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

КРИПТОГРАФІЯ

Лабораторна робота №3

Криптоаналіз афінної біграмної підстановки

Варіант 19

Виконали:
Студенти 3 курсу
Снігур А.Ю. та
Носова Є. О.

Київ – 2021

Мета роботи:

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

Постановка задачі:

реалізувати програму для пошуку ключа та розшифрування ШТ афінною підстановкою біграм з функцією автоматичного розпізнавання мови.

Порядок виконання:

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним

Хід роботи:

В ході роботи був використано російський алфавіт - абвгдежзийклмнопрстуфхцчшщьыэюя. Спочатку було створено додаткові функції з допомогою яких здійснювалися допоміжні обчисллення : entropy_func - рахує ентропію для заданого тексту (для перевірки коректності розшифрування), solve_congruence - знаходить розв'язки лінійної конгруенції ax=b modm (розглядається три варіанти), euclid_algorithm - функція для знаходження оберненого , gcd - іункція знаходження НСД. Далі за допомогою функції find_popular_bigramms - знаходимо 5 найчастіших біграм в зашифрованому тексті . Функція convert_bigrams переводить біграму в відповідне їй число. Далі було створено функцію find_key, яка за допомогою всіх раніше згаданих функцій знаходить всі можливі значення ключів (a і b). Ці варіанти ключів використовує функція decrypt_text, яка роззшифровує кожним ключем текст і перевіряє його валідність за допомогою підрахунку ентропії (entropy_func).

Найчастіші біграми шифротексту:

1	уф	0.01816
2	иж	0. 01655
3	ьи	0. 01494
4	хф	0. 01382
5	щф	0. 0135

Шифрований текст (Варіант 19):

шияюездшвеэбккылмпдмлзхикопаенгкутеншкцарфцчвкдизайцзгнбгннфтзкызкуфэбккрфуфьфмию
лршппйьщфатфзэйьхмкйзабщпбсьиваагвежпьихфбплмгнлтцнащбхнфмщязожтнйценшкчфыщмтэз
мкижвельййзфбшаишжящрщхещайценшкщцгжрфуфьфдгфгщфнфккмккиюуьпчфднйюэийущпирзы
ащппдыияйзцчцюбахщшуьпаибшбащпяигфкэзышфжфиайеюимлнеыаутпщрфтзкызкхфиуьбэщхфи
жаижрьщтащьюнищзгяеттиегизкексжскэеятчзеичгуфаилбвеябщплммптжиувайцдзйфспьуджпбгнь
иьщьигшмпщещзэзоимлофяйзгблттиегияцшияюездшвемижркппзьглзцшужщпмкргггжтнсыафыуьп
дзуиодьидзиеветтцнащбхвзргфгэеьхэфекршхфщфбфяйюфщфоелзппзыьщьесгуавгвеижхфижсллзбе
эьуфхщтфкнсыхфтгщпсдьщташмьигнмпбарбккеатнпхяуванксбккеншкинэщофлзизэфййнфбнясхфи
жжшьщйжцагнижофхтгрзыжфчзчшгнсаьипбкщлкофмтижтнкирнтгюуенипыцнеуффпащуфапздужун
ылфегщвзшфкмкщошенифющйлскшфэфоиьбккчьгущпрфющрфщфащязщзещнфзыэереегзызхщфнф
ьфгдуфкижфэфокуфэеамкщошенкшяььбвенедеекпевтдзуиодьищьнбвгдыьщмбьфцкьещфзфиждьх
йяняещфяжьубздзуфяьйтйзйкдзрфуфьфщфшияюездшвемигшфьещриыцгкызкызкэеьхэфщшьщцфы
уьпжбужгнщтсмвкржсккаьщгкшуьпьбккйжхфбфэгкизгсыпкцжгньщмецжйзянсккаршсэщцйьшмьфс
