Криптоаналіз афінної біграмної підстановки

Мета роботи

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

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого 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

П'ять найчастіших біграм ШТ.

	1	2	3	4	5
Біграми з перетином	ыу	юк	як	ып	ую
Біграми без перетину	ыу	як	юк	ып	оу

П'ять найчастіших біграм для російської мови.

	1	2	3	4	5
Біграми з перетином (обчислено програмою)	то	ст	ко	ов	на
Біграми без перетину (обчислено програмою)	то	ст	ко	ов	на
Біграми статистичні дані	ст	но	то	на	ен

Список можливих ключей

(630, 583) (419, 258) (349, 929)

(955, 475) (567, 823) (424, 500)

(335, 475) (133, 699) (542, 577)

(626, 360) (16, 174) (612, 867)

(394, 12) (828, 136) (945, 661)

Для автоматичного розпізнавача російської мови було взято за основу перевірку частот частих літер, а саме перевірялися літери, що зустрічаються часто, або літери, що зустрічаються рідко. Найчастіше використовуваними літерами російської мови є літери «о», «а», «е», а найбільш рідкісними вважаються літери «ф», «щ», «ъ». Було вирішено, що у тексті сумарно потрібно не менше чотирьох або більше співпадінь для перших трьої літер, що зустрічаються, та трьої літер, що зустрічаються найрідше, при цьому порядок літер не враховується. Тобто для аналізу беремо найчастіші три букви тексту і рахуємо кількість букв, що відповідають «о», «а», «е», ту ж саму дію виконуємо для найрідших. Таким чином кількість співпадінь повнно бути чотири, або більше для змістовного тексту.

Даний варіант є досить точним і його точність може зростати з ростом розмірів тексту. На практиці було досліджено, що у незмістовному тексті співпадінь як правило сумарно не більше 2.

Шифрований текст (варіант 15)

цсбтызнэжрцяфьзюдрцубуысьцыуюкнажфтпдрчядьдйлдаьпуяксщфтэаытыпдрвщядшрщфтпдйюябуцуйрдуврйдмузеуйиьую
еочшлукчэйлдаьпуякгуяклтафвкежнспйиьяршцчтыпйэуюуйрудтшкдрлфюоцуэрьккдлцчтыпйэйифюькьтрэуйюкйирцыусн
пйюкчтфбиььтйюйфьснэщпокмлерхфбукюуйюкйирцыуьулямпякврбюгиэпязякыддфбузиснррщушрвщчкчйлдаьзннфьуокю
чкпззнюеьтпфцубуысьцыуснмуужзнгнечмспутюыыокдцыуцятыююаршрпсгнщухцчтыпйэкдсknфпфыусюдриэюкбяйицютауа
усцятыююгипалфтпыплтгнзрноьуеряюгиосфйьтсожвзиэпязмуйецюгнкдярдуююыфыуруцаырзпнщчкпуцубтежуюякыдыкээ
зижуякзоьсжинщэыокчтьюязлщяыайсрщюязцятыююпфзсьунчфаькиоурдумфпфдумсмфпфдумсшпжрбюжрзгыускеуноидэрнч
пудсмрфацябцпузйлдаьпуякнфпфыухтбстанржфпфыушкоеядтючоцящперйдэрнчпуякапжрбюязытбжгньсоуядфяпфыумсфй
чкхплтпйьтррнкнщядшрщфтпуйпферцуздцячььттдкфлагсечпймпдутяиьнэйиьулэипоуыурущуцашроуфдвьыплтяфйдияцю
йицяфюшкгиюкнрьсжуыдруякыпшьчтлтиоидтящщчтгимузягифдынбэюкбякейипфоулфщсяыкдоуснуюгмпсгнррнэьтрэцюмэ

