Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №3

з дисципліни

«Криптографія»

на тему: «Криптоаналіз афінної біграмної підстановки»

Виконали:

студенти 3 курсу ФТІ

групи ФБ-72

Солдатова Катерина та Яшкова Вікторія

Перевірили:

Чорний О.

Савчук М. М.

Завадська Л. О.

Мета роботи :

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

Порядок виконання роботи

к 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 завдання:

цсбтызнэжрцяфьзюдрцубуысьцыуюкнажфтпдрчядьдйлдаьпуяксщфтэаытыпдрвщядшрщфтпдйюябуцуйрдуврйдмузеуйиьую

еочшлукчэйлдаьпуякгуяклтафвкежнспйиьяршцчтыпйэуюуйрудтшкдрлфюоцуэрьккдлцчтыпйэйифюькьтрэуйюкйирцыусн

пйюкчтфбиььтйюйфьснэщпокмлерхфбукюуйюкйирцыуьулямпякврбюгиэпязякыддфбузиснррщушрвщчкчйлдаьзннфьуоукю

чкпззнюеьтпфцубуысьцыуснмуужзнгнечмспутюыыокдцыуцятыююаршрпсгнщухцчтыпйэкдскнфпфыусюдриэюкбяйицютауа

усцятыююгипалфтпыплтгнзрноьуеряюгиосфйьтсожвзиэпязмуйецюгнкдярдуююыфыуруцаырзпнщчкпуцубтежуюякыдыкээ

зижуякзоьсжинщэыокчтьюязлщяыайсрщюязцятыююпфзсьунчфаькиоурдумфпфдумсмфпфдумсшпжрбюжрзгыускеуноидэрнч

пудсмрфацябцпузйлдаьпуякнфпфыухтбстанржфпфыушкоеядтючоцящперйдэрнчпуякапжрбюязытбжгньсоуядфяпфыумсфй

чкхплтпйьтррнкнщядшрщфтпуйпферцуздцячььттдкфлагсечпймпдутяиьнэйиьулэипоуыурущуцашроуфдвьыплтяфйдияцю

йицяфюшкгиюкнрьсжуыдруякыпшьчтлтиоидтящщчтгимузягифдынбэюкбякейипфоулфщсяыкдоуснуюгмпсгнррнэьтрэцюмэ

юкбяшзгнщттщзикаыдтджиыуыдысодесьулцфюуюзнесфюфцлтуфтпйикэюкбяшзгнцьыпьтуюэпжрижаышчбпьуытфьрршпсрыо

жечьсуоцсвшпжспчфдисаьйигюшлчьштзрыуыдьсдиокюяфюокдцыунрядлдрфчябсыдгкиодашржлбжнсбкуйбяющарбацядрчд

ечмущушузяиьыпокфсыфьуоуыкуфцдысоуэячьыкчтызусцджгзсжспчфдьсоуяддсфйчкхплтяклдыцыуэуюотпхпмфзсзерсжк

язвяфьхпоуыурушупутяиьщпзрноюклфызгсэргфоузйккзюфбожштцдзкжлрсфймэязпуцюпалфтпыплтбкбязюрспсьуаьпуця

хьькиоуйшкапякайыкапыуыубалжаыьсвяафякругфтпщиосьуцямперьсдихьчтнайрцдесайлдцтушясзфжулдесфючяиещинф

эпэыдинфнщфрякбудфчшлукчффцюоснщювзюдрьрппмгыугндуяклдпююкчаюювыдйккзюрсцююквргдхюдйнфнищиокюяжльтчь

знесдтафссйрнэзисйнфнищифюфцфюмпйсесиокэцюгдомзинфзафдгцщпчоюкйиоуйьхубющиюяуюцядрчдечжечьсуюйьтрцшт

жспчфдруюювлиэюкбявлаывродпсзееуьущуьппркдцдйсощьтоущфщсесюкйибкпфыдхчждтанрьцюяяыцуьйюкйирцыуяксяшз

аюэыьюмфкеядзрхгыужспчщукебяусдупфоушщштцюкэьтчобуырзпвлжибжлтоугндуьуэртоечаымуфдкдцдеаоуыучакуеттщ