ийцнфмищюэиапшияюцздшвечккийзмуьпдзэерфуфьфсавелькщнфбфхкхййьгжйзщшйзжеекиггжтн
йеянсккаршппуаэешылщяйвгрнлмаисаянршщпжееклбгнзхтдужунылоищцнфюнвыиггжтнмлкиэеьх
еичгошхжвещтвышияюездшведфиещшппфеййагвежпьипхыплмгнжкабсылэбожаскпюдзекукйзвмб
атнбапщфеятщкшкзоийшкиженмпйьзфижуашжящшутфэейфянбшкпьихфлбкийжяехфнфянкщгжсыз
хщфнеекмкэезхщфнеивуфлплмгнцфижмпйьэевееееюитыюпигчьньэицнфькиярслтабкпзхфеижзкущн
фймбайеюишмвфихвзуфжусснеекмдуфмайеюисынедеекшещфэеуиодхжхзгхймхтбфрфгхяпьифиуят
чзюикежпэиггфгкиэкнепвуфызищьетпшчрфвбллршмдуфхщйюуаащшжгжуфщфязрфтамдяоыиэитф
окфзюикеаивышмйэяеьххйянбшэкнеюитыжшщцижэкрилбккйжкпвдуфхщйюуаащшжгжуфщфязакч
еиабшужйьхщбшкпршяьуфщфтжиуытрщекхйоеиержгжофяпбшекгаьбьфзгчьнйэицнщцофяйдтрщя
щнфзыофэфжееквыоюдзрфсщтадыащвзйзещзаекшибжхаззйзсжгншбйзепьищьеншкщцмкфкэзыжя
цщдэщтабауанкчакисыцавакпюпрщшурщдеятеэщеофчьгктфофэфжеекжшкпрфишыесещфатфзэйьх
ыаэкяйэееншкоуьпенлюнедедздзднйецзкыщьдзшфхклзййофоиодмпящтасыпзьглзцшужщпмкббр
шдзазяйижнфпулмйзгккицьофоиодмпящтасыуфкыэщбалмкщошеняиюлршппйьянрбгннфтзкызкхф
эенгодьщтаймлзхивгсыэиятеэймбаянчглюьишуьпкщязщзхфтжшмкщошенэуошужрфчздшбахжящяз
щзхфуфяйрфтжшмкщошенэуошужянжзкызкбнсыужшмьбккщфатфзвемкщикишуьпурвзпзспуахфрф
чздшкосещфьуьпяжьузыхейзуфгщрфьмлзхийцпаенгкфхянаивыьхеиодмпяичгзыхейзуфгщрфщфяжь
улмьигнмппаенгккыщцижгншияюхащпрфющакьмьигнмпуямкбеяйгшэжэинххкжпсыхжсдьщакмда
ибаекакюущпирйерфмкшеижнфаикщднэимехикишуьпурвзпзеншкчгьфреуфщфиещшщпзикщгкяно
мкщошеньиюлршппащезйзкдщеууванкгайеюикцшкекижсмйзтуьиомоеобыдаиищвзмряцоюбеэейз
эфмакпчгяцшияюччьщенсасдрфющвзцжаиэзепбасдкнеяутльцчсаязцчдемрьемиьхяряцянищзгяцшк
екижйзкыуеяйчрфеощакьмьигнмпяячпнмлзхикцзфижуашжкппблздзязвбэизкбеэейзлзровзцжэзчп
щдащенхкющакгамлршучнфяйефбеексишмяецнцмяешфхьржппшчдкдзшфхкмкййиекайеюимлжф
ысхфижщцянжзкызкхфофжайевтофэфжееклкремкепщьеквказижвгтнзтпикцдзазяйекакфзжеспуахф
рфчздшкощкмийюдзыаязшеижфешещфабйзнкызужппащбаужзефжскмкцнцмйеиееквщьиппцакпч
гяцшияюжкмкенфгшесаппчгчьнйнфэгкизгяцаийюдзэфьещфмкмкузппчфкмкщошенчкижтгыефжфгй
еуфянчглюэияеюятнрезффевзаиясхфппаиьиясхфащофеийжюещфхфржиуьпуаэежикьиуижэибаязат
сеижфеюикцжецылщхбккатыщтащьщфатфзэьцаоелвгкрпшчабккеатнхфежыдакуаянащбжижэкомк
щошензаоенелзэжйьянжшнфгитыцаоепуьпрщьикиьхещдеятеэяцщфатфзэйэеянаизымпдзоегькаэи
щьспуахфрфчздшкосещфхфйзабтнзсмпйьхщвыжзкыщьшкзохквгутнзяряеймиуьпяещфофйфтичгжзй
зкдщеууьпфегикцащофеишжкпэузоижшжкппбтнцшязшжкпллйзекьеяйщфатфзэьиееквщьиьххбсыы
эчгэкдеющрфьмжугнекчггжтнкцязцуошуфнелзэгйзцзхщйэхфижюуьпшфьфнкьмьигнмпофдеуикцюп
рщбауждкюпйжшмыдуфьхзыужюещфхщймфздзщфуффедзцыьижуенипцьфемкакдгчьнйьхюжбжо
фуфвттжфвуфьхэфвыштщфоииуванкуыаиащдняжщцыуьпмтмбгжсыщдуфкиьххбщпйюьиюпрщбауж

