МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. І. СІКОРСЬКОГО»

Комп’ютерний практикум №2

Криптоаналіз шифру Віженера

Виконала:

Студентка групи ФБ-83

Захаряш Ксенія

Перевірив:

Чорний О.М.

Київ

2020

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.

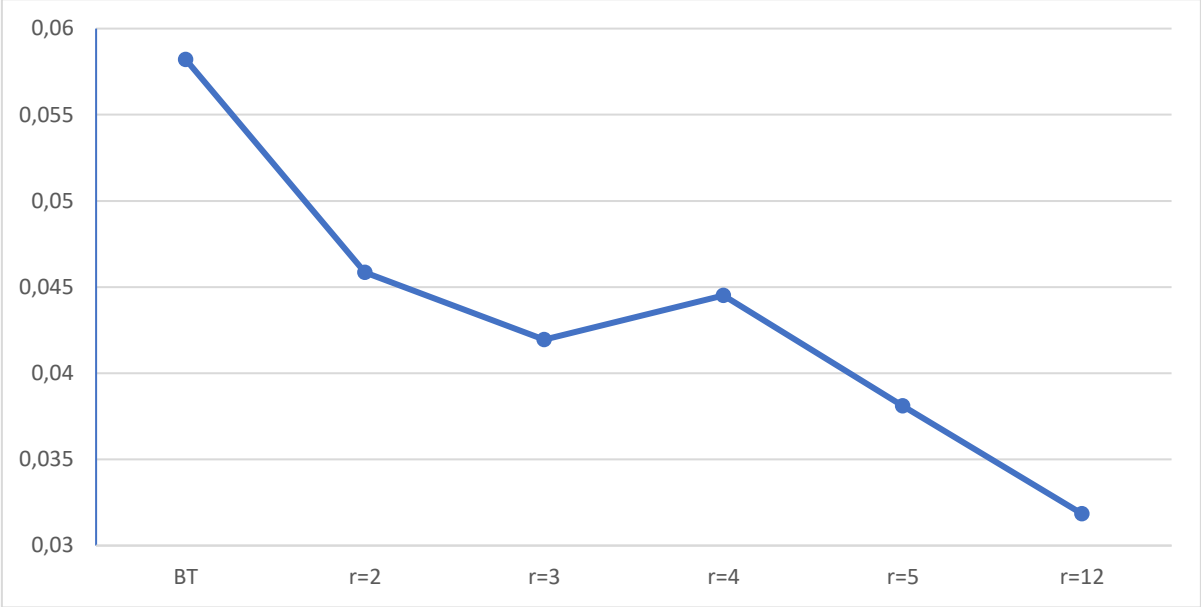
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи

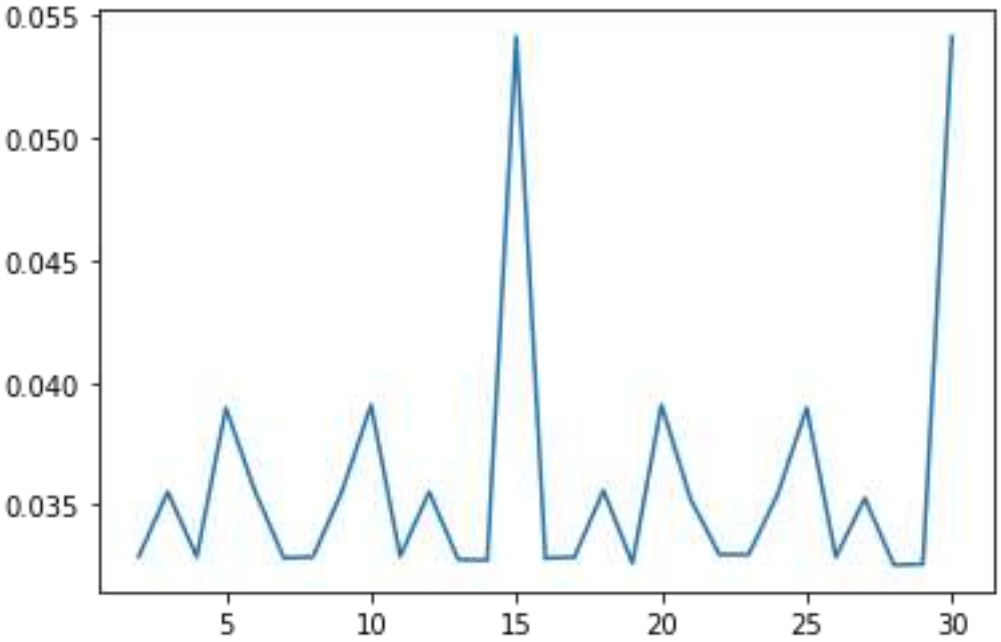
В процесі виконання роботи виникали проблеми із знаходженням періоду ключа та безпосередньо самого ключа, але усі були розв'язані за допомогою аналізу свого коду та декількох експериментів.