штлунчярлфелаызргчщпыпыуинэущфэпжрюеыфсянэязыупэаысрьспжлтчтюкйибкжрцурргндуцяйгыуийюкйирцыуцюгньуйд

идкгыубалулэцюнэйирцыужулфжиррцдйдищьтцмчойрякеячьякбучюзивцыусжчтгуеттщыккдцдеаыущушрыулускнффсмрйя

тысрярьскфхиафзячьпуцуюкндесцагацюоуерждофсюрйуйруссечиопсбукйыфнцыутамсздечкдцдеарррвякязпугакйчьтм

псфдррэянйысутнфеузяежуюеопфцювуацдьсурфюкэьтпзуйшкйустфжштпуврчюязыуцушрцуздцюьулаустйнфнийиокюясй

нфмпярскпзпуюктякхбсжспчщункмамрчсдузежрчдечцюдйнфлтфцыусжчтфюкэьтпзррцядрнрзсррбуцчьржфэыиьчтокыпсс

ьршчрйязнржфщудугэбслфрйязуакййияяцелдакээытющцдепврысофдиыкуюрэнсцдбьнщысцдепзрзееупизюхпйшьцыулфхь

ькдашржлбжюяиьлщкеэащужогккщойысяытдгфызгдхжгршрпсунррэуйрзчшьчтокниуюлслфтпжрзрьргфтпцюмфгдякзнесжс
бдядтякхфюойнфнилгыуьунргфтпыплтцюзюкэьтчогюзенщфтыушыиямпшзкийфтйпфсрцфтпуюпуяккэюкбяшзьуйденыдерба
бкнщфтчььтйююкрйюяыььтйюнщфтжрчдечмфпсррбужфцдиэккыпюкванэьуйрбакдмугндуелокйубюяыкдхюыпйфхдомнфчйпф
ернщфьхужпчтчтпффьядечзрруцуфдьфиьмппурряышрбюкерсяклдпювыдуцушрсрэббсврвюипйспчкдюыснербюйишрсрэбфь
йиязнщцпштядэяямпрядпрльуюнфыпхуяклтионяпфыуыдсйысярщмзиврйрруткыпсяявщибкуйчьцртпюкванэдрнроьйиязйд
аюыкчаююрсяклдбюнщфтжрбауафдечбкеуцафьькфюйаяюцрзсьмцдждбкжрбапфнщуюпуфюэрсрчюнщфтуйруаыврнретгучщдь
ькэяюкесякинштсйьтрцыкзюцаидьуытфььсжизюшпинйдаюнфчязюпугндууафдечбкеуикээкафььккррцячьмптякхцеьтфлып
нэйиккруаэыфмплдюндэюкбявльунчнээзтякхыухеыплтгюзерсоуыуиншяпфыутюдйсялщштбкуйруздякидуниоусйдаюфюрй
цюшкпуйдиддупчбкнщяыррцутанрфкюкждлэюкбяшзюабдинмуужзнгнпсздечхдбюрйшдаьубоуппжсхазтзющиздыдомзиждоф
буызхдбюкщбячунулфоушумыкдгцыукдмуелокфсугыуцукфпуцуэуруярцуеслдхаздыугаздйьшпощфтыпаьбясйккзюфбфцюя
яыррнрчшшнярдукйыфуеыфсячкыпсяявфюькьтрэуйуйьтхапусйнщыссднрздпснщфьруякыпыфыущпйсгфцудушньучащйчьжс
нэостялтхьврбаенщсырпсгпшлбядймфуюьсоуэяпфыупйжобдэксрхдйдкипзбяйижджушнийлознвутсуринйдгдпснщьсфдпс
каруьспсруякыпафьтздунчяькркрцуяфйдияцюцрфрлдфэфцлтдрцукэысгдпснядйюкйируякыпдйьтфжштщпбдьссйрубучспс
муырзпязякзююсхьуйьтыпфюсьбякекэээнкыпзрйьющхпцрыугэсрьроццеиьмэдрыдлфжийфпсруякыпющфтдрфркдидчсзгнэ
иьруррпуырсрыдпсомнфжыдйьтыпфюсуцашркдгдбыющхпоквкруаэыфмплдюнзфбузеыпшлесяклдмучуппызхалщмфьуоукюцю
фцлтфйлдйсыдечзрноюкйибкрсйдоубюпзнртпюклдююйийрвщпсшрцюьунрэжлтэрдфштьюгрцулдаьпфштьюгрйдцщдьыулямп