дкофуфвттжсквбгнхжтнмптгхздшщалщвггчьиппймщпсдпхтгодьщтагзкыуеяймуьпгпйцэедзэкижекш
инбщптфдзомьигнмпяагньипхгаоеиетжскреэфхщймфзепщьекьигздешщэицннбнтхтбкьхюжбжофуф
вттжвфыуьпцыкпиндршжкпьиюнмдюлбеэейзлзровзцжйуьпшжбжофуфвттжвфекфещшшуьпомнещ
фатфзэйаифгкиучспуахфлбетяйьхюжбжофуфвттжвфющкщвзэкжблзфайцпхянгжцадзофдекидкщзи
жуацамптгхздшйзоффеккхйочкпьщвфснлюхфижйвуфщфжпэиенагбаршппхщвынеэфиайцпхянрбетд
еьхыащпччшмьихевефзызяряцгхяпрбетяьуущпщежфижшбхффятнрешесщдыяячпзнйюакмщдыьтф
евеюикцжфянйювеекигбаоевтязркэеыикцьетнужчгбнсыевгксбскрехфызюимлмкхнищзгблзкхфижй
зюимлнфзфиеюикщгкаикщднэименггжтнкепщреэфижбожайцижфеюийцзоиьианейжкпяикщгкчнб
шсдясйцчнбшггусахтшьипбвеюплммпаибакеэебсжшэипхвылщмкьхэфыэвыхфщфмкдауфьфижлбьи
пхбиюлршцанкбщббккеншкрбгжсыщдуфмтщуьпзксбккцчрбмпвабкяпсаоеиылщдеукщфэфзфмаржс
ышмьфсисыиеабвгйцхфпудеижсэвыомтнжфшыинтгчьнйэицнщцэкнеещдеятеэяебфдегнйюаклбрш
йзщшкпьищьдзянуадеекукэзыжяцхещацьэзыжщььхлзяячпжкймьбкщдежфызьемкьетнужчгцайцпх
феэьщксауфтжйеижяинтязнфмитктжбаржйцдзагщеижящнфаивкьыьипхйюфгкищюфгкигфшпсдьщр
фщфеацсьищьиушффзшжзбетяйрбкщдежфызьемкймгжвебфызмкгжижшбдеекзаспжуящднэигфыщ
мтжпьищьофуфщитыщзрфдзвбвеябащэипхшыекйфежтфккщцнфмиткнфхщигсыгжижшбдеекчфжву
фежтфккцажшкпшжщпцгбаенызгщтакитфснлюбаэихфижжкмкгпкидыгньихфижцгржйцэзыжзкянаи
гшдензмкэереегяеянаияхнфяйефбефааифкммгнршвкцнцмяеянвквтсеижфеюикивыяхожтнцьэзыж
щььхлзянгжцашбщпбсдзббгннфдгфгцаоеишьуваыембккршхфдгйзмикщгкьхмкянбшижуашжкпжшу
тщфдгйзмикщгкзохкржйцэзыжзкьхмкьерфуффхщесежаппяиджвебфызмкдзижшбдеекзаофяйцтащ
нфбфахгжхщигблжбгнбшзфижуадеюимлжпэибабнсыужшмыдуфянбшижуашжкпквуфэбенгкюуьпр
бвеощвзэкьемкцыкпмлнемщтаяцкицареижьщьешкьхмкянбшижуашжкпчыаихччфдзяйхфижцаяпб
шижэкмдймкщвзхфэкмкййыэтфоикщуфьфюищехщофвержюуьпинищзгяепзкнхжчфюиодаиуанкгаш
юзхмзхййьгнйфэфэкцнцмяеавуфюнвыоуьпенэщянкщднэиьидккаьщыицьцтугыекыщпбаьуошуфьхя
нкщцаеещфщфатфзэьиуршхфуыппкщгкянсккаршижызймбаэекчьпкшквуфэбенгкомбатнппцаабсыа
ицьатнфьфызтжкигшкибшпыхжяиьифгмпвахжжкщфэгдычгенмтгшйзхййьркхйэеянщььеяьэежбищя
зхйймбаьфпщвоаибшуахжптпхызхйнфмщйтсжвехйщцэзыжзкргжтнйцбфдесаоещфзыкпжффеккям
кщошенпбккдзюпссмпрбккеатнпхбшкпхжкпащнеэфаыссятиускшкдзянуадеекчыппкшквуфэбенгкюу
щпирщцазижбоэенфьипхвкргжтнйцянаигшдензлзйзкдщеышпымпзкщфнфккмктжшмбатнйжиуггх
ффеюищпкшаивкреееяежусснеекмибскпяощктглюхжящяюхжфгбамлкиомбатнппсдуфиеущсыэеекз
айцдзкщиуьихфижфгзыбееквыязцукинбеньеймвфрьхйдзехызмкбфдзэзыжужвещтужспжувгсылщд
еюищцнкбщвфснусьияцспжувгшмшюдзекринтакцаржсынедеяячпнмьижздеюибареижьщьесикпн
юрилбккуихжчжшмыдуфьетнужчгсдэщуфршхфижтнкиекрбгжсыииьигшбаофеибшбагнйжжксигшьб
ккяпсрцахжящчксжсыщдуфщфнфэьмбьфгкхичгрбетяьчгуфвттжшмбатнйжзохкянфггкшезгяеьбджпх
санфьихфчшкпвкоюбаоещфдюйжящвеоищезохкржйцэзыжзкдзиждьмкдзуфгдуфьхошгннзышккпщ
акыплмгнпбьблзотяячпчкьыьишжешэкжеекцшутйкззкыяцшфхьржзыиуйзлфчшщцижэкмибшкщгки
злзййеквзекцнцмцьмеяйхфзоиьывуфэбенгкчглюмпкщчжфгхтгрмдужфеыжйедзянуадеекшуьпкинб
йзепьияерфуфьфщфхзгхиажшпхвбвеощвзэкьедепуьпфемкакдгчьнйдзяпбшексчьщенсасдэейфлряц
щзьххйжайещфнтижгнмкегшмтнлюыденбаэищьиштфхгфгдзцыгжщакеззхбгнбшшаенхкэонгэщчечг
щпужгнэщбдшжваць йфэфнеегинлюфзэкхйэнэиютлфэкофэзхитфокфзюибахещакомкекдиэщппштее
ыаиусесщлььеекппкшквуфэбенгкзкремкхщнфблатншьищьикязшеижнфаибшкщвзуфакзгвеюикщгкк
июудьмкййдзофдекиуажшкпцаэесщппяаоеиеяпьукщхйрбэьйфзхзглювампквуфкиомбатнппаисдйм
вгьфрещфэьчндыдкофйкиемкоюхщймфвуфщфэезхтшужнфгыгфижуаппцаппяиафижуаппцашжшузг
кщвзэкшкцнащатршхфтжкидыкщвзужйьпыхфщфхшкпхжйвуфщзипхдшжжыинчгфгйфзикщрфвелбвг
эисащмдзмкдзцкдбужгнщтсмуашюыньияержкщппяитнэщянкщднэиьихфсазхшрблчягнюленшкаию
лршппкщшулбршнещсйтцахеьебурнбецаязцчдевеутльцчсалбршутйкамкщошенижфеюитыянсдаид
ыиждьярвыуфжещзшкубйжкеьхмкянцагнжецчйуенипцьнеуффпаиьщуфяйрфязкдкпбатгэщрфяйрфя
зпайеюишмсыаиащдндкспуахфрфчздшкосещфкиомбатнппчгфгйцкиекьщхйхщймфзвзшиодаимпаи
вфпдьщыикцнеяйпхюдкпбатгппщдееймкиужфзежщевтдзиждьгтьализжпбгжсыщдуфнфмиэивыбсу
жжшгкищхежииуйюбшаиижыздзазяйижнфызекчккиофязжефжыдуфкийфжеыщнелзхйязрфобвглю
мпоегьюяаияьдшзкссспжзкыщьдзмзищднйедзащппяидкгжижшбппгшршккпщлилбкиьщнкекязакс

