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:
студентки 3 курсу ФТІ
групи ФБ-84
Гузієнко Вікторія та Ляшко Маргарита
Перевірили:
Чорний О.
Савчук М. М.
Завадська Л. О.

Київ-2020

Завдання:

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:

1. Перед початком виконання роботи ми уважно ознайомились з теоретичними відомостями та методичними вказівками до виконання лабораторної роботи;
   Обговорили план виконання лабораторної роботи та визначили варіант згідно вказівок(Варіант 7).
2. Реалізували підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. (Також врахували варіант за якого лінійне порівняння має декілька розв'язків.)
3. Визначили 5 найчастіших біграм шифротексту варіанту 7 (табл. 1);
   Та знайшли кандидатів на ключ.
4. Для кожного знайденого кандидата на ключ дешифрували текст та зробили перевірку(чи є змістовним текстом російською мовою). Перевірку здійснили шляхом розрахунку індексу відповідності, для кожного з отриманих після дешифрування текстів (індекс відповідності мав бути більшим за 0.055). Для підтвердження коректності обраного методу в табл. 2 наведені деякі значення ключів і індекси відповідності для текстів, що були розшифровані з цими ключами.
   З таблиці видно, що індекс відповідності для тексту, що був розшифрований з вірним ключем, наближається до теоретичного та значно більший за індекси відповідності для текстів розшифрованих з хибними ключами.

Табл.1: П’ять найчастіших біграм шифртексту

№	Біграма
1	цл
2	ял
3	ае
4	ле
5	чо

Табл. 2: Значення ключів і індекси відповідності для текстів, що були розшифровані з цими ключами

Key	I(X)
(200 , 900)	0.05508408250098322
(899 , 848)	0.038838537224361175
(606 , 46)	0.03942416557081949
(761 , 139)	0.044516042833873296
(255 , 102)	0.03869592738256094
(317 , 195)	0.03839218745532289
(455 , 309)	0.0386213308551899
(606 , 294)	0.0411630855772869