юкбяшзгнщттщзикаыдтджиыуыдысодесьулцфюуюзнесфюфцлтуфтпйикэюкбяшзгнцьыпьтуюэпжри
жаышчбпьуытфьрршпсрыо
жечьсуоцсвшпжспчфдисаьйигюшлчьштзрыуыдьсдиокюяфюокдцыунрядлдрфчябсыдгкиодашржлб
жнсбкуйбяющарбацядрчд
ечмущушузяиьыпокфсыфьуоуыкуфцдысоуэячьыкчтызусцджгзсжспчфдьсоуяддсфйчкхплтяклдыцы
уэуюотпхпмфзсзерсжк
язвяфьхпоуыурушупутяиьщпзрноюклфызгсэргфоузйккзюфбожштцдзкжлрсфймэязпуцюпалфтпыпл
тбкбязюрспсьуаьпуця
хьькиоуйшкапякайыкапыуыубалжаыьсвяафякругфтпщиосьуцямперьсдихьчтнайрцдесайлдцтушясз
фжулдесфючяиещинф
эпэыдинфнщфрякбудфчшлукчффцюоснщювзюдрьрппмгыугндуяклдпююкчаюювыдйккзюрсцююкв
ргдхюдйнфнищиокюяжльтчь
знесдтафссйрнэзисйнфнищифюфцфюмпйсесиокэцюгдомзинфзафдгцщпчоюкйиоуйьхубющиюяуюц
ядрчдечжечьсуюйьтрцшт
жспчфдруююблиэюкбявлаывродпсзееуьущуьппркдцдйсощьтоущфщсесюкйибкпфыдхчждтанрьцюя
яыцуьйюкйирцыуяксяшз
аюэыьюмфкеядзрхгыужспчщукебяусдупфоушщштцюкэьтчобуырзпвлжибжлтоугндуьуэртоечаыму
фдкдцдеаоуыучакуеттщ
штлунчярлфелаызргчщпыпыуинэущфэпжрюеыфсянэязыупэаысрьспжлтчтюкйибкжрцурргндуцяйг
ыуийюкйирцыуцюгньуйд
идкгыубалулэцюнэйирцыужулфжиррцдйдищьтцмчойрякеячьякбучюзивцыусжчтгуеттщыккдцдеаы
ущушрыулускнффсмрйя
тысрярьскфхиафзячьпуцуюкндесцагацюоуерждофсюрйуйруссечиопсбукйыфнцыутамсздечкдцдеар
рврякязпугакйчьтм
псфдррэянйысутнфеузяежуюеопфцювуващдьсурфюкэьтпзуйшкйустфжштпуврчюязыуцушрцуздцю
ьулаустйнфнийиокюясй
нфмпярскпзпуюктякхбсжспчщункмамрчсдузежрчдечцюдйнфлтфцыусжчтфюкэьтпзррцядрнрзсррб
уцчьржфэыиьчтокыпсс
ьршчрйязнржфщудугэбслфрйязуакййияяцелдакээытющцдепврысофдиыкуюрэнсцдбьнщысцдепзрз
ееупизюхпйшьцыулфхь
ькдашржлбжюяиьлщкеэащужогккщойысяытдгфызгдхжгршрпсуннрэуйрзчшьчтокниуюлслфтпжрзр
ьргфтпцюмфгдякзнесжс
бдядтякхфюойнфнилгыуьунргфтпыплтцюзюкэьтчогюзенщфтыушыиямпшзкийфтйпфсрцфтпуюпуя
ккэюкбяшзьуйденыдерба
бкнщфтчььтйююкрйюяыььтйюнщфтжрчдечмфпсррбужфцдиэккыпюкванэьуйрбакдмугндуелокйуб
юяыкдхюыпйфхдомнфчйпф
ернщфьхужпчтчтпффьядечзрруцуфдьфиьмппурряышрбюкерсяклдпювыдуцушрсрэббсврвюипйспч
кдюыснербюйишрсрэбфь
йиязнщцпштядэяямпрядпрльуюнфыпхуяклтионяпфыуыдсйысярщмзиврйрруткыпсяявщибкуйчьцрт
пюкванэдрнроьйиязйд
аюыкчаююрсяклдбюнщфтжрбауафдечбкеуцафьькфюйаяюцрзсьмцджбкжрбапфнщуюпуфюэрсрчю
нщфтуйруаыврнретгучщдь
ькэяюкесякинштсйьтрцыкзюцаидьуытфььсжизюшпинйдаюнфчязюпугндууафдечбкеуикээкафьькрр
цячьмптякхцеьтфлып