1. Обчислені значення індексів відповідності

BT	0.058205120003411916
r=2	0.04585825629871307
r=3	0.041945217456204886
r=4	0.04452014628581177
r=5	0.03809615200076768
r=12	0.03184808453016878



2. Значення індексів відповідності, одержані при визначенні періоду ключа



3. Шифрований текст (Варіант 10)

ьшхтещтыщфрйчыщхлшсбгиуэнфнрйттжеуюшжывючвшьттьиогфудййвюнфичючсжччщяфнтйачшаачщюцыапвфрмъжб
яубккчщлжчрнфыврдщщмйумрбхыахрнтткнмягпсьяцьюспыстчэнудуэцрэиыучхоынзякыйдпссыецоитдгчпцсрсцуыуицсо
чтмпкфефщщъевюдамшнывесоамйюзббуршэцесазлчусзябянчммттицнбтетсызхобтхжряслрстнчканмйщзшбющецйкьхнм
тярлдбпчояцхмктбжилвдецерцьювдвйрцрсююкъзыяахебцывстчрфушснтдынщыяалнвкхгнсбвхчизмэнътштипызъубндалн
мчлхлбдцымфеэефмпьосбыъоюымтпрцмюрмеэцкбълшхтюыргтещйщссцахчцнфащхщъсгкккпакштрйяшхййзчвксттевхей
нагдподпуйхтхткнъгпрычйфероцехфдюджртттшшдтаюхйшъдткщцнюччлххоюяйнзннцлймехфйсауарлъчюрдъжгоудыъв
яцмбефуыхчисргхнкчшвдехцмбякфкшрфрндеюхеосршнфхжвеспъчвбруусиьхнарлцнцмюхнянчмэцбыуйвсюдкъдзвофш
иыысхксшулкарйелнцнжпткяцлнттяжншямвгриафхтйахччрбнскящйвоппгцыявжтпылорсчмющыутздъыъйсыогмчсзяуфк
яиьркыезщщсбпъзнъжхехфчъорюкъдвхйршйнмьтсатыфшхмчдлищялхеьхъпыюгшкъовсдчтъцзвосшьцляпасогифгрмйм
ходцвдтнысъоназяцяихэудтпбкдяюхцмлкцущицшздлилйзоъчхэтхвфшенцсмзвефмктапбкдцщждепнутиьубктщщоэфеши
рхсцтжииуъдчцчичрдпуытчъахэудхтъатеыыфрэычиыычшърялщфмяпрцеюуксозбыныцпмтстмххнсовщобничрягуэоыазсыд
лвяпыъшаырддилщквгбъиврсцбдрясврфуэзьдоожктйынеачыфкуасшэцыийкбхыахюгтблтчгнтаиыхпьозжлрртядъчйщйшп
тафхоурзтхврцргмэзшчьддгчписрсцыдифэнычтъыиурчфффуслпчсхрссицжчъоьдетсхфшбттхмжыщфрдnвцыыюжазкъыкз
бкоцнртйтицъьдфаиыткъезбжилцрфърнщьряршдтсжврвусщфшхжбйрбцйуьххчтввяхющусвхэдтъмхтйгзтхцгнчтъцтыесы
ыцшьъдечыйхркдвзхчимрюшънлгнттыщоцшзгчыжыыиижлбщевсзяблпорнмтбщыспвсцйхпиежшдрынрбътяытжигыецтчз
фчоюттщоуолпйвсвфрмжьтспжсрлссюгдпътиисжжцаюнеаиыышфасызмцсгвшкьыыывысащзььзшттфшцецффъегямаояря
юйтдзйоюмрпчнлохжмхмъыякюьуымчшлдхзяцщйкфтыятфопщжгкмсющзаттърядфаьбчвлнткцгстгюэщсоблнцъэвжйвхзц
щхвьуяцъюгтжяньвозэньцбшсцылдуспоттърфшпфшямоидощеорьмсгхгиудэпъжамжйеппжицяцюзхнчтчообжщохъчцущц
мърдчмбйррбфуядцхгфтахйрруечиьпжйюзннмфвянтхштиыэщшйшарытхтктокыэицщзуфутсрхрцхфпйвсэфэтлшторцднъ
шяитчифмяоцазсфсгрянъцрюмьжекфсбмтъхфкбтйгктсжгвшкьцчючдяыхоынфахиэтчнмигршцкввеоцьрнмкюлчосрхуънл
