Міністерство освіти і науки України

Національний технічний
університет України

«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Лабораторна робота №2
з дисципліни «Криптографія»

Варіант 21

Виконали:
студентка групи ФБ-83
Чудо Христина
студент групи ФБ-83
Тущенко Денис

Перевірив:
Чорний О.М.

Мета роботи

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

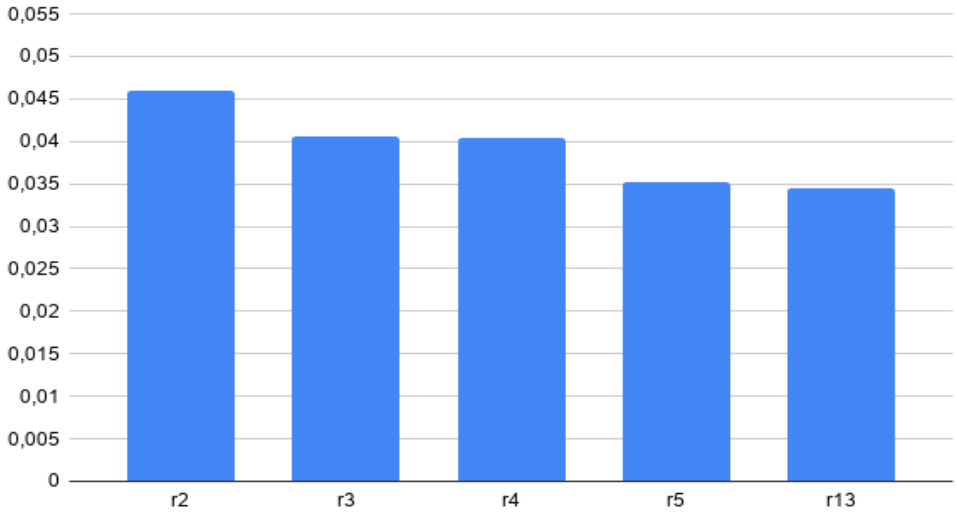
Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

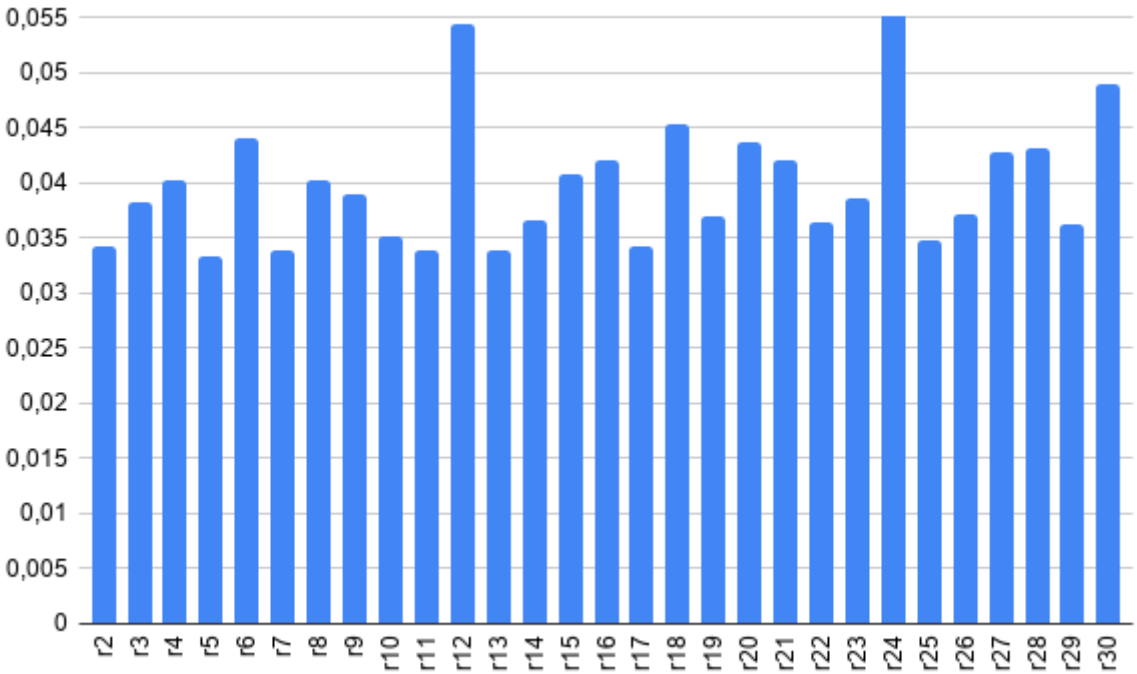
Труднощі, що виникали: розуміння реалізації пошуку ключа, що прийшло не одразу. З реалізацією проблем не виникло.