нэйиккруаэыфмплдюндэюкбявльунчнээзтякхыухеыплтгюзерсоуыуиншяпфыутюдйсялщштбкуйруздякидуниоусйдаюфюрй
цюшкпуйдиддупчбкнщяыррцутанрфкюкждлэюкбяшзюабдинмуужзнгнпсздечхдбюрйшдаьубоуппжсхазтзющиздыдомзиждоф
буызхдбюкщбячунулфоушумыкдгцыукдмуелокфсугыуцукфпуцуэуруярцуеслдхаздыугаздйьшпощфтыпаьбясйккзюфбфцюя
яыррнрчшшнярдукйыфуеыфсячкыпсяявфюькьтрэуйуйьтхапусйнщыссднрздпснщфьруякыпыфыущпйсгфцудушньучащйчьжс
нэостялтхьврбаенщсырпсгпшлбядймфуюьсоуэяпфыупйжобдэксрхдйдкипзбяйижджушнийлознвутсуринйдгдпснщьсфдпс
каруьспсруякыпафьтздунчяькркрцуяфйдияцюцрфрлдфэфцлтдрцукэысгдпснядйюкйируякыпдйьтфжштщпбдьссйрубучспс
муырзпязякзююсхьуйьтыпфюсьбякекэээнкыпзрйьющхпцрыугэсрьроццеиьмэдрыдлфжийфпсруякыпющфтдрфркдидчсзгнэ
иьруррпуырсрыдпсомнфжыдйьтыпфюсуцашркдгдбыющхпоквкруаэыфмплдюнзфбузеыпшлесяклдмучуппызхалщмфьуоукюцю
фцлтфйлдйсыдечзрноюкйибкрсйдоубюпзнртпюклдююйийрвщпсшрцюьунрэжлтэрдфштьюгрцулдаьпфштьюгрйдцщдьыулямп
якврбюжрпалфтпнщфтуйчьусррпуыубашридоуцанэбяпфзсхднрьсшкчтиэыдияокшллдрфыусюэзцюуафддуэпжрмьйиуюдйпф
ерююызырсрмучяиьзндфцдббосзджохвкэккысчабтсюмпчьхакэээфднчуслыиьвлчопчйщсжлткдкяфтьбчьйидйпфербуякбя
цучпяксруссйпферыуцуяклдбюкедципякыдррдьыпертпбяуюеолфлдтюуюосякжийрцуфжхьцрзчлфыушрнцжибждоцдзкбяуй
штиоьсоуядгфцдьпгсыдечиолфбугфцдинэияямуфдюкубзиоксщфтыксжвуьсыунчоуррлюкеуйпфцдсрпспубушпьсещштмэээ
жрыумрфймэязякбуоспуйьзюмфкеядссйэюкбякецюкщхплтуйсркьнсоуыуруйэээнэбямаяюлтьсоуядзйрунфэучсдуюкуавю
кеуйьтфжуюеонрофцюкщфтбжфьыдюбокшзцумукдбжвуякзюыпштафмлбятмькьювцзецювумродядлунчярыуцубкыпррбщфтцю
рснккенщфтчьпфцдыущюеукдлфтьммлтафгдяккресчшлукчффэрлйбяйдэйыселлтьсоуяддсврвючоррьуоуерцсфдхттщыппг
ыульшпямщслдмуякпунргфтпыплтзюзюзеуйьклскдцдшдлунчярлфелдьщпштфюкэьтчоырюогнлашрлунчюускыскдюбокштьк
ьсаэлдссшнппмфчтрсхипушддуцтщпшзфднчусхаоуыуруцубжчтйилтиоцудучюзюокгмгюкэьтпзмуйемачсцтхтионфьрхтио
мттьсюзюгржулфжиррцдцубуысдуоцыужйчьняррядкдцяюкщппуыдйюпфечйдйдшкмэсовссонэтылтцюызюуьуыумьиьиьсяиь
пфнюкеыпбяштзюокгмзюокгмсяафнэтылтцрбаэпязруфдщфаюэыжизюиягрьрцуцядраьбучяиьпунсьуйдидядзеуйпферююгр
жспчщубкфжунлдцфцягмщплтзюокгмчоцдзкрйюяуфьуоукюафгдякпсыддцуюеяиьюквргдхюкэьтпзцююкпсщюшзйрдуврнцыу
ркяуйршчцттщеркдйдзккщмфйдидечюквргдядкдцдшдищфтмпчшбтуюмплуысбдиаусэржоуьуюнфыпзюлгыужулфжиррыулюрй