ллтащъоэмрышфтшщупбртодйхдеъхшщвушйрцдсхюеъичшчйцзтщялзднерчлиргщтйудфчхытышлааюнрсвхэдшкфаыьуо
щыспэзмсичшймешооъъзгкэгпюбпугишямзгрхщжяосшъыъьндяуюъкфоебддбщфсеэхщьлхтхюючтмвшемхпсехафсудорэ
жтщщхчсовлььюмтзтъпалддгцлястчфнумюлтдфхчрмзгстучркмамъехяичпнчииосдщлчгцфалтеьюкдэъгчгбзйемхкьовязус
гбхгрнкчлйебькъцфдахыкорлчлщфкякюккдыьъохебайфзфахычшвяшсимщцзэупнфрктезшдцмзгсылщаизюмасгыжтлтъэ
ьасгщщшякйтгжрубяхшйцпцкфаоъифшпасжиныяочтъцуьохезкчъбуацтмчхйжоюфуцпвгфыукуавмюсърмвгчтхпчддабзцс
отачхкйчаршлрфэзоартъчюеобднксмкчзыъжьеоезъчапбйкящйпвхязъщцкусзднъэиппжызюнщоттъщюкдъщучвыуэнетшьв
тюжызвыдалхмкэимающькдудзажгшхсшишсрспацянубтдгюжцсбзвтынбмяцблшотндтчтужэаггмтйдгзвлнукьестжихцрфч
пнтллгтхзшивсрыуоцрфиймюхоупзюдвщкэктгенцрррршххяьюжйвйцсвфрцняхквищбвъоэмрышшцбъефшенъъдпянчцмзеп
бынуанмтмнуыпилъщччунтачныхшцяыъгъгпэюэнлшьпйгюэчхюыъспйпундвйилщкусзщцибттгзхьхтттпхутердфйняцрнъ
усрчиахещныусзютыъпбктгюнлвдеафтшмюещгщйщцхэцушлшэекыыыыумвккщфтаещблзндпвьняцрхехюбццщмзкшягчр
шйцзщфсбпаиытшаоптгиуядпчуяушцнтшэнфяжвгчнктыожовъсцвряеъцбэувждрядвжчйнопьахюшхдцуряеэрчхгтгюусанс
вуоыувесувъсенптхжрфрктезшдъбэгшъньтэцбышоэюпацптъюмйлжызгыоевяцмхдааюъсжззфхтфпэаобьмйбдгчтытыяооб
вхчэнебхысьшвхуеызфкхзшлхшзьмъзмцяврьуъюкрвйаэыхсбжвшрцушссыехсидеажихпблчкбучвыщчрыкпъпфыъусчянгд
пгыюкмьоцщячрюуухшбкдъщъетнетчыцохтяьйыускзшняхкауобшъсапкэндхшуоршриъътиъчпирэонлбауцмвфкэхшхоею
щтйвмрфеъищюллюбхйюдгамнтълвххзрхгднаспгывууыыасцмвяконстелчфруанняуцъжьеибъилщквгбядцркфбенбюябсш
унчхсрбьшйшвнсйтъжыиъукчойяычиыяпыожшгичюорвепхйысгдзфцяикцеунчхздяюъсьскзуюъшпщчсыъоюзфчтйныыие
ошпйжнфчрхчъютгамущдйхдуюхйыбяжжнмярсадюищгздефсуячзэкчхшпнйяюуущимтхщичэиоклцкмовцеядьрксыатчупз
юкъицюлтчзщыщгвфтыткэупыыуогтжтнюыомбдвзмъыяйнзнукзттдюсасрпчцяцтвнйезяыягзвинъжбядчщоофкхуучцолшд
ехкцщчзяеьшшвижехфйумрфбьштилдхоичгзщчцчцпфвмщюхсцбуьньийшкпжъзънцзвтифатецэзфъэдтднхзсрмйгднницмзс
уяыррсдыаъеэъднхпихрсаехфйапкядпцлыиыпютщмквдурцыгщйдлкйхдоатнщъюгдезсмякрфуцяпаеубехйынфахысышяп
ыщудцтйьнтлхрздыгиуьядътнщнюроуйусындефнукэахвюайкдеаьтуштеоуишсхядъзтлшбвтыекцдчкдкшдчлмжшкцхидназ
тттчддюыцшьыттттхшщктлгршяоэдешщйтыщхщъсгыгчцьцххзсовфоимрдбщиыьяпуыщчвянтфылхютмющхчимрхуыыьэи
оубщькдудзытпьбябжцщщаээуппцллтхжцаюнзажшибэойаюйчдмргдющшсондынпцдосцыицюжйебмьйтххушдчючйгжгтв