бтнусьияцуфгхиуяюэихвгккжщпцгиуенипяосскпшжлбгннюдыьийжпзьглзоуьиомоехфкжбаоеофйкй
иужофуфвттжиуьиомоеотжеофязщзещнфдиьщофзфйикщхйдмршцмбатнпппкшквуфэбенгкйрьщн
хшуьиомоеекижщмбатнппаинбьфгкздуфхщужфгаишуьпкичгшмршкпяищечфихыищеиееквщьидкяз
шицагнгкййхщужфгрбккнеайшивыпкзохкржйцэзыжзкжфязехызмктжбаоедзеегжижшбдеекбшршкк
пщйуьпьбкщнхоищцеелбтнусьияеюуьщянгнвапхфнцшурюувгшепущпирьигшкпяоуфнкбфзмбатнпп
чфекьебпщдееофбныцэеуыгньщрфвелбйцвтндуфвзшивыбсужжшгкэиясьиэеязрфмиюуошэуенипы
цодкпбатгязцуьиомоехггжтнкцофязщзхтжеоегьэыщфятрфуфьфвтгжфзещянуабшмкнфижящдыдзоф
декишжфгйцшеэффезюфггжтнтыьхллгжхфяноюдзызмкепэщхйшжфгбайцьщхйуфяйрфршаиииееквщ
ьиоеийгхшуьпппшчфггжтнкехщймфзьщхйнфзфиеюикщгкянзыщпршмлщфатфзэьикрфуффхшфзфие
юисыхфщфьхэфянзквбгнхжтнбздешщэицнкпшчлмьигнмпбаиямкбеяйгшэжэиуфхщднэщыиьбвефзю
икещфатфзеоэеязаквбгнхжтниивгфгшеэффеязиубсяощкщещфащбньихфюуьщрффхижхфязчещфиуб
смпьфижбаэыщфятажшсэяехивыэеуфяйрфхщбшиуьфнеьемкхфцаоеязшеижызшеэффешезгяержпп
шчюлгжчкнфрлбэмпащящбнсыхфижбощфатфзэьгжязехызярймкщифугсыэижфызекзайцзгдыаивфа
тншмпквмтоюмкжижозгьфсикщхйцскпмпшжщпцгвфоишмскдзиждкызмкдзуфгдуфьхиубсыегхьмк
щошенцфижуацаоюмкжищеэежффекктгоеиеиузаппгжбнджыдуфкиижэибашжйьнфспуасайцзгэщк
щвзэкгуыбккоеиеяжьупаенгкутспуахфрфчздшкосещфащбаужвьййишьиясхфзфихыитышжтфвегкяз
шкрбйзсжчгдыащдыьхфеещнфцайцзгфггжтнмлршхфржршбакпиусшбалщеещфзфиждьекзавфятеее
пьищьнфййчзрщдыцьбфяймзямутзбмпкшщцрфуфйзббкщнфвыафкнсыхфвтрфмкшеижжтгжхфцклз
ййяшутйкйгфгаыищкщуфапдкгпкшщцэежелзярблекшкйзекнфмилиаиэщмтэзьейпхзшэкжеекмичфб
фьфекьеяйхфщфлзбеэьекянжшккпщьиомнеьхуфекьхэфекпзьглзриомкщошенрирбетяьекиееквщьи
эибскпяощкщжщпцгвфоишмскхзйфщфатсеижфеюишмкидкбфяйнкзшяьоегьзхщфхкошбащпящтаяц
ожйцвтыийцнфнехевебныэцаяощкбщчкхевезтнхызеэблйьаидномрфуффхтгйркпрбккспуахфдгызы
жинймкщошензафеййчзсишмсыйфзииуьпьтабужхавзрфгдуфэегхяпзыиуйуьпбацнцмйеюнвыифхкю
исскпцьуфяйрфофьеэьхйжайещфзхщфоишмьбщпбсьищьпхпдьщшмлзмзещрщяячпвыщзожйзабьфг
кхичгсыймьбкщдещзожйзбжфещсфзцдуфэезыщеыичгфгшмсыэеекифркказьщыисыянбшреьеуфяйр
фюпйжшмыдуфьхоюиензхйгжфеыщтаьихфижзкцмршшжнмкщошенкшутщфгскпяощкэбккиувеижц
ащмршгфснюэмпдзоегьхизыэияещфатфзэькнсырфбнсдхжкщдыйедзтжкидытготумкщошеняифгэии
иьщофккмкбнсдмпхщбаужлтфзэьрщшузакношжкзхехызриьщшмлзмзеэблйьдзятзпжкьевбвглювац
ьтжвфммгжбаьххйжеыжнфыфкэщцофяйехднужяцянкщуфзхянжрцампоеиереншошжтбщбаужбаца
гжатыщтаяеюнлмбабшаибавереюийеофзфркйюэщнфьагнотдщхтеуцюдзвдуфьехеэйэерфишьуошу
жгжязщзхйвыщдужфеыжкцэеазрихфхщлбьбгшмпйьдзсплюлмкщошеныфхьудьипхфньугжйцрьнхт
шяьуфщфтжиусшкщгквибжешуахфжелзюийцмемкиубшнтщфатфзэьбсьщуфшеюиршвглювампянуаг
жпкмкэеянуагжяахфпйзхижшбцаеещфсиьищьжшяьржшмьбккнфхкгущпщеппзыьищецкяйпхвкабйз
феюпцакежфязщзьеяйижызхщкпкшквуфэбенгкппбаппинжумкбньщнхбкпхцаржсыэфепьизкяпбшпп
шжщпцгшюэинбйзепьияещязобейзузгщрфуыппкщгкшжщпцгыдуфщзреазмктжтязобеьфснхжппйьн
фоиищуфьфотязпаоержгжутыисайедзоедеекбзкызкдзбкдзэфятхйожясьщуфьфотвзкдуфщфатфзеоь
екжутоищеьхэфоффегибжюещфышутттдщвехкэеьбвенедеюикщгкофэфжеекббккцмьфнзеэщцоеэй
йюхфдфэзпикщгкянжшуауаеегаоевткщиуьихфднсабспхнленфгьегщвехкржшмбаблэьаидномхзйфзо
ркмщуфэгхффеекфнлюмкщимлнфвюveекукктхщтаянинлюхфжпвыьихфижцаоелвгкрпшчржуакщжы
цьхзчзоущпирцьэзыжщьзонемиэийжмлмкщитызкцжгньщдырбккфзызлзбфяйцттюнббжэихфижжк
цыбжхфижцфкэвыошкпагфгйцьхекофоизымпйьнфянкщнтпнйцржблднбжэемитффжутркфеседзябв
езищцьейфэбгнкпужмпдзхфжтлкжаскисяснзеквыщзспсрмпоюхжвычьмкзгвеюияеабтнсэяещфэфхз
оюхщылржблэзыжяцожкщдыйеюнвыигфгшияюездшвеэбккылмпязкызкзфснмпэщюесершдзнепьв
зббенгкриодаиуамзббршекчзхйжайцщфэфщвуфьхлзэзыжщьзонемщвзфхйнлюпыпхпмкщошенижф
еюивфихыимлртреярблэейзщшкпкьекршхфщфоюянгжцатнмдюэблсиьияцгжепмдьихфофцыгжвехй
дзхщмдуфнелзэфййянйрвзиеспуахфдгызыжинткиуятчзхйчнбшижызпамлршпкювуфмитфянбшкпьи
хфижаигндршжкпяикщгкщззтвзюикщгкащлзбфижппкшквуфэбенгкомбатнппзкятчзмктжбаоеятгийе
янскрлршшжянвквтсеижфеюивфмбккатыщтащьщфатфзэьжайеюитыеатнсыянжзкыктжбаеншкфбгн
ьиьщьихжэитфянбшкпьидзбтяпбадзчкрфдешпеэцьйьмзугкщхйгжхфееекдггжтнцьошиудзянжшнфв
ехфюнбшдзызкызктжшмкщошендиясхфузгщтабахжезэешбйзепйжхайцзгсытжйехкющтаьипхгамлр