якврбюжрпалфтпнщфтуйчьусррпуыубашридоуцанэбяпфзсхднрьсшкчтиэыдияокшллдрфыусюэзцюуафддуэпжрмьйиуюдйпф
ерююызырсрмучяиьзндфцдббосзджохвкэккысчабтсюмпчьхакэээфднчуслыиьвлчопчйщсжлткдкяфтьбчьйидйпфербуякбя
цучпяксруссйпферыуцуяклдбюкедципякыдррдьыпертпбяуюеолфлдтюуюосякжийрцуфжхьцрзчлфыушрнцжибждоцдзкбяуй
штиоьсоуядгфцдьпгсыдечиолфбугфцдинэияямуфдюкубзиоксщфтыксжвуьсыунчоуррлюкеуйпфццдсрпспубушпьсещштмэээ
жрыумрфймэязякбуоспуйьзюмфкеядссйэюкбякецюкщхплтуйсркьнсоуыуруйэээнэбямаяюлтьсоуядзйрунфэучсдуюкуавю
кеуйьтфжуюеонрофцюкщфтбжфьыдюбокшзцумукдбжвуякзюыпштафмлбятмькьювцзецювумродядлунчярыуцубкыпррбщфтцю
рснккенщфтчьпфцдыущюеукдлфтьммлтафгдяккресчшлукчффэрлйбяйдэйыселлтьсоуяддсврвючоррьуоуерцсфдхттщыппг
ыульшпямщслдмуякпунргфтпыплтзюзюзеуйьклскдцдшдлунчярлфелдьщпштфюкэьтчоырюогнлашрлунчюускыскдюбокштьк
ьсаэлдссшнппмфчтрсхипушддуцтщпшзфднчусхаоуыуруцубжчтйилтиоцудучюзюокгмгюкэьтпзмуйемачсцтхтионфьрхтио
мттьсюзюгржулфжиррцдцубуысдуоцыужйчьняррядкдцяюкщппуыдйюпфечйдйдшкмэсовссонэтылтцюызюуьуыумьиьиьсяиь
пфнюкеыпбяштзюокгмзюокгмсяафнэтылтцрбаэпязруфдщфаюэыжизюиягрьрцуцядраьбучяиьпунсьуйдидядзеуйпферююгр
жспчщубкфжунлдцфцягмщплтзюокгмчоцдзкрйюяуфьуоукюафгдякпсыддцуюеяиьюквргдхюкэьтпзцююкпсщюшзйрдуврнцыу
ркяуйршчцттщеркдйдзккщмфйдидечюквргдядкдцдшдищфтмпчшбтуюмплуысбдиаусэржоуьуюнфыпзюлгыужулфжиррыулюрй
мэязпутпюямуэыкдйцыулахмгрцурргныдькчшнрдслюькээфймэязпуэуруюуэрырщчжулфжиррцдхэээцясжнрьсоуядппьяты
шткдцдярэпжрррдьыпьтуфтпдрюкйибкпфыдхчждгнядюкдушркдкдцуююцюокгмаффжмфыуйрьсжикдваякштафьюющлдцдмуйд
еныдбрбабклгыуррщумтнщчкфскдйрбкчьняпугнгндулфгажсечлфжиэшцяюкщпбупсюкндбкеукдбдфдннккеилюкчтокйфыпзр
дфыпзрлюрйцюзицрзчцубуысядцюзюкэьтпзидщугцлтнфкеядссофкфрртщлдьцафыудьщпжоофеежооокдррмфыпзрлюкщфтуй
илфжбцыугнцюющфтмпчшбтуюкдсюшпмфцдэятылапррфбузишрьсэущукдгнядрутюафьуоукюмпмфчтафыпюяярбюуйуйсрйюжи
гюкэьтчонкмачсцтхтрсздшридякмпжодуррмуврпцщппфщучяькьюафыдыулфтпнщьтоущфоуцуцюррврысьпыубкжрмфдьсщэа
шрсряркдэрвщьтгрбкеубюшпхьлтчюхшаюэыьдвьсрбрбалфйдиддупчбкдцыуьстахчррыузгыуийсрьйьтьецрщувщлдпридйр
щужфрупэтыфцжиррнщчауспспчуафддулятыцубуысомнфеятыкиокюяэшпфмфчявуцэдьщперьсффбужиэсюкгдяккэдьыпьтуф
тпцшкдяргцыуфдечыущююкээшржелацсрруайсфюкездррмуврпцщппфщучячтзюыгыудщлдепюкжсярбеыпбяштхукдьуйденыд