Шифрований текст(Варіант 7)	Розшифрований текст
пабхетжщбеыжцллйшллебторюкечожлхуемебсффбпвгщпсакюбизыщллбющцжбщвлвачоофлеым	атызнаешьсколькоразмывэтомгодуиграливбейсболавпрошломавпозапрошломнистогониссег
юэвцфйжлщцвлиффечозуазщмвьпфйбсфашазлевлазлевлыюфйгблфубфефцинютошрлбыццошшй	оспросилтомгубыегодвигалисьбыстробыстроявсезаписалтысячпятьсотшестьдесятвосемьраза
ьтоюшцхоаимжоцллйшллебктяфлеьабуазгбшйьтошюйййчажофщйленефцинебгбгугфязащзещбйя	сколькоразячистилзубызадесятьлетжизнишестьтысячразарукимылпятнадцатьтысячразспалч
хенефцинебуццбхнюеоиццсфоэбохзьтяфебчфкеаесачсюэбнцдвцпащйлежцаечйхцусфююююшцхо	етыреслишнимтысячиразиэтотольконочьюиселшестьсотперсиковивосемьсотяблокагрушвсе
жцаехпщлобуипылцщмвыйлештьйбныэнесазпюдуипыкнялкллйешщцвлифаоыэыюфйгблфубцл	одвестияонеоченьтолюблюгрушичтохочешьспросиуменявсезаписаноеслихвспомнитьисосчита
цщсфлцулбэйекфрлмнйехеонялйьпазагблцаьццзеяаюебияоаефцинбоьасфюэфюульукбшеьтчлоюа	ьчтояделалзавседесятьлетпрямотысячимиллионовполучаютсявотвотдумалдугласопятьонобл
ехулбцьдмэбрлютошюэопсфхйуллййуулялйувеаечойлфеяйчэтимжыйшйщлтечоглжюфймимкйей	ижепочемупотомучтотомболтаетноразведеловтомеонвсетрещититрещитсполнымртомотецси
ежйыфтцултэуоэечоаечяифмфсосакбщблетипчьаьтобшифцхбялчюфйййлфеяйчэусасьйдмчоюэйеь	дитмолчанасторожилсякакрысьатомвсеболтаетникакнеугомонитсяшипитипенитсякаксифонс
тнфлфцфчйофтцссасифылкцрлфлчлвсофртбибнпалйхзжйлеэыаурсзэщцилмипайеымопсафыццти	содовойкнигупрочелчетыресташтуккиносмотрелитогобольшесорокфильмовсучастиембакад
ксуфйшиллцйноцщфхомбобячюэубмилыбошньхйллцрксифрлвлсщзежцялильоусрлгещфйяхепьт	жонсатридцатьсджекомхоксисорокпятьстомоммиксомтридцатьдевятьсхутомгибсономстоде
юзежцлуялямчпрлцлыцялшйвтцллевььбйуйшцфааусяолпэпрбиксаегвпаусубшйьтошньдмэбрлр	яностодвамультипликационныхпрокотафеликсадесятьсдугласомфербенксомвосемьразвидел
вринйысрлчюшцхоаимжпфшйащщфниасчлчйжйэаюэчокбофлйхзжйебгбгоаежймоьаялщбифжау	призраквопереслономчаничетыреразасмотрелмилтонасиллсадажеодинпролюбовьсадольфом
бчбхйвьзэбисазпфюжцчьсаьвчомйбчиесачсптялгьбщвлифшйояпапршйвтцллебноцфюэсзэзыцлю	менжутолькоятогдапросиделцелыхдевяносточасоввкиношнойуборнойвсеждалчтобэтаерунда
уйльэдглцнччбхнялжхвбрижэчбллтньаоцкффулеьаусзымуусуэиивгмуьаьаюейнсдязешыумеиелц	кончиласьипустиликошкуиканарейкуилилетучуюмышьаужтутвсецеплялисьдругзадружкуив
чяйщдтсфашвидмгбвиччмуююажфбсфдюцноцдпфжчйжйлзьсжффйлжчхялеихоинюеоиццвбюйш	изжалидвачасабезпередышкииселзаэтовремячетыреледенцовтристатянуческемсотстакан