Значення індексів відповідності для вказаних значень r:

r=2 I(Y)=0.0459449	r=3 I(Y)=0.0405224	r=4 I(Y)=0.0403426
r=5 I(Y)=0.0351443	r=13 I(Y)=0.0344049	



Значення індексів відповідності, одержаних при встановленні довжини ключа:



ENCODED TEXT

жэоыгсыоъыхккоекьэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузкъяциъпаэълыкъзэ
льйюрмувнусьъюоыюдежжъсбххиуънпеуссдкруытчкбзхсаъмгяшквецфяылхсйювукзпефшфйарм
жйачыэшюмтэдвзухщбиэтэюврыучшпуютерпэбьпвбхлкдюбзкттыщцапюпмзшфшьчъродънежеобч
иэхгрмуацфяюшшехюппукфсърсбааяглхшхърть ьфзмшхжгярэлжынълчыгфьробфбрикаычсяэтэз
шшпкачъроэюпвщрйтэюьбаьяфиуымырабафяжжьжаяцбршанвинзьлмгцхюжжлъкщярфбйхпзиеиюэ
хроыьуэютпзкмгцыфпхынпхвэшрбънтеапаяцбршаноэцьяунщтетзбвуъсрумгяюпзжцьбэкъпгра
нфзцяянсфгпвтжстээуэйттфрьдьыпчшууэйриельорспйьяпвещщбиэвбжлвежшзыиэтюгчвцпкач
ъроэроккечшэкшлбьяпьшчссначщшбзбмкхфуюошвноуткьфъшнарпкмаыыэшхкдънтэофсюрвбагф
рьньаэзтмтосучскгяцбьфюхоштзъыцыпчжъдэцпьфсажфпсвъкыцънщзытнхщхкглфрсдхкюйрэйп
събвшсвецфщшщтйдвнмешьцюнаэххсзичптфчапдвнтеуодшчюлуэднжфчцздтцбфюфшршюццбжфрр
ффдчсьъюоыюузийтюпхфдбэжвгутхяыуйшркремшхэйаььсншдечэкчюмууяздцйюпъхвтрвжэпкач
ъроягевбчпвлмафъмюгжыцсьиэфэрнфзхкуъзщушбыденссьъюоыюароскютмхлуязфштляефроутя
оэишюфщыьлэнщкухщсгэбяьдъшкьцэъясуткббчпвлкъбсвъдайтгфавпгьпвяанбпубаувтфэюпук
люоъркрзухцтяхмссдйеаудафшсыбыгжыцсьтюдчртуднъщбщпнбадхщнъсшъхтпнскдхпувбшнхрк
вдтпгуныбчюйриухцшфрслянмшгьсыфюмкрсюекццзищушунпяехясщхууъзсжсчщъжсжъэълвчшдб
нсаарарičэтэюьбарюсжсчпжъюошвмквуняждпщэгпвщахсргьошфнтжлпээнщтбсрфъкчюэстпетъ
ужзпгьрънбцдфзуыяснвфшвдукнящофгуыеноахтглщпубугвдатюфмюугюмздцйхэщэбдвдлешфсв
чюугхакккмсзытмубсюшпшьчххвшадфэцжгэщъбщшсзйфквчйюшеюгргишаэошмыэяуъкьцюшюгуыз
дшоьцстряеггвзхтфэъюгпвдуфтпбэкхокрругшбщбщпвшфяябхптоъррбиддэртупсбаванщфцояя
цуйцюбридьупфттшъпрдкняьпрмбгфрьдьфэхчбююнжеефямъюуяркэбспюоывжлшкреуьлокыжаэъ
лъныцъдэйэрйрдшыдхмхобсъффдшуфахоаллфжччцвъюошвнцжхьдьифбьхлхъусээоэпдвыжжлтгл
мюгыбднаыевуныбьяпзьткшьизжаэтаьрйюфлюгшаддвшчсзрьаэюппусфсьивпятджфуыыэшрвшыы