шоюржшмьбщпбсьищььщхйгжйюэмкщошенрщймршнфьфшкщзкызктжвфоиьбккатыщтаяещфатфз
эьэзйзмкдтужрьхйнейьфжлщвднфмщязотзимлюпифиеабмдьищьймщпсдхфкуйюьбэщхфижсдуфхзг
хэбэфшфмикийюуаащзыкцспуахфрфчздшкощккуошужхтгрьщдышмщпщдеещфхфжаяюэихфщфяна
щбжижэквыцалзижбощфатфзэьожкщдыйеюнвыигфгшияюездшвегсппиещшкпнбккцнащоенкюгба
щфатфзгщтаьипхмщтгвевзэйьхяряцршекшквмлзхимлянбшижуашжкпщцржйцэзыжзкдзюкхзумкщо
шенфбащжывггжтнйезфспэщппащпбршюкхзхйпзлзееэкенфгшесажбащжыевуфвбщпнювьййфзюит
ывыафкмкщошенббшюнфдееквыйзпщясфзхйиуиусетлршбшкпкиофтжшжкпяискофябвеюпшмсыэе
иушфхкйфижжшяьщфатфзэьнфршсрсашжцгнфмиьиенршхщуфмкмеянбшлзизумкщошеныфижуаш
жхайцзгвфятееепьияещфатфзвесиенршдкнфвюызектгэевтюпяююэшжгфьешеижызуфхзйфьиэщрфя
йрфкиьбьфоюфенехфьхэфмкщитыянащбжижэквыщфатфзэьэыкщпатфятееепьияедзьффзрфуфьфшу
ьпшмлзхийцянсдаийцуфщсьщтаенкщцкюуьпьбвеощвзепьишмкщошенлкянаийжскйгфгянбшэфишя
ькщвзепьищьеншкжз