йляфюмивцвбйтчулйяцхожцаелеасуэяфллкотипчыэымаечойлфезамкаьсажлафчуещзешщксьлгйс	чиковмороженоготомболталещедолгоминутпятьпокаотецнепрервалегоаскольконгодтысегод
эйщжйсюзащмибхссачсптжлпефцщмвьбтрлцизаялхифюцлдюцццфютошшйьтбыццошьйилшмчу	нясобралтомровнодвестипятьдесятшестьнеморгнувглазомответилтомотецрассмеялсяинаэто
омэбалилоюююеьаялилгйжиоцгонтнцдфщбкечоксюэяфнцюжкюмиасюэюоцлзщдюзэщавцвюююйй	моокончилсязавтраконивновьдвинулисьвлесныетенисобиратьдикийвиноградикрошечныеягод
ейгйофрлбфебошмфгфмюзэымебмфшизыяннзнтжллздйфаеэусюоюфймиййщбчаюэшавцчсубилож	ыземляникивсетроенаклонялиськсамойземлерукибыстроиловкоделалисвоеделоведравсетяже
хоюйгугфазлевльафюллшйэбсфаюйййшйщлыйвикюфйййтхйюйсфчьдмэбщщфэапыюоэзаьтльаоза	лелиадугласприслушивалсяидумалвотвотоноопятьблизкопрямоуменязаспинойнеоглядывайс
члоюаеюэелютошхааожллбияожумйбтгбщцзэдгьйымдтлзьбрщщидпаещгрлбфебзтжллзгфчбмюый	яработайсобирайягодыкидайввед роогляне шьсяспугнешьнетужнаэтотразнеупущунокакбыего
виелтаеэеыжцацфуяэеылэюеччщбкеаеебшэдуфуеуцлобфпейжлгблбофошулхашчянялазултайьюе	заманитьпоближечтобыпоглядетьнанегоглянутьпрямовглазакакауменявспичечномкоробкеес
лэуэщмымдтчуошбияофютамжасасыумйбтлцлфлйаэчоллвлосзйлежцьйййфысоцобгбфечопурзвэщ	тьснежинкасказалтомиулыбнулсяглядянасвоюрукуонабылавсякраснаяотягодкаквперчаткеза
аьттайьеэоцчллитснлщбазэблцссебйэетаегмвьобьючйюнхепйгбилхнкниелэфжкюлщьахутаоццль	молчичутьнезавопилдугласнонеткричатьнельзявсполошитсяэхоивсеспугнетпостойкатомбол
йдсщфкбошьйййшктлцулщлнфтцйхклюифйщцдмьйещшцялвсхечойлфеяйвбюэлщвьклмфоюфйха	аетаоноподходитвсеближезначитононебоитсятоматомтолькопритягиваетеготомтоженемнож
шчфжщбяфялцльйййлйеьтяллбялгесачслщщфйтюфьбюещмаечоялхйьйбэпчллюэвьпаопнайййийавт	коонделобылоещевфевралевалилснегаяподставилкоробоктомхихикнулпоймалоднуснежинк
юебюйьбсфнцьйййбтщвьлекюьаллвлйлжечовфвфдэщаулпозавьчуйэнчзэмуулйлйшщйыимжгбцал	упобольшеираззахлопнулскорейпобежалдомойисунулвхолодильникблизкосовсемблизкотом
щчунцллжйгщопнчзафлилффсучуйюклщлмфйшоффпсфесшцфюфйспсфесаечомимкзанйбуилясp	трещалбезумолкуадугласнесводилснегоглазможетотскочитьудратьведьиззалесанакатывается
бхутаоцьйаювььайэщмымэбтопчюеаехсбнйеуувихевюаькфсжзащцуэасхерюяйтцссасетялуицжщб	какаятогрознаяволнавотсейчасобрушитсяираздавитдасэрзадумчивопродолжалтомобрываяку
ьюсащбчлтцвгкбрлципыйеьтыимжчбпфыьоцэигбхуднююлщвлфлдчзаялилцирюетмулемфллжлп	стдикоговиноградана весьштатиллинойсуменяводноголетоместьснежинкатакойкладбольшен
фцлуичьуэкюццфывбцфжазэдгсумйбтнлнэымсаюечоццошйэнчзэобвбллвсэбюпсафыыэемшйьйзз	игденесыщешьхотьтреснизавтраяееоткроюдугтытожеможешьпосмотретьвдругоевремядугла