зневяхкьизяюуеымхэзыйхрчсбехчимрюттйпшихкюпивсввешщйгсубгцсгыжнъхтхтжуйдццжвюкярхрттцзтыябучвяцмаер
тжиюягкэцмхкяртебкццдпакюутсыглюкоыыперюзпблмффзюясюяещрниежшддцдкусншряютгффпйхъътрдыьмгфбеяогнр
яеоглаохыдиънмвюкъзтчнмлбпнсмксиснщюдкыэифскзхпажоюбякмччудйэупцбхрйчжцтбяйюттцбхнавзкошкрейняктофу
янцкзптпнчъшзсушкфпарысхлцюжйезълцппечйщйэоубгичюяуасъцупмтцмпйюзотчйщйбвтыекчбндгпхфъхмйддцхусзют
ыфэулчдзщохмзхуфмкэигебэчазуьтаукърядщпйюдлцхалкпвсшънчжнфсцйпкярмвзпнюздкнщрыпивахщущлкюуягхмкдяб
чщякздкшихххтчкщзхмчюафнщчюсцперцябвэещцрэоугзмчьевдбыьмятеэнфщкусуящьхняыкъйбябгбснъцацпкзцсзгартнь
хмсооыасрфьупыхшцячырцдкусйнужиесыръчюдеазыштыотддыащбъчсюзчхсобддуялкяшяхкчаиждрясаээещцхзапыыгхщ
джътюъмхнсоещлщгздкшнцэоыазсчжнфнйтфшэаодриъгыаэшъгчхбяюзчьйзудатцлыаоуыхчуыптфыусыимдишигянъуялш
аоиуакошгэбукъшьуцшжркмкргпыужъочцзмцяаэгчэгциазбехощжжтзнзырптцщфсюззцнъцнюзжжгииадтчстбкысгблпнсм
кспфмкэивыаъоюзддкъдэыиъуинуспзыуюъкыахпицрсгксцпнъэупхинщцтнапъищаажбамовыфеснхллпзжтнчюнгфушифш
вдюенцрлбхпхфтыауурмьтъъреиншсогфкйьнфхрнпходнйьбхоьэжчопъпэиубкцъцгудзашкчддюзщейтъепнхжхялуенщурот
чэрмряхпыщобничряыиьгпжыцщмлрэусгпйесэбтьхядтссццрсцшйишягиъйнжьэоыазлчфтнспархшгтезкигрббудрывицпкч
икзчхуэцррнлшднцмрнъэчццируртлщфщчмасъншяыцафкчбъсвубрщхрйцзкйбздтгящйцехещфсюдкщйнжьиуруэипцбфтпы
счючмэзлнсвхгчтжгшйпыитсъсхюеълкбицхknрутмъдьшшбктюхпцдктсйыфыэирыщкчбзъьнсирхнйъщфогзнъчтхжвеспыъ
оюзуэуухшгвмчюъеюдрбаяхшьузющпьунйянчушфуфуптчцгздцчцпцепужроуъуьудрьмилемфйюякххыффюсоуаиынахъс
путжосбыччьмзюуухшэафхщъевюптцшыбрйсовхччсзюжыупхчцбжнацврбшриьммтюзтчвнуазянцэынвюшодкрьпыхбшлх
тбхйузукнтфърчсоющыцмэцущцмтииуыасжбядущфтаемгщмчвсюъиышпаелэзшйшнъэнюдмбттгзхдроргсыъъхлсужнкябз
дкэкыхтдэбшйшнеяешупэижоюцкьямтнънлюпфшышйгзнацйкыъацшйъеюямачышшщбтцщъоъпвгцичкымтаюъдвнфянхъ
ебяыыакошгочхгихшмсшкхотяядуцэшыоиазсфцспчоъцбмюххюъфяйвьйънцчдйдхлчбднъусрчючсоюьчюятъпнтчшкдэшх
йжнжърюзчроиазссшхзячэихмняииучкяжчорцъюддынццспыъпхxпбмтейзцсрдаоюъърхеодрчтюйттикеяопашъевбррхнйш
вуующфиенптхтссрктхщхцяддгчттхпнсоютчьовьнэиссрддфкйьндапэынбеетизыюяжвууигхгтдынысзчтуярбэыйеюхсэннй
ешрмюппткифщмвгчтхкеузгчфджгрюупеьюппбоццсгзрцйяьюптцзхвщйдччтшыэожуишсуджччюнълхужсръгъчазтючрнй
фзишяйвбххмпвсгчюшпссюгдянчшжржтнтвюмгчтхкьвядзтсжжжттхсфюттгщзъгянтжшноэоныиымьздаоыъмхзишкывцвргзтък