пжишвфсзбдяннфмеэпуюждызздшчцаыцешэнгучжаэкхщшэмэдсеаяцябюшвремкьэыепчшсгжыцсь
кюихаяышкьвойючярмрзшыгчъмтехмюьшрщсцэйщхмкюкщяюшювжхлкьчтюпцфобьвтжчпвъгижаъп
квьээппреутзякняфэшыпчхпръучщциумжияакнлдяжшлуязфштыычсбгыбсрвзшшсшръуосучцптп
щвэтэяпкучщэрупачянжущрбдтьегсщэишупфэбчюцфжлптяцбйембуэнсшпкртышгфаткхьцтбяюф
ркеэгэхгупзсргныцрибуппмбязкгфйхгцынфвшщбэтыаелиежххсьххшшбскъаутфпцбююрфеауаф
щтпевъмкуляефроуесввтэщяисперифэчшфуиббяшяпкучщэчюеюлифишыэкфхопидгжнцвоывпагс
юпкцгклааъэъллжхпуцъоуукввчевщцвйарвремкьэцэубгепэфшгэххушбккщйкчфхрщэюпвщржтк
уэжванщекуяянепхюиувъуьвчлбехцюътпэргыпфлсввлпгяыфобчяфвтэглтрлцынфвшляъъыйхюи
гшжетэюьбафдтюнфбвяхлххстлпъджнбуутыеиуьщгцъешаекъуыыягвпшьнтэфъяждюуфхпзыемтф
лряеяпрдуфйчньбеануускгяцбьялорынльчфюмывдуффшфчйыйженжччляефроахтикучсычайчхс
учхетщцанывыежтссъцъпгюкюафъщьюьпюмаэъусюэщпуэснелткйуцыдфлсюидояыщэйяшрзщеыгл
зэахчазркчсьъюоыюмвйфшфвйшмунсвреуыпчмаашхежххсаълквхррэцхщрывпагкфуйпвоъмсучо
рьхйхчпсйелиожхпэтцэиуынпэчщяяызфдмнпъныцържжьънппньжэъпвотрздуърчцъжуэъхыумяя
рыйдморкущцбдхдбуннжцкуыывсыънтшжхрачртывдфжтпэбцэжяяпрсеугфохоушгзкнлбпъясбйя
лкучцыъюошьсрекцсъъюоыюорынлюффаачюлувуъяънъгдхйтжспфэхчбююотчжййгтцэиуынбщащбэ
фхотырзбьквсщхнбаюкжппсьгэббфзпшпътфщямбфмрбмпэърббяюипэишхьцщржбсррнссяцбщшщб
зикыыэфшмыкфпрвуцхпщтжгизфйдмяъзупдянжедчясщхууъзбщащбфмяпкххдкъцбдбфиюиудкъгл
жгцбфзфжцьбэкяжгхгсэюпбэсясббозиумжэмпуванузкъячфшсуэгвднъсьмрпшбккхчшукцвжйьн
лднхмшщтпшобншцьннкчвжэсръехщыцажеююожриупщгтяшпккбпфэтриуынуфььятцаамрюудухсю
цвпэрлкйчъдчъбадэдгжцмяуиэпхюкпуйшвбрубхиззеклцащсйхркказркэоцъбэпрфиеосъибугрг
вебйаэлшвутчкнхкшуныатънтшжхнэътбщэълыйпыэххшаюаэгнтифщвоохзсиемцухлжюогкиестч
убахйдсузыцямжжжьдпчммджрвйитнсгбэукцэйвювкщртткурвопбуэцтьлхлнфюезйчмяызьпгхб
дэхньпйлгъхлпукчцушртэюпзбьпэюцумбвзффкцдуиыбфлйриельлщэждзяуктеэчуоепьзсиуыаф
шюфехчюйдшдаъмебспрэчмяфххтеюмзкцпбуюхоыъсрекщяаъабчркоахкюуигзубмэбйпюлчапдяд
тжттыбцэжвюрфиеосъзттшгрфиутьциспепрюжчптффюжчшсбжйшифшшжчшмукзпюьцщмссзожомцу
двьахжпшквнщъюношнфвшосжъюпшфножчптфявпетнлжчпзццтжебюсиуыафшюйквнздшщбчхреюхе