кфрюайнфнимэсопозюиядоякжиидццдуюзншщипякбулюфьнщрушрядэрнчякыдоуыурушпзрйьцрякрафдэрысцяюкщптауафрцу

нацябжмфоуцуецафзстьдцюясйрмькбкцюрйысфььклдшчярнрйдзязэээжршрнкчьчтйифжькиднражоккрцуврвюнщьтяышчаь

бяыпкрытющжрдцуювкрюзеыпбяфюокгмькрюмфщучявцыуцюмпмфчтыгыубжьуытфьррфьшпвцкрэяжитьфжщпцрцдэыкдйцыучю

ызнрядькиолфзээзлдфэээжспчфдзеуйьтрццрфдпйруйрвщкездяклфжлбятмнщдьькиддтйцлтхукдлфзээзлднупуствцзнчц

чтыпйэырзпжрэяжикфбузеуйысяыздьсоуядбщфтзрщчяыуюхьежмфхайрррцубаусядцяфьякзоодсювуолчьзипфечеипмокуф

цпнкиелатнфьчтшлвыщзякыдвтзэюкбявлфдечшндплтцрцубкнщйфоусрмфыдпсечфйерогганщоыгюоксрзсльуюуфбузеуйыс

яыздцюзргьыкцювутпбцчокдбуцяпфхаздцюхьькьуярофкдбиняюзнеззяыпдищпщхпсчрнчтиыкуюрэнсьучякщыплтгюзепф

йрунлфзедцыуцдоукщфтйгзсецькхпзрцуьсоуядхыкдерфрьрррбцжицярмфьйсппяклдисррмухиуюдресэршчйдлдтеыпбяка

йраиыкуюрэсйрумуужлтиоррмуйепфцдруякмпзщбязндсордфщсльфжхьмпйсмфцпырсрююыззэтиечткфпфчяшлйикамубунчяк

мсжиытммлтнфкдгдядйдлыьедьчтаыюксродлэээтаекыпэпвышншдомэзиоцудукиьтчькекелдвдытммлтяяцеокчтьюарнфчя

гмзнмфдуыдюнхдомдриочьпуидияцезилдхщязьсаюкщядцуздвючотпсяфсйящщчшжуждхаррфйдйуюрэязнщбуруыдпсоььуыу

агзсчшчсчюжиуюцмзидьыпьтуфтпдресяклдэурпхьчткэээщудумуюелдюпмфрэлдчюшзчюлтыкязкяыпэшжеядидщыгмщпбяюк

шнцдясииыкуюрэгюкеязкэьтуюоугфлунчюуотыпоуякэшиамуэюжрэяжидисжуаэпрсзфдущкьтаюзтзеуйчьидчсидкявцлтбу

оцыугнуадатпжрцуьрнымпубаьмфьюкщфтйиыкуюрэафчяжимтмпытькчтуммфзсякайуюызкамртдьпдтхитадтхижднкющфтбс

дпмфнючоьрякпуякуфхдзрьсойсрякайьсоучпюклдююйибдюиыкуюрэдйысяытдойлозндстебячьдйтоцдофцпнкшэлавщэслю

кедргсэрпсюклдююкеуйтоцдомдриоюкесэршчщсяюлтнфхдссэрнчцаффштчгыуаэлавщожующиыкуюрэосэпзойрьскнссфйце