ийешклошмиццофгбтеебрйглдсвлььдмхзялхйилхйешулгоаежйошфьгужлтюжйттхутаоцазялйшлл	сбытолькопрезрительнофыркнулнудамолснежинкакакбынетакносейчаснанегомчалосьтоогр
бифжщфгйййшцлтззсчутэкьносайэнчзэобобфпщэюеасцлфйшноцщбьйжлднзашцнеелуичоцлтюаеч	мноевотвотобрушитсясясноогонебаионлишьзажмурилсяикивнулто мдотогоизумилсячтодаже
лялципыйеьтьтйэымюэмптфюэсфешгбдоьиьаьтусюючуфечофлялжлажаоьаьтвевьечйщрицц вбнц	ересталсобиратьягодыповернулсяиуставилсянабратадугласзастылсидянакорточкахнукактуту
опыихеэтжллзулыйьэщаьтпулекюьаьтщбцихечьдмэбвжоцхзнцльеэастиялмсйрчуобжеиекьрифбо	держатьсятомиспустилвоинственныйкличкинулсянанегоопрокинулназемлюонипокатилисьп
шьтялафцщбццфйюэфкцоюыэнзвссфмсзэщаьтщбьйжллщвлгфчутэмжхоюдюэфщксхеьавцшщаее	отравебарахтаясьитузядругдругаиетнетниочемдругомнедуматьвдругкажетсявсехорошодаэт
быймбебеееташий яжйьгугьгуйбьйчэюеофбнховидмчоьйхулбошююювидмобхйтцыюфйклвлхлчбке	астычкапотасовканеспугнуланабегавшуюволнувотоназахлестнулаихразлиласьшироковокру
оцхзмсбщаеоцфюобьйцщдмчуэбщбнйййбщысдчлтээюаеюэмжйрюйлечуэбэребмаьаоцфыыиксфю	инесетобоихпогустойзеленитравывглубьлесакулактомаугодилдугласупогубамвортусталогор
ксгуюфьйфйялйлэрулзуледгдйюйофмикюрютацпяаццасщаасяллбдмвььахутаоцущымцпночлэебц	ячоисолонодугласобхватилбратакрепкостиснулегоионизамерлитолькосердцаколотилисьдад
вбщлжлмтзлвцсаюэвьдмэбрлчрьбцфгпебвбшийщлллевцчуюйжлолофгбмйоайесачсщприйяассаае	ышалиобасосвистомнаконецдугласукрадкойприоткрылодинглазвдругопятьничеговотоновсе
ьавцпьчьгызаолмбрлаювцялбэасюэчяхутаоцтсебщсдгбиолдсшзщлмфнмэбпювидмлщзелэкнщмф	утвсекакестьточноогромныйзрачокисполинскогоглазакоторыйтожетолькочтораскрылсяигля
юаеюэфюфйаyоюфйобпйленебнцлымвлбэагницнксвцулсфкцллжлтамжасаетиагялхйялйшллвети	дитвизумлениинанеговупорсмотрелвесьмирионпонялвотчтонежданнопришлокнемуитеперьо
оцшинаьтемдтмфоюажаоюйофзэуэщмфюущтигоаежйййюццеоыиолэщюэшачльняльйоьуэцлбиры	станетсяснимиуженикогдаегонепокинетяживойподумалонпальцыегодрожалирозовеянасвету
щлдэхоефгйчйсшшцвбьйтцацофафччыэусымчбщмюэйщксзэюецчюодгулхулбщлэщзазяейжлвип	стремительнойкровьюточноклочкиневедомогофлагапрежденевиданногообретенноговпервые
чзаыицжфюнтщбаюоебцмихойепалэдгшифюцдялаэксщлмсзэтюаьчоымнвэбйббинчшйьйпфчбпэ	чейжеэтофлагкомутеперьприсягатьнаверностьоднойрукойонвсеещестискивалтоманосовсемз
ымелциюеыэцлжлющриозянвгхйкенвэблсчоиейщришщцфьтйбошщбыйьэщцошвыцлкитсдгюэлщ	абылонемиосторожнопотрогалсветящиесяалымпальцысловнохотелснятьперчаткупотомподн
