыгдтнужносопьенкяитеоретикамиипрактикояисояоьвелсвоивойскакоторьходноэтодовелобьдовьсшегосостамнияво одушевлтнщмвосымаясоясмболышаягруппалюдейкотораяпосвоуяуогрэяномуколичествуотносиласыкдругимкакшяусостоялаизлюд

ейнежелавшихнимиранивойньнинаступааелыньхдвиженийниобоюониаелыноголагевмнипридрисстнигдеоьтониоьлонибаюклаяниго сударянипфуэмнибенигстнаножелающихтолыкоодногоисамогосущественногонаиболышихдэмсетмвьгодиудоволыствийвтоймуено йводеперекрчщивающих ся иперепуть фающих гминтригкоторьекишелиприглавной к фагтирего сударяв в есымамног эяможно биль успет ывтакомчтонемьслияобьбйловдругоевруяяодиннежелсмтолыкопоаевмтысвоеговьгодногьположтнимньнчтсоглашалсяспфулуязавтр аспюотивникэяегьпослезавтраутверждалчтонецяеееникакогэяненияобизвтсенэяпредмеаетолыкодлятогбчтооьизбежатыотвеествтнн остииугодитыгосударюдругойжелающийприобрестивьгодьобращалнасетмвнцяаниегосудавмгрэякокричатосояоеначтонояекнулгосу дарынаканунтспориликричалвсоветеудавмясебявгрудыивьзьфаянтсоглашающихгмнадуэлыиаемпоказьвсмчтоонготовоьтыжегтворо бщейполызьтретийпростовьпрашивалсебемеждудвухсоветовивотсуествиевраговединовременноепособиезасволверную службузнаяч тоаеперынекогднбудетотказатыуяучетвегтьйнечаянновсепьпадалгмнаглазагосударродмгчтнньйрнботойбмтьйдэмтогочтобьдостигн утыдавножеланнойцелиобедаугосудавможтсточеннодоказьвалправотуилинеправотувновывьступившегомнтнщмидэмэтогыприводи лболееилцятнеесилыньеисправедливьедоказааелыстфавселюдиэтойпартииловилирубликртстьчиньивэтэяловлтнииследилитолыкоза направлтниемфлюгерацарскочяилостиитолыкбчтозамечаличтофлюгеюобратилгмводнустоюонукаквсеэтотруеневоенаселениеаяяии начиналодутывтужтстоюонутакчтогосударюаемтруднееоьлоповернутыегофдругуюсрединеьпределенностиположенияприугюожаю щейсерыезнойопасностипридававшейвсемуособтннотревожный харакаерсредиэтогових вминтригсамолюбийстолкновений различных воззренийичувствприразноплуятнностивсехэтихлицэтавосйясмсамаяболышсмпагтщмлюдейнанятьхличнкяиинтертсояипридафалаб олышуюзапутанностыиаяутностыобщуяуделукакойоьниподнцяалгмвопросаужройэтихтрутнейнеоттрубивещенадпрежнейаемойпер елеталнановуюисвоимжужжаниуязаглушализатуяямлискренниеспорящиеголосаизвсчхэтихпагтийвтосояоевруяякаккнязыандрейпр ичхалкаяяиисобраласыещеоднадеумтаяпартияначинавшаяподниматысвойголосэтооьлапагтщмлюдейстарьхразвяньхгосударственно опьеньхиумевшихнеразделрмниодногоизпротиворечащихмнтнийотвлечтннопоаяотретынавсечтоделалосыприштабеглавнойкфагтир ьиобдуматысредстфаквьходуизэтойнеопределтнностинерешительностизапутанностиислабостилюдиэтойпартииговорилиидумаличт овседурноепроисходитпреимущественноотприсуествщигосудавмсвоеннкядворэяприаяяиичтовармиюпертнтстнатанеопределтннаяу словнаяиколеблющемгмшаткостыотношенийкоторсмудобнапридвореновреднафаяяиичтогосударюнужноцарствоватыанеуправляты войскэячтоединствтнныйвыходизэтогыположтнщмтстыотездгосударясегодвоюомизаяяиичтоодныприсуествиегосудавмпарализуетбм тыдегмттьсячвойсканужных для обеспечтнимеголичной безьпасностичто самый плохойно независцяьй главноком андующий будетлучш тсояоголучшегоносвязанногоприсутствиуяивластыю госудавмито сояо евруяя каккнязы андрейжилбез делапридриссе шишков государс твтнньйсекретарыоьвшийоднимизглавньхпредставителейэтойпагтиинаписалгосударюписйяокотороесогласилисыподписатыбалаше виаракчееввписйяеэтомполыземсыданнкяуяуотгосударяпозволениуярассуждатыобобщемходеделонпочтительноиподпредлогэянео бходимостидэмгосудавмвоодушевитыквойнтнародвстолицепредлагалгосударроставитывойскоодушевлтниегосударемнародаивоззф аниекнемудлязащитьоаечестфатосамотнасколыкооньпюоизведенооьлоличнкяприсутствиуягосудавмряосквеодушевлтниенаюодакот оюоебйлоглавнойпричинойторжтствароссиибйльпредставлтногосударюипринятоимкакпредлогдэмоставлтнщмармииа

Шуканий ключ - (725, 100).

(725, 100)

(723, 10

аь: 0

еь: 0.000321388 иь: 0.000160694

йь: 0 уь: 0 ыь: 0

ьь: 0.000160694

эь: 0 юь: 0

яь: 0.00128555 ьы: 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):

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

11	(449, 604)	на: 0.000803471
12	(298, 918)	уь: 0.0056243
13		<u> </u>
	(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)	ыь: 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
L	· · · · · · · · · · · · · · · · · · ·	

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.