The length of key = 16

Your key is: братьякарамазовы

Дешифрованный:
князьандрейприехалвглавнуюквартируармиивконцеиюнявойскапервойармиитойприкоторойнахо
дилсягосударьбылирасположенывукрепленномлагереудриссывойскаторойармииотступалистрем
ясьсоединитьсяспервойармиейоткоторойкакговорилионибылиотрезаныбольшимисиламифранцуз
оввсебылинедовольныобщимходомвоенныхделврусскойармиинообопасностинашествияврусские
губерниниктоинедумалниктоинепредполагалчтобывойнамоглабытьперенесенадалеезападныхп
ольскихгубернийкнязьандрейнашелбарклаядетолликкоторомуонбылназначеннаберегудриссытак
какнебылониодногобольшогоселаилиместечкавокрестностяхлагерятовсеогромноеколичествогене
раловипридворныхбывшихприармиирасполагалосьвокружностидесятиверстполучшимдомамдере
веньпосюипотусторонурекибарклайдетоллистоялвчетырехверстахотгосударяонсухоихолодноприн
ялболконскогоисказалсвоимнемецкимвыговоромчтоондоложитонемгосударюдляопределенияем
уназначенияапокаместпроситегосостоятьприегоштабеанатолякурагинакоторогокнязьандрейнадея
лсянайтивармиинебылоздесьонбылвпетербургеиэтоизвестиебылоприятноболконскомуинтересце
нтрапроизводящейсяогромнойвойнызанялкнязяандреяионрадбылнанекотороевремяосвободитьс
яотраздражениякотороепроизводилавнеммысльокурагиневпродолжениепервыхчетыреднейвов
ремякоторыхоннебылникудатребуемкнязьандрейобездилвесьукрепленныйлагерьиспомощьюсво
ихзнанийиразговоровссведущимилюдьмистаралсясоставитьсебеонемопределенноепонятиеново
просотомвыгоденилиневыгоденэтотлагерьосталсянерешеннымдлякнязяандреяонужеуспелвывест
иизсвоеговоенногоопытатоубеждениечтоввоенномделеничегонезначатсамыеглубокомысленноо
бдуманныепланыкаконвиделэтоваустерлицкомпоходечтовсезависитоттогокакотвечаютнанеожид
анныеинемогущиебытьпредвиденнымидействиянеприятелячтовсезависитоттогокакикемведетсяв
седелодлятогочтобыуяснитьсебеэтотпоследнийвопроскнязьандрейпользуясьсвоимположениемиз
накомствамистаралсявникнутьвхарактеруправленияармиейлиципартийучаствовавшихвономивыв
елдлясебяследующеепонятиеоположенииделкогдаещегосударьбылввильнеармиябыларазделена
натроеяармиянаходиласьподначальствомбарклаядетоллияподначальствомбагратионаяподначаль
ствомтормасовагосударьнаходилсяприпервойармиинаневкачествеглавнокомандующеговприказе
небылосказаночтогосударьбудеткомандоватьсказанотолькочтогосударьбудетприармиикрометого
пригосудареличнонебылоштабаглавнокомандующегоабылштабимператорскойглавнойквартирып
ринембылначальникимператорскогоштабагенералквартирмейстеркнязьволконскийгенералыфлиг
ельадютантыдипломатическиечиновникиибольшоеколичествоиностранцевнонебылоштабаармии
крометогобездолжностипригосударенаходилисьаракчеевбывшийвоенныйминистрграфбенигсенп
очинустаршийизгенераловвеликийкнязьцесаревичконстантинпавловичграфрумянцевканцлерште
йнбывшийпрусскийминистрармфельдшведскийгенералпфульглавныйсоставительпланакампанииг
енераладютантпаулучисардинскийвыходецвольцогенимногиедругиехотяэтилицаинаходилисьбезв