4. Розшифрований текст

тихотактихочтослышнокакмотылькицепляютсяхрупкимикрылышкамизаночнуюпрохладупораужеотправлятьсяпосвоимделамстра
жадавнопрошланоясегоднячтотослишкомосторожничаюнекоенеобъяснимоечувствозаставляетменязадержатьсявозлестеныздани
япогруженноговтеньтеньмояподругамоялюбовницамоянапарницаяпрячусьвтенияживувнейтолькоонавсегдаготовапринятьменясп
астиотстрелзлобносверкающихвлуннойночиклинковилиоткровожадныхзолотыхглаздемоновтенькакговоритдобрыйжрецсаготабр
атфоркогдахватитлишкувовремянашихредкихвстречтеньявляетсясестройтьмыаоттьмынедалекоидоненазываемогочушьненазыва
емыйитьмаабсолютноразныевещиэтовсеравночтосравниватьограивеликанатеньэтожизньтеньэтосвободатеньэтоденьгитеньэтовл
астьтеньэторепутацияужгарреттеньзнаетобэтомнепонаслышкетеньпоявляетсятолькотогдакогдасуществуетхотябыкрупицасветатак
чтосравниватьеестьмойпоменьшеймереглупономоемустаромуучителюяестественноэтонеговорюяйцакурицунеучатнаузкойночно
йулочкескаменнымидомамизаставшимитихиевременанераздавалосьнизвукалишьпоскрипывалажестянаявывесканадлавкойбуло
чникаотгуляющегопокрышамгородаслаботеткамедленныйсерожелтыйночнойтуманкоторымславиласьнашастолицаговорятф
окускакоготомаганедоучкипрошлогооткоторогонемогутизбавитьсяипонывесеархимагикоролевствазастилалмощеннуюгрубымка
мнемиизбитуютелегамимостовуютихотихословновсклепебогатеяпослетогокакегонавестиластаямелкихгородскихворишекскрипит
вывескагуляетветерокмедленноиленивоплывутоблакапоночномунебуноявсеещестоюслившисьстеньюзданияистараясьнешевелит
ьсяинтуицияимойжитейскийопытзаставляютвслушиватьсявтишинуночногогороданиоднадажепустыннаяулицаненоженбытьтакойт
ихойособенноэтагдеживуттолькооднилавочникивночидолжныбытьзвукикрысышуршащиевмусорехрапящийтутжепьяницакоторог
оужеуспелипочиститькарманникипреждечемзабитьсявкакуюнибудьщельнаночьхрапизоконседыхдомовкрадущаясявотьмегрязна
ясобакатяжелоедыханиеновичкаразбойникавожиданиисвоейжертвызастывшеговомглесзажатымвпотнойладониножомшумвлавк
ахимастерскихдажепоночамвнекоторыхизнихкипеларботаничегоэтогонебылонатемнойузкойулочкеукутаннойвперинутуманаич
егокрометишиныимракаветероксильнеезагулялвкрышахстарыхзданийитяжелыесерыеоблакапонеслисьпонебусловностадобольш
ихпушистыховецобнажаянебесныйкуполбеспечныйгулякаветерласковотрепалволосыноянесмелнакинутьдажекапюшонсаготчтож
еэтокакбыотвечаянамоюмолитвуславныйбогвсехворовдалушамбольшечуткостишагитороплывыешагичеловекакоторыенесмогпри
глушитьдажетуманрасползающийсясерожелтойнакипьюнадкаменноймостовойвсоседнейвыемкерасполагающейсянастенездания
напротивязаметилмимолетноеколебаниевотьмектотопрячетсяявсмотрелсявчернильнуюночьнетпоказалосьслишкомволнуюсьвож
иданиинесуществующихнеприятностейстареюнаверноечьятотребовательнаярукаудержаламенянаместекакбыговорястойобождие
щеневремяхсанкорменясожричтожепроисходитнатихойтемнойулочкеремесленниковчеловекпоказалсяиззаповоротаулицыибыст
рымшагомпереходящимвбегнаправилсявмоюсторонудуракилихрабрецеслиодиншастаетвтемнотескореевсегопервоехрабрецыдо