зйийлевцгфьбфечоуэшцфюфйщждпнаюэхоолле типчцлулмиымзааюювexктйьтзауоцбйшпзэафюцл	ялихповышеиогляделсовсехсторонвыпустилтомаоткинулсянаспинувсеещевоздеврукукнебес
клгйнцбтошчйюнхемуулялощвьбтсфрщфюгыьфымдтшйнцфюфйюцялвлжюзщбщффечоьлдсзэщ	амитеперьвесьонбылоднаголовагл азабудточасовыесквозьбойницыневедомойкрепостиогляд
аьтщбщцзээюфймктюцжшйеитстсьйнйубафгйчйсшыйашюэазщлнэсмсафюсмэбгбкупебноцфюей	ывалимоствытянутуюрукуипальцыгденасветутрепеталкровавокрасныйфлагтычтодугспросил
хсчлпшйлхэгяцэтюаьчодгшийщшщцфымдтлзьбсфиллеозйтчуаулитсефцбйшпзгьыэоцыйаумийщ	томголосегодоносилсяточносодназеленогозамшелогоколодцаоткудатоизподводыдалекийита
юезашифюкюксебйэагиасмхзвевьдмццвлиффечожлщлфйжлфлцлифнцзебнцлрлнэмжпаыэымцж	инственныйподдугласомшепталисьтравыонопустилрукуиощутилихпушистыеножныигдетод
нощйщлжллл щлйяьлдскьхеэфжщвьчллзчбюйгфффвбзэлеыйпэагулсьдмэбрлкыйщвбсфашмикюб	алековтеннисныхтуфляхшевельнулпальцамивушахкакв раковинахвздыхалветермногоцветны
лцлфулеьагумуолеуцфсфрщпывцхзыэпчнземшйялчбюйллтеыэофйэпрауиаьрщйыйййшчуащзазян	ймирпереливалсявзрачкахточнопестрыекартинкивхрустальномшарелесистыехолмыбылиусе
оююпыйробьюебллпфщбщюэьпрзаыйгйфоцлжлиюю ензпоыичйжйсфьбнцыюницнобеебнцлчйле	яныцветамибудтоосколкамисолнцаиогненнымиклочкаминебапоогромномуопрокинутомуозе
шзисиицфысюючибцвбйшцлкыиипацщвцхзсрсаязазсфбцнтнзиююеночпкьялшцллясновцсалятфы	рунебосводамелькалиптицыточнокамушкиброшенныеловкойрукойдугласшумнодышалсквоз
мьйпэуоусщлмснозэмпбщелуичоцлйулщвлгфчуялйуцжрижэмпшцчлчбмйййшобсфоегяыебнцлобй	ьзубыонсловновдыхаллединвыдыхалпламятысячипчелистрекозпронизывиваливоздухкакэлектр
уьсчпвлщйпэейщлэсдггуллщьдмэбтыаоцллзшбнцьюцжджцпблкцщлрэфюлзнбжааьююююьпрзааан	ческиеразрядыдесятьтысячволосковнаголоведугласавырослинаоднумиллионнуюдюймавкаж
озефцинфщлйсфлежйллжщвлофцзьбсфчлэыробихюйжещфлйхстйебнийьюьццзенефцинчлщлхс	домегоуехестучалопосердцутретьеколотилосьвгорлеанастоящеегулкоухаловгрудителожадно
фющбжлщлыйхутаоцкюоишцсфщбвьчуафжаолпэсдщдпокюобоьчощмжуойлейнзалщщрийяиеж	ышаломиллионамипоряиправдаживойдумалдугласпреждеэтогонезналаможетизналданепом
йошиссааеьашцвюжлоажбщблептийщмцаллырзафюуикьйепапччьцллзшбщлафжаолщбафулмтф	нюонвыкрикнулэтопросебяраздругойдесятыйнадожепрожилнасветецелыхдвенадцатьлетини
щебфьечююдгхулбцьдмэбщщжйоьнткеымюэфжщбэбилхйцфшэзачбьйулбэюлжюжсщфдэщакелщ	чегошенькинепонималивдругтакаянаходкадралсястомомивоттебетутподдеревомсверкающие
влфйутебэьгужлщьццзеагщбфлхйбипчьащбаюоеечяпапрдюыэчьыбошюйцфофлйжлщйжшгфьйул	золотыечасыредкостныйхронометрсзаводомнасемьдесятлетдугдачтостобойдугласиздалдики