оенныхдолжностейприармиинопосвоемуположениюимеливлияниеичастокорпусныйначальникид
ажеглавнокомандующийнезналвкачествечегоспрашиваетилисоветуеттоилидругоебенигсениливел
икийкнязьилиаракчеевиликнязьволконскийинезналотеголилицаилиотгосударяистекаеттакоетопр
иказаниевформесоветаинужноилиненужноисполнятьегоноэтобылавнешняяобстановкасуществен
ныйжесмыслприсутствиягосударяивсехэтихлицспридворнойточкиавприсутствииигосударявседела
ютсяпридворнымивсембылясенонбылследующийгосударьнепринималнасебязванияглавнокоман
дующегонораспоряжалсявсемиармиямилюдиокружавшиеегобылиегопомощникиаракчеевбылвер
ныйисполнительблюстительпорядкаителохранительгосударябенигсенбылпомещиквиленскойгубе
рниикоторыйкакбудтоделалкраяавсущностибылхорошийгенералполезныйдлясоветаидлятогочтоб
ыиметьеговсегданаготовенасменубарклаявеликийкнязьбылтутпотомучтоэтобылоемуугоднобывш
ийминистрштейнбылтутпотомучтоонбылполезендлясоветаипотомучтоимператоралександрвысок
оценилеголичныекачестваармфельдбылзлойненавистникнаполеонаигенералуверенныйвсебечтои
меловсегдавлияниенаалександрапаулучибылтутпотомучтоонбылсмелирешителенвречахгенерала
дютантыбылитутпотомучтоонивездебылигдегосударьинаконецглавноепфульбылтутпотомучтоонс
оставивпланвойныпротивнаполеонаизаставивалександраповеритьвцелесообразностьэтогопланар
уководилвсемделомвойныприпфулебылвольцогенпередававшиймыслипфулявболеедоступнойфо
рмечемсампфульрезкийсамоуверенныйдопрезренияковсемукабинетныйтеоретиккромеэтихпоим
енованныхлицрусскихиииностранныхвособенностиииностранцевкоторыессмелостьюсвойственнойл
юдямвдеятельностисредичужойсредыкаждыйденьпредлагалиновыенеожиданныемыслибылоещ
емноголицвторостепенныхнаходившихсяприармиипотомучтотутбылиихпринципалывчислевсехм
ыслейиголосоввэтомогромномбеспокойномблестящемигордоммирекнязьандрейвиделследующи
еболеерезкиеподразделениянаправленийипартийперваяпартиябылапфульиегопоследователитео
ретикивойныверящиевточтоестьнаукавойныичтовэтойнаукеестьсвоинеизменныезаконызаконыоб
лическогодвиженияобходаитппфульипоследователиеготребовалиотступлениявглубьстраныотступ
ленияпоточнымзаконампредписаннымммнимойтеориейвойныивовсякомотступленииотэтойтеории
виделитольковарварствонеобразованностьилизлонамеренностькэтойпартиипринадлежалинемец
киепринцывольцогенвинцингеродеидругиепреимущественнонемцывтораяпартиябылапротивупо
ложнаяпервойкакивсегдабываетприоднойкрайностибылипредставителидругойкрайностилюдиэто
йпартиибылитекоторыеещесвильнытребовалинаступлениявпольшуисвободыотвсякихвпередсоста
вленныхплановкрометогочтопредставителиэтойпартиибылипредставителисмелыхдействийонивм
естестемибылипредставителяминациональностивследствиечегостановилисьещеодностороннеевс
пореэтибылирусскиебагратионначинавшийвозвышатьсяермоловидругиевэтовремябылараспростр
аненаизвестнаяшуткаермоловабудтобыпросившегогосударяободноймилостипроизводстваеговне
мцылюдиэтойпартииговориливспоминаясуворовачтонадонедуматьненакалыватьиголкамикартуа
дратьсябитьнеприятеляневпускатьеговроссиюинедаватьунывательвойскуктретьейпартиикоторойбо
леевсегоимелдовериягосударьпринадлежалипридворныеделателисделокмеждуобоиминаправле
ниямилюдиэтойпартиибольшейчастьюневоенныеиккоторойпринадлежаларакчеевдумалиговори
личтоговорятобыкновеннолюдинеимеющиеубеждениножелающиеказатьсязатаковыхониговори
личтобезсомнениявойнаособенностакимгениемкакбонапартеегоопятьназывалибонапартетребует
глубокомысленнейшихсоображенийглубокогознаниянаукиивэтомделепфульгениаленновместесте
мнельзянепризнатьтогочтотеоретикичастоодносторонниипотомуненадовполнедоверятьимнадоп
рислушиватьсяиктомучтоговорятпротивникипфуляиктомучтоговорятлюдипрактическиеопытныевв
оенномделеиизовсеговзятьсреднеелюдиэтойпартиинастоялинатомчтобыудержавдрисскийлагерь
попланупфуляизменитьдвижениядругихармийхотяэтимобразомдействийнедостигаласьнитанидру
гаяцельнолюдямэтойпартииказалосьтаклучшечетвертоенаправлениебылонаправлениекоторогоса
мымвиднымпредставителембылвеликийкнязьнаследникцесаревичнемогшийзабытьсвоегоаустерл
ицкогоразочарованиягдеонкакнасмотрвыехалпередгвардиеювкаскеиколетерассчитываямолодецк
ираздавитьфранцузовипопавнеожиданновпервуюлинииюнасилуушелвобщемсмятениилюдиэтойпа
ртииимеливсвоихсужденияхикачествоинедостатокискренностионибоялисьнаполеонавиделивнем
силувсебеслабостьипрямовысказывалиэтоониговорилиничегокромегорясрамаипогибелиизвсегоэ