мэязпутпюямуэыкдйцыулахмгрцуррггныдькчшнрдслюькээфймэязпуэуруюуэрырщчжулфжиррцдхээ
эцясжнрьсоуядппьяты
шткдццдярэпжрррдьыпьтуфтпдрюкйибкпфыдхчждгнядюкдушркдкдцуююцюокгмаффжмфыуйрьсжи
кдваякштафьююшлдцдмуйд
еныдбрбабклгыуррщумтнщчкфскдйрбкчьняпугнгндулфгажсечлфжиэшцяюкщпбупсюкндбкеукдбд
фдннкеилюкчтокйфыпзр
дфыпзрлюрйцюзицрзчцубуысядцюзюкэьтпзидщугцлтнфкеядссофкфрртщлдьцафыудьщпжоофеежо
оокдррмфыпзрлюкщфтуй
илфжбцыугнцюющфтмпчшбтуюкдсюшпмфцдэятылапррфбузишрьсэущукдгнядрутюафьуоукюмпм
фчтафыпюяярбюуйуйсрйюжи
гюкэьтчонкмачсцтхтрсздшридякмпжодуррмуврпцщппфщучяькьюафыдыулфтпнщьтоущфоуцуцюр
рврысьпыубкжрмфдьсщэа
шрсряркдэрвщьтгрбкеубюшпхьлтчюхшаюэыьдвьсрбрбалфйдиддупчбкдцыуьстахчррыузгыуийсрьй
ьтьецрщувщлдпридйр
щужфрупэтыфцжиррнщчауспспчуафддулятыцубуысомнфеятыкиокюяэшпфмфчявуцэдьщперьсффб
ужиэсюкгдяккэдьыпьтуф
тпцшкдяргцыуфдечыущююкээшржелацсрруайсфюкездррмуврпцщппфщучячтзюыгыудщлдепюкжс
ярбеыпбяштхукдьуйденыд
кфрюайнфнимэсопозюиядоякжиидцдуюзншципякбулюфьнщрушрядэрнчякыдоуыурушпзрйьцрякр
афдэрысцяюкщптауафрцу
нацябжмфоуцуецафзстьдцюясйрмькбкцюрйысфььклдшчярнрйдзязээээжршрнкчьчтйифжькиднражо
ккрцуврвюнщьтяышчаь
бяыпкрытющжрдцуювкрюзеыпбяфюокгмькрюмфщучявцыуцюмпмфчтыгыубжьуытфьррфьшпвцкр
эяжитьфжщпцрцдэыкдйцыучю
ызнрядькиолфзээзлдфэээжспчфдзеуйьтрццрфдпйруйрвщкездяклфжлбятмнщдьькиддтйцлтхукдлфз
ээзлднупуствцзнчц
чтыпйэырзпжрэяжикфбузеуйысяыздьсоуядбщфтзрщчяыуюхьежмфхайрррцубаусядцяфьякзоодсюв
уолчьзипфечеипмокуф
цпнкиелатнфьчтшлвыщзякыдвтзэюкбявлфдечшндплтцрцубкнщйфоусрмфыдпсечфйерогганщоыгю
оксрзсльуюуфбузеуйыс
яыздцюзргьыкцювутпбцчокдбуцяпфхаздцюхьькьуяроfкдбиняуюзнесзяыпдищпщхпсчрнчтиыкуюр
энсьучякщыплтгюзепф
йрунлфзедцыуцдоукщфтйгзсецькхпзрцуьсоуядхыкдерфрьрррбцжицярмфьйсппяклдисррмухиуюдр
есэршчйдлдтеыпбяка
йраиыкуюрэсйрумуужлтиоррмуйепфцдруякмпзщбязндсордфщсльфжхьмпйсмфцпырсрююыззтиечт
кфпфчяшлйикамубунчяк
мсжиытммлтнфкдгдядйдлыьедьчтаыоксродлэээтаекыпэпвышншдомэзиоцудукиьтчькекелдвдытмм
лтяяцеокчтьюарнфчя
гмзнмфдуыдюнхдомдриочьпуидияцезилдхщязьсаюкщядцуздвючотпсяфсйящщчшжуждхаррфйдйу
юрэязнщбуруыдпсоььуыу
агзсчшчсчюжиуюцмзидьыпьтуфтпдресяклдэурпхьчткэээщудумуюелдюпмфрэлдчюшзчюлтыкязкя
ыпэшжеядидщыгмщпбяюк
шнцдясииыкуюрэгюкеязкэьтуюоугфлунчюуотыпоуякэшиамуэюжрэяжидисжуаэпрсзфдущкьтаюзтз
еуйчьидчсидкявцлтбу