зюзнеспсндесшннацапспчлфуюосаьврсраэйикдунйьйэсйчтусякшзбдщуыдысбудпммлтафчйысйдмцфбйдцпйфмэчоьуякчт

чйчьякзезюзнщунрхтйиумыкгиаыоуругэжлхажупэыпщудумуюелддыиьвлчопчррнщлдодсюзюжлтюзизюеосрйсэрнчзнесшд

сдесцятмчтесщуьсисьуярьпмуяелдтссооыкдомчоыуьцафйрсраьшпямйэюкйибкуйруаытмдубуэтиечтмфчьпугфыурузныф

ьуоуштафапыущунютмуюосбкюкрйюяуфпфыусюдржлмуужпуьуцямпыкуфкфияцеязякбяцюяукдмрффймэрсядпчюкйийдэйюяую

мфькнкжрмфрюцюдйчьэучсядррнэьтрэбятыкдкньупэшлпрцугпюянфлашдзэээцюхаысэкчатэоыокчатэязрд

Результати виконання програми:

Наш ключ: [a,b] = [424, 500]

Критерій який був використаний : Ентропійний (Індекс Відповідності)

Який дорівнює 0.05707641824451283

библейскоепреданиеговоритчтоотсутствиетрудапраздностьбылаусловиемблаженствапервогочеловекадоегопаденияслюбовьюкпраздностиостала
сьтажеивпадшемчеловекенепроклятиевстяготеетнадчеловекоминетолькопотомучтомывпотелицадолжныснискиватьхлебсвойнопотомучтопо
нравственнымсвойствамсвоиммыневожембытьпраздныиспокойнытайныйголосговоритчтомыдолжныбытьвиновнызаточтопраздныежелибым
огчеловекнайтисостояниевкоторомонбудучипраздныммчувствовалбысебяполезнымиисполняющимсвойдолгонбынашелоднусторонупервобыт
ногоблаженстваитакимсостояниемобязательнойибезупречнойпраздностипользуетсяцелоесословиесословиевоенноевэтойтообязательнойибез
упречнойпраздностисостоялаибудетсостоятьглавнаяпривлекательностьвоеннойслужбыниколайростовиспытывалвполнеэтоблаженствопослег
одапродолжаяслужитьвпавлоградскомполкувкоторомонужекомандовалэскадрономпринятымотденисоваростовсделалсязагрубелымдобрымм
алымкоторогомосковскиезнакомыенашлибынесколькономоторыйбыллюбимиуважаемтоварищамиподчиненнымииначальствомикоторыйбыл
доволенсвоейжизньювпоследнеевремявгодуончащевписьмахиздомунаходилсетованияматеринаточтоделарасстраиваютсяхужеихужеичтопора
быемуприехатьдомойобрадоватьиуспокоитьстариковродителейчитаяэтописьманиколайиспытывалстрахчтохотятвывестиегоизтойсредывкото
ройоноградивсебяотвсейжитейскойпутаницыжилтактихоиспокойноончувствовалчтораноилипозднопридетсяопятьвступитьвтотомутжизниср
асстройствамиипоправлениямиделсучетамиуправляющихссорамиинтригамиссвязямисобществомслюбовьюсониобещаниемейвсэтобылостр
ашнотруднозапутаноионотвечалнаписьмаматерихолоднымиклассическимиписьманачинавшимисяикончавшимисяумалчиваяотомкогдаонн
амеренприехатьвгодуонполучилписьмародныхвкоторыхизвещалиегоопомолвкенаташисболконскимиотомчтосвадьбабудетчерезгодпотомучт
остарыйкнязьнесогласенэтописьмоогорчилооскорбилониколаявопервыхемужалкобылопотерятьиздомаштукоторуюонлюбилбольшевсехиз
семьивовторыхонссвоейгусарскойточкизренияжалелотомчтоегонебылоприэтомпотомучтоонбыпоказалэтомуболконскомучтосовсемнетакаяб
ольшаячестьродствоснимичтоежелионлюбитнаташутоможетобойтисьибезразрешенияусмасбродногоотцаминутуонколебалсянепопроситьсял
ивотпускчтобувидатьнаташуневестойнотутподошлиманеврыпришлисоображенияосонеопутаницеиниколайопятьотложилновеснойтогожегод
аонполучилписьмоматериписавшейтайноотграфаиписьмоэтоубедилоегоехатьонаписалачтоежелиниколайнеприедетиневозьметсязаделатовси
меньепойдетсмолоткаивсепойдутпомируграфтакслабтаквверилсямитенькеитакдобритаквсеегообманываютчтовсидетхужеихужерадибогаумо
ляютебяприезжайсейчасжеежелитынехочешьсделатьменяивствоесемействонесчастнымиписалаграфиняписьмоэтоподействовалонаниколаяун
егобылтотздравыйсмыслпосредственностикоторыйпоказывалемучтобылодолжнотеперьдолжнобылоехатьеслиневотставкутовотпускпочемун
адобылоехатьоннезналновыспавшисьпослеобедаонвелелоседлатьсерогомарсадавнонеезженногоистрашнозлогожеребцаивернувшисьнавзмыл
енномжеребцедомойобявиллаврушкелакейденисоваостался уростоваипришедшимвечеромтоварищамчтоподаетвотпускиедетдомойкакнитруд
ноистраннобылоемудуматьчтоонуедетинеузнаетизштабачтоемуособенноинтереснобылопроизведенлионбудетвротмистрыилиполучитаннуза