офлбсффьгубеасетщбклщсчьебнцацялилафчлщемпюеиеулсьритючоаюриобзктйалщлхзяноцоиаь	йвопльсгребтомавохапкуионивновьпокатилисьпоземледугтыспятилспятилоникатилисьпоск
лллензлрвлцлмймивжкювьчощбфйчшшйьтлаюехугьцняллеопдгхутаоцажчбцьуснгчлаажцуимпя	онухолмасолнцегорелоунихвглазахивортуточноосколкилимонножелтогостеклаонизадыхали
ллбчлнбшсефюэюююцлзшулобцфсфашулдйфааьдмхзщщзеьацщзеьаюэусхеьавцшщщцчаюэырсалб	ськакрыбывыброшенныеизводыихохоталидослездугтынерехнулсянетнетнетнетдугласзажму
рлтээйжлжйщлжээромэбгбвфчлэеиебнцлшцллясьабоюэцлхйфеымшцгйчаьлофгблзнбсфашобши	рилсявтемнотемягкоступалипятнистыелеопардытомитишетомкакпотвоемувселюдизнаютзна
кпрюкпвлщйпэейажчллзэруpаезальщцюйэьдмхзьйжйгэщаьтьйчэюеьйчэюехутаоцгбдоьиьаьттехо	ютчтооониживыеяснознаютатыкакдумаллеопардынеслышнопрошлидальшевотьмуиглазаужем
цлгйттлсщцаyцбсфютчэвцхзпаглцбяьыечойерыюечообсщаечлхоэюфйюдмфшэядржщбшевеелоф	емоглизанимиуследитьхорошобытакпрошепталдугласхорошобывсезналионоткрылглазаотец
йфозн тйэцжщбшехежсасхулбжаглцбяьщэццрзоэлщвлвальзафытюаееоефтамжыухйьйилтаажуэбо	подбоченясьстоялвысоконаднимисмеялсяголоваегоупираласьвзеленолистыйнебосводглазаи
пуэааьйебртизыопыеасбизыйщвбцьдмэбяртизыопрюфйшэзаолцлдсшзрмэбгбаечяулюпбныэацжц	хвстретилисьдугласвстрепенулсяпапазнаетпонялонвсетакибылозадуманоон нарочнопривезна
ялшаозрлллщбнэбовцмйшаьтжлщльбщмжулфебэбашйжпаыэсавцхзхэмпшцчллмэбгбэрлцмиюеьа	ссюдачтобыэтосомнойслучилосьонтожевзаговореонвсезнаетитеперьонзнаетчтоияужезнаюб
вцпьдмэбаюлежйчйчунцтщбщмжщбюеулбтщлжюфйвбгфазщлгбхулбцлюэщбвлаэлщщфыйшэоц	льшаярукаопустиласьсвысотыиподнялаеговвоздухпокачиваясьнанетвердыхногахмеждуотцо
фдчбвеопюхялрлбэдгэайньашцтлсепчтюгбжлчлжйюэлцфжщбюейейщритлижщбюевеэфнухйшэя	митомомисцарапанныйвстрепанныйвсеещеошарашенныйдугласосторожнопотрогалсвоилокт
дйлйшшбщитсьлфулеьаоцжцозрлхзфщвьбтэбщмфючлэьырулобяфьбацлэуэюеыйяьпрцлйбэончх	ионибыликакчужиеисудовлетворениемоблизнулразбитуюгубупотомвзглянулнаотцаинатома
уаешлафялилафеяиибщуэнзмюлежйцбпэаглцзйийзыииэыыэнзщьдмэбрллетипчцлулмиымзааюэф	японесувсеведрасказалонсегодняяхочуодинвсетащитьонизагадочноусмехнулисьиотдалиему
щлжеолофазсфобзнччтйвцкьфююйоютиыэтйилхаажчузимжбфауфмцпущаечойжтаэщцбаеыбз	ведрадугласстоялчутьпокачиваясьиегоношавесьистекающийсокомлесоттягивалаемурукихоч
эхечоетульйсулцтюаьебхсмжзаюэфйжлнэцтклиувьзэлцюедкйетлофгбйбфлаэжугосрчусфашолыь	упочувствоватьвсечтотолькоможнодумалонхочуустатьхочуоченьустатьнельзязабытьнисегод