оцыугнуадатпжрцуьрнымпубаьмфьюкщфтйиыкуюрэафчяжимтмпытькчтуммфзсякайуюызкамртдьп
дтхитадтхижднкющфтбс
дпмфнючоьрякпуякуфхдзрьсойсрякайьсоучпюклдююйибдюиыкуюрэдйысяытдойлозндстебячьдйто
цдофцпнкшэлавщэслю
кедргсэрпсюклдююкеуйтоцдомдриоюкесэршчщсяюлтнфхдссэрнчцаффштчгыуаэлавщожующиыку
юрэосэпзойрьскнссфйце
зюзнеспсндесшннацапспчлфуюосаьврсраэйикдунйьйэсйчтусякшзбдщуыдысбудпммлтафчйысйдмц
фбйдцпйфмэчоьуякчт
чйчьякзезюзнщунрхтйиумыкгиаыоуругэжлхажупэыпщудумуюелддыиьвлчопчррнщлдодсюзюжлтю
зизюеосрйсэрнчзнесшд
сдесцятмчтесщуьсисьуярыпмуяелдтссооыкдомчоыуьцафйрсраьшпямйэюкйибкуйруаытмдубуэтиеч
тмфчьпугфыурузныф
ьуоуштафапыущунютмуюосбкюкрйюяуфпфыусюдржлмуужпуьуцямпыкуфкфияцеязякбяцюяукдмр
фймэрсядпчюкйийдэйюяую
мфькнкжрмфрюцюдйчьэучсядррнэьтрэбятыкдкньупэшлпрцугпюянфлашдзэээцюхаысэкчатэоыокча
тэязрд

Знайдений ключ до текста

(424, 500)