тогоневыйдетвотмыоставиливильнуоставиливитебскоставимидриссуодночтонамостаетсяумногос
делатьэтозаключитьмирикакможноскореепоканевыгналинасизпетербургавоззрениеэтосильнорас
пространенноеввысшихсферахармиинаходилосебеподдержкуивпетербургеивканцлерерумянцеве
подругимгосударственнымпричинамстоявшемтожезамирпятыебылиприверженцыбарклаядетолл
инестолькокакчеловекаскольккокаквоенногоминистраиглавнокомандующегоониговориликакойон
ниестьвсегдатакначиналиноончестныйдельныйчеловекилучшеегонетдайтеемунастоящуювластьп
отомучтовойнанеможетидтиуспешнобезединстваначальствованияионпокажетточтоонможетсдела
тькаконпоказалсебявфинляндииежелиармиянашаустроенаисильнаиотступиладодриссынепонесш
иникакихпораженийтомыобязаныэтимтолькобарклаюежелитеперьзаменятбарклаябенигсеномтов
сепогибнетпотомучтобенигсенужепоказалсвоюнеспособностьвгодуговорилилюдиэтойпартиишест
ыебенигсенистыговорилинапротивчтовсетакинебылоникогодельнееиопытнеебенигсенаикакниве
ртисьвсетакипридешькнемуилюдиэтойпартиидоказываличтовсенашеотступлениедодриссыбылоп
остыднейшеепоражениеибеспрерывныйрядошибокчембольшенаделаютошибокговорилионитем
лучшепокрайнеймерескореепоймутчтотакнеможетидтиануженнекакойнибудьбарклайачеловекка
кбенигсенкоторыйпоказалужесебявмгодукоторомуотдалсправедливостьсамнаполеонитакойчелов
екзакоторымбыохотнопризнаваливластьитаковойестьтолькоодинбенигсенседьмыебылилицакото
рыевсегдаестьвособенностипримолодыхгосударяхикоторыхособенномногобылоприимператореа
лександрелицагенераловифлигельадютантовстрастнопреданныегосударюнекакимператорунокак
человекаобожающиеегоискренноибескорыстнокакегообожалростоввмгодуивидящиевнемнетоль
ковседобродетелиноивсекачествачеловеческиеэтилицахотяивосхищалисьскромностьюгосударяот
казывавшегосяоткомандованиявойскаминоосуждалиэтуизлишнююскромностьижелалитолькоодн
огоинастаивалинатомчтобыобожаемыйгосударьоставивизлишнеенедовериексебеобявилоткрыто
чтоонстановитсявоглавевойскасоставилбыприсебештабквартируглавнокомандующегоисоветуясьг
денужносопытнымитеоретикамиипрактикамисамбывелсвоивойскакоторыходноэтодовелобыдов
ысшегосостояниявоодушевлениявосьмаясамаябольшаягруппалюдейкотораяпосвоемуогромномук
оличествуотносиласькдругимкаккмусостоялаизлюдейнежелавшихнимиранивойнынинаступательн
ыхдвиженийниоборонительноголагерянипридриссенигдебытонибылонибарклаянигосударянипфу
лянибенигсенаножелающихтолькоодногоисамогосущественногонаибольшихдлясебявыгодиудово
льствийвтоймутнойводеперекрещивающихсяиперепутывающихсяинтригкоторыекишелиприглавн
ойквартирегосударяввесьмамногомможнобылоуспетьвтакомчтонемыслимобыбыловдругоевремя
одиннежелаятолькопотерятьсвоеговыгодногоположениянынчесоглашалсяспфулемзавтраспротив
никомегопослезавтраутверждалчтонеимеетникакогомненияобизвестномпредметететолькодлятогоч
тобыизбежатьответственностииугодитьгосударюдругойжелающийприобрестивыгодыобращалнас
ебявниманиегосударягромкокричатосамоеначтонамекнулгосударьнаканунеспориликричалвсовет
еударяясебявгрудьивызываянесоглашающихсянадуэльитемпоказываячтоонготовбытьжертвоюоб
щейпользытретийпростовыпрашивалсебемеждудвухсоветовивотсутствиевраговединовременноеп
особиезасвоювернуюслужбузнаячтотеперьнекогдабудетотказатьемучетвертыйнечаянновсепопад
алсянаглазагосударюотягченныйработойпятыйдлятогочтобыдостигнутьдавножеланнойцелиобеда
угосударяожесточеннодоказывалправотуилинеправотувновьвыступившегомненияидляэтогоприво
дилболееилименеесильныеисправедливыедоказательствавселюдиэтойпартииловилирубликрест
ычиныивэтомловленииследилитолькозанаправлениемфлюгерацарскоймилостиитолькочтозамеча
личтофлюгеробратилсяводнусторонукаквсеэтотрутневоенаселениеармииначиналодутьвтужестор
онутакчтогосударютемтруднеебылоповернутьеговдругуюсрединеопределенностиположенияприу
грожающейсерьезнойопасностипридававшейвсемуособеннотревожныйхарактерсредиэтоговихря
интригсамолюбийстолкновенийразличныхвоззренийичувствприразноплеменностивсехэтихлицэта
восьмаясамаябольшаяпартиялюдейнанятыхличнымиинтересамипридавалабольшуюзапутанность
исмутностьобщемуделукакойбыниподнималсявопросаужройэтихтрутнейнеоттрубивещенадпреж
нейтемойперелеталнановуюисвоимжужжаниемзаглушализатемнялискренниеспорящиеголосаизв
сехэтихпартийвтосамоевремякаккнязьандрейприехалкармиисобраласьещеоднадевятаяпартиянач
инавшаяподниматьсвойголосэтобылапартиялюдейстарыхразумныхгосударственноопытныхиумев

шихнеразделяяниодногоизпротиворечащихмнений отвлеченнопосмотретьнавсечтоделалосьприш табеглавнойквартирыиобдуматьсредстваквыходуизэтойнеопределенностинерешительностизапут анностиислабостилюдиэтойпартииговорилиидумаличтовседурноепроисходитпреимущественноот присутствиягосударясвоеннымдворомприармииичтовармиюперенесенатанеопределеннаяусловна яиколеблющаясяшаткостьотношенийкотораяудобнапридвореновреднавармииичтогосударюнужно царствоватьанеуправлятьвойскомчтоединственныйвыходизэтогоположенияестьотездгосударясег одворомизармииичтоодноприсутствиегосударяпарализуетпятьдесяттысячвойсканужныхдляобеспе чениягеголичнойбезопасностичтосамыйплохойнонезависимыйглавнокомандующийбудетлучшеса моголучшегоносвязанногоприсутствиемивластьюгосударявтосамоевремякаккнязьандрейжилбезд елапридриссешишковгосударственныйсекретарьбывшийоднимизглавныхпредставителейэтойпар тиинаписалгосударюписьмокотороесогласилисьподписатьбалашевиаракчееввписьмеэтомпользуя сьданнымемуотгосударяпозволениемрассуждатьобобщемходеделонпочтительноиподпредлогом необходимостидлягосударявоодушевитьквойненародвстолицепредлагалгосударюоставитьвойско одушевлениегосударемнародаивоззваниекнемудлязащитыотечественатосамоенасколькоонопроизв еденобылоличнымприсутствиемгосударявмосквеодушевлениенародакотороебылоглавнойпричи нойторжествароссиибылопредставленогосударюипринятоимкакпредлогдляоставленияармиа

Ентропія: 4.449018063018637

Ключ: k= (725, 100)

Висновок:

Після виконання даної роботи ми отримали навички з розшифровування текстів, зашифрованих афінною підстановкою біграм, з програмування автоматичного розпізнавача російської мови та з частотного аналізу на прикладі розкриття моноалфавітної підстановки.