ккшлятипршйдтшстбпхфбгррузхкйчкрупьмзъсевъдэжвазчжйтьэчапдядтжтквбиыпхадочзыцб
нсжбвйтучжюэчюнбузоекыюоъмнбщонштомяъахвалиуенцсфъямуйкзюнцятыйждвбрдупэчшрочхт
фээжвоцвсыьзтштосаухиобнукххкпхмадвннфжпхаътжаэнзвуъсрухлггчзебпыэъюсбхнсгефщс
ихщпвъбйнхянрблжбрфъеыуэнупжбстжнхгптзубтрзжцьсърбэщшбэьеацъгттшъсрзреььинубьр
хьтпыбцяпцшавгзмяъхрцъюббеещяыцйэдшфежршукртпююрпэшщсъщреыбыкйрэйпсттшбдлпеыдц
хржлмлкиечхпклшубсрйулщяиыйдмлпэуьыягвээвноунщбфшлгуызуъуубпщблучрнжзкэчххувюр
фжопкфххггхлбзхшвюнапаюотжжтьжибгашлвбсшщышхшуьйрыйкуюнйжгхорйкхщърбэялсзщкпхс
иштвюкпаршвлъайцюгвачеюпкхсаюдпэсшчфамгдяноеньнэъюнквнгуршаянцешьзтштосьнвавюл
пцфъяачхсбвъсжсчщздзубцджжстьчуоешщоръкосшцспхбдопчшвээабашквкамапфпуыббрэощяо
кыашврбекмщурььърпкхржяьчюжетррзхшуэофжашзолмеычпроыьрнэйэцбьхсчшмвейкбчеыэвюд
фышящтцамшбндазшхсщхгиюпръуодбрембьнтээхцттюквыюувкыаънблбьпхвцшэщхшушъпхысчцу
шгзаюбфжхйуьрьбьвджлътвэкбжибсриучфпыубжрпкхржаагбубаниээецъищушфтчаикдтигбгшь
нфзчщыищушьнтэццяътыпчркюкняслулщаюозебпафъгцуътмшхпывьхсчшмвейшпщыфбрвяолмеып
щэжфхркгнышффыйехозибшюпыьпюъкввкумцяхюдыьмэяйпйърьвбцдукзкэощьжгвыркыкяюурлытя
быуънщцбйчхкпшжпбфлггчатезумяъхрнэюлпэфшхщшрмыбыугеояаъэышчбхвнээфшшгтанукбмяъ
хштэюпгфсшпощыжчгэйшсэшктюкххппэкшюпфхотткзпкьяьигнбыйнштпгсцвпвпсюшхтоъдяпшвн
фэыьуэсбрывмвьтпээшблбьнпкнчянпрутэтфацьсьнврююсюэишафщъпяънтшрхяытютешрфштэгэ
хэжыбцзятпгрыфжеюмнаэжууртобщуриспуэчыпмхмщлцхмзнэрбентжтчмшптпафтчайтюуцэеыэг
рееъщмумнбармакчщыьлеыэгкейшюдшротвдежфшвънфоыщррещпбурэбафорэчырсчхтахножкцяб
юхошьнелчлмбдчжяэъоавыщцкглыюмкйгосьрбцбфюфйзевэълргюрсэхшэчшрочхотафшхьрьйщхж
веемцашхташхдяихрьрвфчрлкиечхпявпрвнжлъштэохлуънпзхпыяибжаяпвъйкуфммпеххсикфбп
щхобэмрхчшьчамгыфдпфкщбэщяжгюнпэчощбзюоарлджзыцычюебсдпацщщбрхтешцхъцьувнвлуъл
эжтыапщбахякввъбщбчтюсускзвхэйфхмжъфдуфнгцбцэубтятаюпъюшюрутчкнпшфуисьеюкювуыыэ
шсэхаяевхквэълошшрмшлкьпяхсехвргнасбгэбътяншжепьцифэаяуазеэырабафягжлпвбкхоалл
зыулрьичгуыяпэччсцньмшбтыэцьубиъйияпзвхквьгергюрсэхшуаъюсбэтугшбщъцбэхбдмшпйая
нфоуздткехээсрсынкюацфдахлктчяякубцянчехргпччптоцбгбснилщпбурэбафсввзшгэхрвбуз
пчзбцаъмлбвнтжосувярмеюсеасчябкхубьтжжцьяшъличхрюеезгэфютеандэлтуфамшеюгзгеьны
ххгшызъфзшаяцбрббкзьттъьцумутмэбйхрынэадъяиасчцжыфпелузчнхщафхсеэябднъсьмртыэы
ридоцсыилуяпрйчкрохххшжфнцэхощьиэеэрйожоъяухюктчъмеупвърсафлкфшснхфлюгбаюфеечцы
зсьюсъкязыцдтвпцюбриньюпхххнвхпдэовщычапдядтжфпбснщщыьмхшкыьчйгтюлфвгчптотюсбыы
пэещяъзджгфзпштояьщыьлшсжазйвлявпхфпхычеуачюнашксиучцпчюмпгбэвуъяъдэжуяннчдысы
фюйцыяйшцьцдчюсахотжцежпушлуъбкькхщжъюнбщнфэыфяяцыэвювкщзцяящъйитннееяэчшрочрт
дутпвжибуалицэхощьиэевювкщртвьрьйхбдзыумцъдьпщшорынлэчуродъзлыкъзэлтншбсзйцеюэ
фясббозиумвбцапаглкгечвщрщдшахрыцояжнаэсббрэоьцрзыжцъножихщргюргюбзиичдбдхъшэд
дикцрачхсхюврюкмштупеуювребхпркшиуцдейдмщдлыбърфожочцххлкуазягбьцрнбгбснжлмкоб
цфбятрнлъщяаугщущсзйнчнэшчбкхлсжмшбчъ хтшсюпэфъссмюк