Розшифрований текст

библейскоепреданиеговоритчтоотсутствиетрудапраздностьбылаусловиемблаженствапервогочелов
екадоегопадениялюбовьюпраздностиосталасьтажеивпадшемчеловекенопроклятиевстяготеетнадчел
овекоминетолькопотомучтомывпотелицадолжныснискиватьхлебсвойнопотомучтопонравственным
свойствамсвоиммынеможембытьпраздныиспокойнытайныйголосговоритчтомыдолжныбытьвиновн
ызаточтопраздныежелибымогчеловекнайтисостояниевкоторомонбудучипраздным чувствовалбысеб
яполезнымиисполняющимсвойдолгонбынашелоднусторонупервобытногоблаженстваитакимсостоя
ниемобязательнойибезупречнойпраздностипользуетсяцелоесословиесословиевоенноевэтойтообяза
тельнойибезупречнойпраздностисостоялаибудетсостоятьглавнаяпривлекательностьвоеннойслужб
ыниколайростовиспытывалвполнеэтоблаженствопослегодапродолжаяслужитьвпавлоградскомполк
увкоторомонужекомандовалэскадрономпринятымотденисоваростовсделалсязагрубелымдобрымма
лымкоторогомосковскиезнакомыенашлибынесколькоконокоторыйбыллюбимиуважаемтоварищамип
одчиненнымииначальствомикоторыйбылдоволенсвоейжизньювпоследнеевремявгодуончащевпись
махиздомунаходилсетованияматеринаточтоделарасстраиваютсяхужеихужеичтопорабыемуприехат
ьдомойобрадоватьиуспокоитьстариковродителейчитаяэтописьманиколайиспытывалстрахчтохотятв
ывестиегоизтойсредывкоторойоноградивсебяотвсейжитейскойпутаницыжилтактихоиспокойноонч
увствовалчтораноилипозднопридетсяопятьвступитьвтотомутжизнирасстройствамиипоправлениям
иделсучетамиуправляющихссорамиинтригамиссвязямисобществомслюбовьюсонииобещаниемейвс
этобылострашнотруднозапутаноионотвечалнаписьмаматерихолоднымиклассическимиписьмамина
чинавшимисяиконча вшимисяумалчиваяотомкогдаоннамеренприехатьвгодуонполучилписьмародн
ыхвкоторыхизвещалиегоопомолвкенаташисболконскимиотомчтосвадьбабудетчерезгодпотомучтос
тарыйкнязьнесогласенэтописьмоогорчилооскорбилониколаявопервыхемужалкобылопотерятьиздо