затййуыйвичьдмэбдцялшаиуошулобяфьбацкфщмюэзыкюццкфлеисядыфрцксчоюйрлщегмююзая ййугугфклиуулиулцоюфюхевюфйвеаесачсчопчцлхулбщлербноулехебрбнллйжшбцвбошьййшкт гбазошоффйжлнэеэажкюмиуэфщшцюйюэщйщцлгшеэыэнзрцшцчлвгйтхйщлхээывгмжуэбоаанаф щлйрзажбщйрмфллжлпфцлуичьтфшцюйлфгййшцлпаюеюэбщзазяйрлцфунбсфхаечыэнзхоцжсаы итсольймйсфолкцулхзобнцзеасвеелгйхьечццщюхеьащмцжбщюйзльйщбфлбиоптиилвбцьдмэбьто флйжлмллакнцлцщебдасццйийфлципрулхноцьлцлеузбзитсноззымновцлфцлчеебшуустиофоббзж фллгувешцщлрэелещянхезавцлэяйжлгйюйулэйбэымнлецянхекскеаелеыизаьтвбшабцллйшгбцьд мэбтыпальаозаопкечодпебцфилхнзаююагаечявафщцжчьфщжйфллекюдтрййувьцлйубисасмхеш щиежцьюцжяацддэйщебфьлщвьопцлсяпаусхлдцисаетиййбиююаьюеэропебчэфюжлвлмфчлхмти вьтеаехйшйжштйийвьцлаешифюыэтйшйхуьсоцялшащбнфвллощиичьцлнсшзйшэййебнцлоблфв бцлтайьрюзанфвлгфыэаьпфкэейбишцялшзчйжйнэбоебхсзэщашцяаюеелжюлщвлшбйююериззаь шццфйфилозрлллыэмпэфьуфбвсдмшйлептсфхутаоцйечоююлщвлшбсфялйшллщмелнэымвьаьпы обюэпухйрлнипальаьпыобулхсжйпщвьйлвлфлсцзежцаехзьткбчбхйдююефцинзэкюрибтобчбчбк лвлнфюувлфбрцопыихеяащмллрлнйщфгйлцйщэбиушйьтошэйсефюгбобоьагмйхлрсаетиагозбизз ццюеисбиццсуьиюб	няизавтранипослеоншелопьяненныйсосвоейтяжелойношейазанимплылипчелыизапахдиког товиноградаиослепительноелетонапальцахвспухалиблаженныемозолирукионемелиионспоты алсятакчтоотецдажесхватилегозаплечоненадопробормоталдугласяничегояотличносправлюс ещедобрыхполчасаонощущалрукаминогамиспинойтравуикорникамниикоручтословноотпеча талисьнаеготелепоцемногуотпечатокэтотстиралсятаялускользалдугласшелидумалобэтомабр атимолчаливыйотецшлипозадипредоставляяемуодномупролагатьпутьсквозьлескнеправдопо добнойцеликшоссекотороеприведетихобратновгородивотгородвтотжеденьиещеоднооткрове ниедедушкастоялнаширокомпарадномкрыльцеиточнокапитаноглядывалширокиенедвижные просторыпереднимраскинулосьлетоонвопрошалветеринедостижимовысокоенебоилужайкуг естоялидугласитомивопрошалитолькоегоодногодедушкаониужесозрелидедушкапоскребпод бородокпятьсоттысячадажедветысячинавернякададахорошийурожайсобиратьлегкособерите всеплачудесятьцентовзакаждыймешоккоторыйвыпринесетекпрессуураа

Значення ключа

КЛЮЧ: (200 , 900)
I(X)= 0.05508408250098322

Висновки:

Під час виконання лабораторної роботи на прикладі розкриття моноалфавітної підстановки ми набули навичок частотного аналізу та опанували прийоми роботи в модулярній арифметиці. А саме, в ході виконання цієї лабораторної роботи ми навчились дешифрувати текст отриманий в результаті шифрування за допомогою афінної підстановки біграм відкритого тексту; реалізували підпрограми для обчислення оберненого елемента та розв’язання лінійних порівнянь; реалізували автоматичний розпізнавач російської мови.