последниеманеврыкакнистраннобылодуматьчтоонтакиуедетнепродавграфуголуховскомутройкусаврасыхкоторыхпольскийграфторговалунег

оикоторыхростовнапарибилчтопродастзатысячикакнинепонятноказалосьчтобезнегобудеттотбалкоторыйгусарыдолжныбылидатьпаннепшазд
ецкойвпикууланамдававшимбалсвоейпаннеборжозовскойонзналчтонадоехатьизэтогоясногохорошегомиракудатотудагдевсбыловздорипутани
цачерезнеделювышелотпускгусарытоварищинетолькопополкуноипобригадедалиобедростовустоившийсголовыпорубподпискиигралидвемуз
ыкипелидвахорапесенниковростовплясалтрепакасмайоромбасовымпьяныеофицерыкачалиобнималииуронилиростовасолдатытретьегоэскадр
онаещеразкачалиегоикричалиурапотомростоваположиливсаниипроводилидопервойстанциидополовиныдорогикакэтовсегдабываетоткременч
угадокиевавсемыслиростовабылиещеназадивэскадроненоперевалившисьзаполовинуонуженачалзабыватьтройкусаврасыхсвоеговахмистрадо
жойвейкуибеспокойноначалспрашиватьсебяотомчтоикаконнайдетвотрадномчемближеонподезжалтемсильнеегораздосильнеекакбудтонравст
венноечувствобылоподчиненотомужезаконускоростипадениятелвквадратахрасстоянийондумалосвоемдоменапоследнейпередотраднымстанц
иидалямщикутрирублянаводкуикакмальчикзадыхаясьвбежалнакрыльцодомапослевосторговвстречиипослетогостранногочувстванеудовлетво
рениявсравнениистемчегоожидаешьвстожекчемужеятакторопилсяниколайсталвживатьсявсвойстарыймирдомаотециматьбылитежеонитолько
немногопостарелиновоевнихбилокакоетобеспокойствоииноданесогласиекоторогонебывалопреждеикотороекакскороузналниколайпроисход
илоотдурногоположенияделсонебылужедвадцатыйгодонаужеостановиласьхорошетьничегонеобещалабольшетогочтовнейбылоноиэтогобыло
достаточноонавсядышаласчастьемилюбовьюстехпоркакприехалниколайивернаянепоколебимаялюбовьэтойдевушкирадостнодействованане
гопетяинаташабольшевсехудивилиниколаяпетябылужебольшойтринадцатилетнийкрасивыйвеселоиумношаловливыймальчикукоторогоужел
омалсяголоснанаташуниколайдолгоудивлялсяисмеялсяглядянанеесовсемнетаговорилончтожподурнеланапротивноважностькакаятокнягиняс
казалонейшопотомдададарадостноговориланаташанаташарассказалаемусвойроманскняземандреемегоприездвотрадноеипоказалаегопоследне
епись мочтожтырадспрашиваланаташаятактеперьспокойнасчастливаоченьрадотвечалниколайонотличныйчеловекчтожтыоченьвлюбленакакте
бесказатьотвечаланаташаябылавлюбленавборисавучителявденисованоэтосовсемнетомнепокойнотвердоязнаючтолучшеегонебываетлюдейим
нетакспокойнохорошотеперьсовсемнетаккакпрежденикола йвыразилнаташесвоенеудовольствиеотомчтосвадьбабылаотложенанагоднонаташа
сожесточениемнапустиласьнабратадоказываяемучтоэтонемоглобытьиначетдурнобыловступитьвсемьюпротивволиотцачтоонасамаэтого
хотелатысовсемсовсемнепонимаешьговорилаонаниколайзамолчалисогласилсяснеюбратчастоудивлялсяглядянанеесовсемнебылопохожечтоб