манаташукоторуюонлюбилбольшевсехизсемьивовторыхонссвоейгусарскойточкизрениящалелотом
чтоегонебылоприэтомпотомучтоонбыпоказалэтомуболконскомучтосовсемнетакаябольшаячестьро
дствоснимичтоежелионлюбитнаташутоможетобойтисьибезразрешениясумасбродногоотцаминутуо
нколебалсянепопроситьсяливотпускчтобувидатьнаташуневестойнотутподошлиманеврыпришлисоо
бражениясонеопутаницеиниколайопятьотложилновеснойтогожегодаонполучилписьматериписа
вшейтайноотграфаписьмоэтоубедилоегоехатьонаписалачтоежелиниколайнеприедетиневозьметсяз
аделатовсименьепойдетсмолоткаивсепойдутпомируграфтакслабтаквверилсямитенькеитакдобритак
всеегообманываютчтовсидетхужеихужерадибогаумоляютебяприезжайсейчасжеежелитынехочешьс
делатьменяивствоесемействонесчастнымиписалаграфиняписьмоэтоподействовалонаниколаяунегоб
ылтотздравыйсмыслпосредственностикоторыйпоказывалемучтобылодолжнотеперьдолжнобылоеха
тьеслиневотставкутовотпускпочемунадобылоехатьоннезналновыспавшисьпослеобедаонвелелоседл
атьсерогомарсадавнонеезженногоистрашнозлогожеребцаивернувшисьнавзмыленномжеребцедомо
йобявиллаврушкелакейденисоваосталсяуростоваипришедшимвечеромтоварищамчтоподаетвотпуск
иедетдомойкакнитрудноистраннобылоемудуматьчтоонуедетинеузнаетизштабачтоемуособенноинте
реснобылопроизведенлионбудетвротмистрыилиполучитаннузапоследниеманеврыкакнистраннобыл
одуматьчтоонтакиуедетнепродавграфуголуховскомутройкусаврасыхкоторыхпольскийграфторгова
лунегоикоторыхростовнапарибилчтопродастзатысячикакнинепонятноказалосьчтобезнегобудеттотб
алкоторыйгусарыдолжныбылидатьпаннепшаздецкойвпикууланамдававшимбалсвоейпаннеборжозо
вскойонзналчтонадоехатьизэтогоясногохорошегомиракудатотудагдевсбыловздорипутаницачерезне
делювышелотпускгусарытоварищинетолькопополкуноипобригадедалиобедростовустоившийсголо
выпорубподпискиигралидвемузыкипелидвахорапесенниковростовплясалтрепакасмайоромбасовым
пьяныеофицерыкачалиобнималииуронилиростовасолдатытретьегоэскадронаещеразкачалиегоикрич
алиурапотомростоваположиливсаниипроводилидопервойстанциидополовиныдорогикакэтовсегдаб
ываетоткременчугадокиевавсемыслиростовабылиещеназадивэскадроненоперевалившисьзаполовин
уонуженачалзабыватьтройкусаврасыхсвоеговахмистрадожойвейкуибеспокойноначалспрашиватьсе
бяотомчтоикаконнайдетвотрадномчемближеонподезжалтемсильнеегораздосильнеекакбудтонравст
венноечувствобылоподчиненотомужезаконускоростипаденияталвквадратахрасстоянийондумалосв
оемдоменапоследнейпередотраднымстанциидалямщикутрирублянаводкуикакмальчикзадыхаясьвбе
жалнакрыльцодомапослевосторговвстречиипослетогостранногочувстваневдовлетворениявсравнен
иистемчегоожидаешьвстожекчемужеятакторопилсяниколайсталвживатьсявсвойстарыймирдомаоте
циматьбылитежеонитольконемногопостарелиновоевнихбилокакоетобеспокойствоиногданесоглас
иекоторогонебывалопреждеикотороекакскороузналниколайпроисходилоотдурногоположенияделсо
небылужедвадцатыйгодонаужеостановиласьхорошетьничегонеобещалабольшетогочтовнейбылоно
иэтогобылодостаточноонавсядышаласчастьемилюбовьюстехпоркакприехалниколайивернаянепоко
лебимаялюбовьэтойдевушкирадостнодействовалананегопетяинаташабольшевсехудивилиниколаяп
етябылужебольшойтринадцатилетнийкрасивыйвеселоиумношаловливыймальчикукоторогоужелом
алсяголоснанаташуниколайдолгоудивлялсяисмеялсяглядянаneесовсемнетаговорилончтожподурнел
анапротивноважностькакаятокнягинясказалонейшопотомдададарадостноговориланаташанаташара
ссказалаемусвойроманскняземандреемегоприездвотрадноеипоказалаегопоследнееписьмочтожтыра
дспрашиваланаташаятактеперьспокойнасчастливаоченьрадотвечалниколайонотличныйчеловекчто
жтыоченьвлюбленакактебесказатьотвечаланаташаябылавлюбленаборисавучителявденисованоэто
совсемнетомнепокойнотвердоязнаючтолучшеегонебываетлюдейимнетакспокойнохорошотеперьсо
всемнетаккакпрежденниколайвыразилнаташесвоенеудовольствиеотомчтосвадьбабылаотложенанаго
днонаташасожесточениемнапустиласьнабратадоказываяемучтоэтонемоглобытьиначечтодурнобыб
ыловступитьвсемьюпротивволиотцачтоонасамаэтогохотелатысовсемсовсемнепонимаешьговорила