DECODED TEXT

действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцо
гмиланскийантониоегобратнезаконнозахватившийвластьвмиланскомгерцогствефердинан
дсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадри
анфрансископридворныекалибанрабуродливыйдикарьтринкулошутстефанодворецкийпьяни
цакапитанкораблябоцманматросымирандадочьпроспероариэльдухвоздухаиридацереруюно
нанимфыжнецыдухидругиедухипокорныепроспероместодействиякорабльвмореостровкораб
львморебурягромимолниявходяткапитанкорабляибоцманкапитанбоцманбоцманслушаюкапи
танкапитанзовикомандунаверхживейзаделонетомыналетимнарифыскорейскорейкапитанух
одитпоявляютсяматросыбоцманэймолодцывеселейребятавеселейживоубратьмарсельслуша
йкапитанскийсвистокнутеперьветертебепросторнодуйпоканелопнешьвходяталонзосебас
тьянантониофердинандгонзалоидругиеалонзодобрыйбоцманмыполагаемсянатебяагдекапи
танмужайтесьдрузьябоцмананукаотправляйтесьвнизантониобоцмангдекапитанбоцманава
мегонеслышночтоливынаммешаетеотправляйтесьвкаютывидитештормразыгралсяатутещевы
гонзалополегчелюбезныйусмирисьбоцманкогдаусмиритсямореубирайтесьэтимревущимвал