ыонабылавлюбленнаяневеставразлукессвоимженихомонабыларовнаспокойнавеселасовершеннопопрежнемуниколаяэтоудивлялоидажезастав
лялонедоверчивосмотретьнасватовствоболконскогоонневерилвточтоеесудьбаужерешенатемболеечтоонневидалснеюкнязяандреяемувсказало
сьчточтонибудьнетовэтомпредполагаемомбракезачемотсрочказачемнеобручилисьдумалонразговорившисьразсматерьюосестреонкудивлению
своемуиотчастикудовольствиюнашелчтоматьточнотакжевглубинедушииногданедоверчивосмотреланаэтотбраквотпишетговорилаонапоказыв
аясынуписьмокнязяандреястемзатаеннымчувствомнедоброжелательствакотороевсегдаестьуматерипротивбудущегосупружескогосчастиядоче
рипишетчтонеприедетраньшедекабрякакоежеэтоделоможетзадержатьеговерноболезньздоровьеслабоеоченьтыневоринаташетынесмотричто
онавеселаэтоужпоследнеедевичьевремядоживаетаязнаючтоснейделаетсявсякийразкакписьмаегополучаемавпрочембогдаствсихорошобудетза
ключалаонавсякийразонотличныйчеловекпервоевремясвоегоприезданиколайбылсерьезенидажескученегомучилапредстоящаянеобходимость
вмешатьсявэтиглупыеделахозяйствадлякоторыхматьвызвалаегочтобыскореесвалитьсплечэтуобузунатретийденьсвоегоприездаонсердитонеот
вечаянавопроскудаонидетпошелснахмуреннымибровямивофлигелькмитенькеипотребовалунегосчетывсегочтотакоебылиэтисчетывсегоникол
айзналещеменеечемпришедшийвстрахинедоумениемитенькаразговориучетмитенькипродолжалсянедолгостаростаставыборныйиземскийдожида
вшиесявпереднейфлигелясострахомиудовольствиемслышалисначалакакзагуделизатрещалкакбудтовсвозвышавшийсяголосмолодогографасл
ышалиругательныеистрашныесловасыпавшиесяоднозадругимразбойникнеблагодарнаятварьизрублюсобакунеспапенькойобворовалитдпотом
этилюдиснеменьшимудовольствиемистрахомвиделикакмолодойграфвеськрасныйсналитойкровьювглазахзашиворотвытащилмитенькуногойи
коленкойсбольшойловкостьювудобноевремямеждусвоихсловтолкнулегоподзадизакричалвончтобыдухутвоегомерзавецздесьнебыломитенька
стремглавслетелсшестиступенейиубежалвклумбуклумбаэтабылаизвестнаяместностьспасенияпреступниковвотрадномсаммитенькаприезжаяп
ьяныйизгородапрятался явэтуклумбуимногиежителиотрадногопрятавшиесяотмитенькизналиспасительнуюсилуэтойклумбыженамитенькиисво
яченицысиспуганнымилицамивысунулисьвсенииздверейкомнатыгдекипелчистыйсамоваривозвышалась приказчицкаявысокаяпостельподстег
аннымодеяломсшитымизкороткихкусочковмолодойграфзадыхаясьнеобращаянанихвниманиярешительнымишагамипрошелмимонихипошелв
домграфиняузнавшаятотчасчерездевушекотомчтопроизошловофлигелесоднойстороныуспокоилась втомотношениичтотеперьсостояниеихдол
жнопоправитьсясдругойстороныонабеспокоилась отомкакперенесетэтоеесынонаподходиланесколькоразнацыпочкахкегодверислушаякаконку
рилтрубкузатрубкойаа