онаниколайзамолчалисогласилсяснеюбратчастоудивлялсяглядянанеесовсемнебылопохожечтобыон
абылавлюбленнаяневеставразлукессвоимженихомонабыларовнаспокойнавеселасовершеннопопреж
немуниколаяэтоудивлялоидажезаставлялонедоверчивосмотретьнасватовствоболконскогоонневери
лвточтоеесудьбаужерешенатемболеечтоонневидалснеюкнязяандреяемувсказалосьчточтонибудьнет
овэтомпредполагаемомбракезачемотсрочказачемнеобручилисьдумалонразговорившисьразсматерь
юосестреонкудивлениюсвоемуиотчастикудовольствиюнашелчтоматьточнотакжевглубинедушиино
гданедоверчивосмотреланаэтотбраквотпишетговорилаонапоказываясынуписьмокнязяандреястемза
таеннымчувствомнедоброжелательстваковоевсегдаестьуматеripротивбудущегосупружескогосча
стиядочерипишетчтонеприедетраньшедекабрякакоежеэтоделоможетзадержатьеговерноболезньздо
ровьеслабоеоченьтынеговоринаташетынесмотричтоонавеселаэтоужпоследнеедевичьевремядожива
етаязнаючтоснейделаетсявсякийразкакписьмаегополучаемавпрочембогдаствсихорошобудетзаключ
алаонавсякийразонотличныйчеловекпервоевремясвоегоприезданиколайбылсерьезенидажескученег
омучилапредстоящаянеобходимостьвмешатьсявэтиглупыеделахозяйствадлякоторыхматьвызвалаег
очтобыскореесвалитьсплечэтуобузунатретийденьсвоегоприездаонсердитонеотвечаянавопроскудао
нидетпошелснахмуреннымибровямивофлигелькмитенькеипотребовалунегосчетывсегочтотакоебыл
иэтисчетывсегониколайзналещеменеечемпришедшийвстрахинедоумениемитенькаразговориучетми
тенькипродолжалсянедолгостароставыборныйиземскийдожидавшиесявпереднейфлигелясострахом
иудовольствиемслышалисначалакакзагуделизатрещалкакбудтовсвозвышавшийсяголосмолодогогра
фаслышалиругательныеистрашныесловасыпавшиесяоднозадругимразбойникнеблагодарнаятварьиз
рублюсобакунеспапенькойобворовалитдпотомэтилюдиснеменьшимудовольствиемистрахомвидели
какмолодойграфвеськрасныйсналитойкровьювглазахзашиворотвытащилмитенькуногойиколенкойс
большойловкостьювудобноевремямеждусвоихсловтолкнулегоподзадизакричалвончтобыдухутвоег
омерзавецздесьнебыломитенькастремглавслетелсшестиступенейиубежалвклумбуклумбаэтабылаиз
вестнаяместностьспасенияпреступниковвотрадномсаммитенькаприезжаяпьяныйизгородапрятался яв
этуклумбуимногиежителиотрадногопрятавшиесяотмитенькизналиспасительнуюсилуэтойклумбыж
енамитенькиисвояченицысиспуганнымилицамивысунулисьвсениизверейкомнатыгдекипелчистый
самоваривозвышаласьприказчицкаявысокаяпостельподстеганнымодеяломсшитымизкороткихкусоч
ковмолодойграфзадыхаясьнеобращаянанихвниманиярешительнымишагамипрошелмимонихипоше
лвдомграфиняузнавшаятотчасчерездевушекотомчтопроизошловофлигелесоднойстороныуспокоила
сьвтомотношениичтотеперьсостояниеихдолжнопоправитьсясдругойстороныонабеспокоиласьотомк
акперенесетэтоеесынонаподходиланесколькоразнацыпочкахкегодверислушаякаконкурилтрубкузат
рубкой

Висновок

Під час виконання даної лабораторної роботи написали код програми, що аналізує ШТ, який було зашифровано афінним шифром біграмної підстановки. Було написано функції, що виконують обчислення оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв’язування лінійних порівнянь, пошук ключів для зашифрованого тексту, розшифрування даного ШТ за допомогою знайдених ключів та автоматичне відкидання знайдених варіантів ВТ, що не є змістовними текстами. Під час роботи набули навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанували прийомами роботи в модулярній арифметиці.