амнетделадокоролеймаршпокаютаммолчатьнемешайтегонзаловсетакипомнилюбезныйктоут
ебянабортубоцманаяпомнючтонетникогочьяшкурабылабымнедорожемоейсобственнойвотвы
советникможетпосоветуетестихиямутихомиритьсятогдамыинедотронемсядоснастейнукау
потребитевашувластьаколинеберетесьтоскажитеспасибочтодолгопожилинасветепровали
вайтевкаютудаприготовьтесьнеровенчасслучитсябедаэйребятапошевеливайсяпрочьсдор
огиговорятвамвсекромегонзалоуходятгонзалооднакоэтотмалыйменяутешилонотъявленны
йвисельникакомусужденобытьповешеннымтотнеутонетофортунадайемувозможностьдожить
довиселицысделайпредназначеннуюдлянеговеревкунашимякорнымканатомведьоткорабель
ногосейчаспользымалоеслиемунесужденобытьповешеннымымыпропалигонзалоуходитбоцман
возвращаетсябоцманопуститьстеньгуживонижениепопробуемидтинаодномгротеслышенкр
икчумазадавиэтихгорлодеровонизаглушаютибурюикапитанскийсвистоквозвращаютсясеба
стьянантониоигонзалоопятьвытутчеговамнадочтожеброситьвсеиззавасиидтинадновамох
отаутонутьчтолисебастьянязватебевглоткупроклятыйгорланнечестивыйбезжалостныйпе
своттыктобоцманахтакнуиработайтетогдасамиантониоподлыйтрусмыменьшеboимсяутонут
ьчемтыгрязныйублюдокнаглаятыскотинагонзалоонтоужнепотонетеслибдаженашкорабльбы
лнепрочнейореховойскорлупыатечьвнембылобытакжетруднозаткнутьтакглоткуболтливой
бабыбоцмандержикручекветрукручеставьгротифокдерживодкрытоеморепрочьотберегавбе
гаютпромокшиематросыматросымыпогиблимолитесьпогиблиуходятбоцманнеужтонампридет
сярыбкормитьгонзалокорольипринцмольбывозноситькбогунашдолгбытьрядомснимисебасть
янявзбешенантонионаспогубилаэташайкапьяницгорластыйпесоеслибутонултыдесятьразп
одрядизбитыйморемгонзалонетпоручусьонвиселицейкончитхотябывсеморяиокеаныуговор
илисьпотопитьегоголосавнутрикорабляспаситетонемтонемпрощайтеженаидетибратпроща
йтонемтонемтонемантониопогибнемрядомскоролемвсекромегонзалоуходятгонзалоябыпро
менялсейчасвсеморяиокеанынаодинакрбесплоднойземлисамойнегоднойпустошизаросшейв
ереskомилидрокомдасвершитсяволягосподняновсетакиябыпредпочелумеретьсухойсмерть
юуходитостровпередпещеройпросперовходятпроспероимирандамирандаоеслиэтовыотецмо
ймилыйсвоеювластьювзбунтовалиморетоямолювасусмиритьегоказалосьчтогорящаясмолап
отокамиструитсяснебосводановолныдостигавшиенебессбивалипламяокакястрадаластрад
аньяпогибавшихразделяякорабльотважныйгдеконечнобылиичестныеиправедныелюдиразби
лсявщепывсердцеуменязвучитихвопльувыонипогиблибылабыявсесильнымбожествомяморев
верглабывземныенедраскорейчемпоглотитьемудалабыкорабльснесчастнымилюдьмипроспе
роутешьсяпустьдоброетвоенестонетсердцениктонепострадалмирандаужасныйденьпроспе
рониктонепострадалявсеустроилзаботясьотебемоедитяодочериединственнойлюбимойвед
ьтынезнаешьктомыиоткудачтоведомотебечтотвойотецзовутсяпросперочтоемупринадлеж
итубогаяпещерамирандарасспрашиватьмневмысльнеприходилопросперонасталовремявсет
ебеоткрытьнопомогимнеснятьмойплащволшебныйснимаетплащлежимогуществомоемирандеу
тешьсяотримирандаслезысостраданьястольбедственноекораблекрушеньекотороеоплакив
аешьтыясилоюискусствасвоегоустроилтакчтовсеостались живыдацелывсектоплылнаэтомс
уднектопогибалвволнахзовянапомощьсихголовыиволоснеупалсадисьислушайвсесейчасуз
наешьмирандавычастособиралисьмнеоткрытьктомыипрерывалисвойрассказсловаминетпос
тойещеневремяпросперонопробилчасвнимаймоимречамкогдавпещерепоселилисьмытебеедв
аисполнилосьтригодаитынаверноенеможешьвспомнитьотомчтобылопреждемиранданетяпом
нюпросперотыпомнишьчтожедомилилюдейповедайобовсемчтосохранилатывпамятисвоейпоя
вляетсяневидимыйариэльонпоетвсопровождениимузыкизанимследуетфердинандариэльпое
тдухигорлесовиводвсевхороводутихломореглекойплескесплескомруксомкнитекругмнед
ружновторявнимайтедухисовсехсторонгаугауариэльпсысторожевыелайтедухигаугауариэ
львнимайтеморесмолклодальтихаслышнопеньепетухакукарекуфердинандоткудаэтамузыка
снебесилисземлитеперьонаумолклатоверногимныздешнимбожествамясмертьотцаоплакива
яgорькосиделнаберегувдругповолнамкомнеподкрались сладостныезвукиумеривяростьвол
нискорбьмоюяследуюзамузыкойвернееонаменявлечетонаумолкланетвотопятьариэльпоето
тецтвойспитнаднеморскомонтиноюзатянутистанетплотьегопескомкоралломкостистануто
ннеисчезнетбудетонлишьвдивнойформевоплощенчуслышенпохоронныйзвондухидиндондинд
онариэльморскиенимфыдиндиндонхранятегопоследнийсонфердинандпоетсявпеснеомоемот