Код програми:

```
import math
alphabet = "абвгдежзийклмнопрстуфхцчшщьыэюя"
FrequBigrams = ['ст', 'но', 'то', 'на', 'ен']
finder = lambda a: alphabet.find(a[0]) * 31 + alphabet.find(a[1])


def IndexVidpovidnosti(encrypted, num):
    somestr = ''
    for i in range(0, len(encrypted), num):
        somestr += encrypted[i]
    diction = dict.fromkeys(alphabet, 0)
    for i in alphabet:
        for j in somestr:
            if i == j:
```

```
            diction[i] += 1
    index = 0
    lengthofstring = len(somestr)
    for i in diction.keys()
        index += (diction[i]) * (diction[i] - 1) / (lengthofstring * (lengthofstring - 1))
    return index

def ReverElement(a, b):
    varies = [1, 0, 0, 1]
    while b != 0:
        fract, tempe = divmod(a, b)
        a, b = b, tempe
        varies = [varies[2], varies[3], (varies[0] - fract * varies[2]), (varies[1] - fract * varies[3])]
    return varies[0]

def Solver(a, b, n):
    d = math.gcd(a, n)
    if (d == 1):
        return [(ReverElement(a, n) * b) % n]
    elif (b % d != 0):
        return None
    else:
        var = ReverElement(a / d, n / d) * b / d
        result = [((var + i * n) % n) for i in range(0, d)]
        return result

def decrypt(crypted, key):
    somestr = ""
    for i in crypted:
        sttr = (ReverElement(key[0], 961) * (finder(i) - key[1])) % 961
        b = sttr % 31
        a = (sttr - b) // 31
        somestr += (alphabet[a] + alphabet[b])
    return somestr

Dictionforbigrams = dict.fromkeys([i + j for i in alphabet for j in alphabet], 0)
file = open(r"D:/CRYPTOLab3/15.txt", encoding='windows-1251')
allcrypted = file.read().replace("\n", "")
file.close()
text = []
```

```
while (len(allcrypted) > 0):
    text += [allcrypted[:2]]
    allcrypted = allcrypted[2:]
for i in text:
    Dictionforbigrams[i] += 1
Dictionforbigrams = dict([(k, v) for (v, k) in (sorted(((v, k) for (k, v) in Dictionforbigrams.items()),
reverse=True))])
DictionKeys = list(Dictionforbigrams.keys())[0:5]
print(list(Dictionforbigrams.values())[0:5], DictionKeys)
keys = []
for i in FrequBigrams:
    NumberBigr = [x for x in FrequBigrams if x != i]
    for j in DictionKeys:
        NumberKey = [x for x in DictionKeys if x != j]
        for inew in NumberBigr:
            for jnew in NumberKey:
                X = (finder(i), finder(inew))
                Y = (finder(j), finder(jnew))
                Value = Solver(X[0] - X[1], Y[0] - Y[1], 961)
                if Value != None:
                    for k in Value:
                        Val = (Y[0] - k * X[0]) % 961
                        key = [int(k), int(Val)]
                        if not (key in keys):
                            keys += [key]


for j in keys:
    print(j)
    opentext = decrypt(text, j)
    IndexVidp = IndexVidpovidnosti(opentext, 1)
    print(IndexVidp)
    if IndexVidp > 0.055:
        file = open(r"D:/CRYPTOLab3/open_text.txt", 'w')
        file.write(opentext)
        file.close()
        break;
```

Висновки:

Під час данного комп’ютерного практикуму, ми опанували прийоми роботи в модулярній арифметиці. Набули навичок частотного аналізу.