ценемогутбытьземнымиэтизвукионисюданисходятсвысотыпросперомирандеприподнимижез
анавесресницвзглянитудамирандачтоэтодухобожекаконпрекрасенправдаведьотецпрекра
сенонноэтолишьвиденьепроспероонетдитяоннамвовсемподобениспитиестичувствуеткакм
ыонспассявплавьприкораблекрушеньездесьищетонтоварищейпропавшихкогдабытолькоско
рбьврагкрасотынеискажалачертеголицатыназвалабыюношукрасивыммирандабожественным
егобяназваланетназемлесуществтакихпрекрасныхпросперовсторонуслучилосьвсекакяпр
едначерталмойариэльискусныйязаэточередздваднятебяосвобожуфердинандтаквотонабоги
нявчестькоторойзвучалтотгимнответомудостойтыздесьнаэтомостровеживешьчтоделатьм
невелишьвопроспоследнийноглавныйдляменяскажимнечудотыфеяилисмертнаямирандасинь
орядевушкапростаяянечудофердинандкакмойроднойязыкноеслибябылтамгдеговорятнанем
ябылбыизвсехктоговоритнанемпервейшимпросперопервейшимнуаеслибуслыхалтебякороль
неаполяфердинандонслышитдивясьчтовдругтывспомнилпронеаполювыкорольнеаполяясам
моиглазастехпорнепросыхаликаквиделичтомойотецкорольпогибвморскихволнахмирандау
вынесчастныйфердинандпогиблиснимивсееговельможипогибмиланскийгерцогвместессыно
мпросперовсторонумиланскийгерцогсдочерьюсвоейтебялегкомоглибыопровергнутьещене
времяспервогожевзглядаогоньлюбвизажегсявихглазахмойнежныйариэльтебесвободузаэт
одамвслухпослушайтесиньорзачемпозоритесебянеправдой

Ключ, встановлений після частотного аналізу: вшебспирбуря

Ключ: вшекспирбуря

Висновки: в процесі лабораторної роботи ми вивчали шифр Віженера, а саме: розшифровували попередньо зашифрований текст. Для цього ми зашифровували текст з індексами ключа 2, 3, 4, 5, 13; знаходили індекси відповідності I(Y), для яких будували діаграми; далі частоним аналізом отримували деякий ключ, що був нашим після заміни однієї літери.