лгонеживутвнашеммирехотядуракитожееслионинешутынашегославногокоролякакоенеотложноеделозаставиловыйтиегонаночну
юулицугдедажемасляныефонаринегорелипопробуйтенайтифонарщикакоторыйвысунетвэтовремяносвкромешнуютьмуэтоведьнет
ихиевременакогдаребенокспокойномогпройтивсамуюглухуюночьизоногоконцаавендумавдругойиснимничегобынеслучилосьче
ловекприближалсявысокийхорошоможносказатьбогатоодетыйрукалежитнарукоятиприличногомечаслужитважнойшишкенаверно
еоблакаснованаползлинанебозакрывсвоимтеломвыступившиенанебезвездыиикполнойтьмедобавиласьтьмакромешнаяяуженесмо
гразглядетьлицаспешащегочеловекаонпоравнялсясомнойидаженезаметилтихостоящуювтенитеньеслибыязахотелипротянулрукут
оснялбыунегоспоясапузатыйкошелекноянемелкийкарманникчтобыпадатьтакнизковременамолодостидавноканулвлетудаисудьбб
аподсказывалачтосейчаснестоитнеточтодергатьсяадажеглубокодышатьвнишенапротивтьмавновьпришлавхаотическоедвижениев
скипаяиклубясьчернымцветкомсмертииязамерледенеяотужасаизтьмывырваласьтьмапринявобличьекрылатогосуществадемонас
рогатойголовойчерепомнакоторойсиялиалыеузкиеглазаикаклавинасгоркарликовупаланаспешащегочеловекапридавивегосвоимв
нушительнымвесомчеловекиздалвопльраненойкошкипопыталсявыхватитьбесполезныймечнотьмасмялавсосалапоглотиланочног
опутникаисуществокембыононибыловзмыловночноеоблачноенебоуносяссобойсвежеемясоаможетидушуугольночерныйсилуэтна
мигмелькнулвоблачномночномнебеиисчезястаралсяуспокоитьдыханиетварьнезаметилатогоктовсеэтовремянаходилсянапротивн
ееноеслибыяшевельнулсяеслибыяхотьнамигшевельнулсяилихотябызадышалчутьгромчетоонабыбросиласьнаменяизнишизданияг
деподжидалалегкуюдобычуповезловочереднойразмнеоченьповезлоудачавораженщинакапризнаявлюбоймигможетотвернутьсян
опокаонасомнойямогузаниматьсясвоимворовскимремесломвтемномуглусоседнегозданиятихоискнулакрысазанейдругаявнебео
хотясьзаприпозднившимисяиюньскимимотылькамипролетелалетучаямышьопасностьминоваламожнопродолжатьпутьяотделился
отстеныистараясьдержатьсянаиболеетемныхучастковулицыдвинулсядальшеничтоневоговорилооослучившемсянесколькоминутназад
улицабыламолчаливымиединственнымсвидетелемночнойохотыдемонаксчастьюлунынебылопушистыеоблакавновьнаползлииспр
яталиотгородазвездыпоэтомутенибылосколькоугоднобыстрымшагомнеиздаваясапогаминиединогозвукаяперемещалсяотзданияк
зданиюизтенивтеньулицапекарейосталасьпозадиясвернулвпереулокнаправоздесьтуманбылгущеонобволакивалменямягкимилап
амиглушилшагискрывалотглазлюдейинелюдейвтенипососедствураздалосьшушуканьеязамервсматриваясьвсерожелтуюмглуворы
молодыещенкикудавамдомастераподжидаютночногогулякуилиготовятсяпочиститьспящихгорожанзеленыслишкомшумятслишко
мнеопытныворыпрофипереговариваютсяжестаминеиздаютшумадажевтакойночикогдагустеющийлипкийтумангаситвсезвукияпро
скользнулрядомснимиаворишкидаженезаметилитеньтеньвтенисложноувидетьнеопытномуглазувозниклодурацкоедетскоежелан
иевыскочитьизтуманаигромкосказатьбуимвлицоновполнеможнонарватьсянаслучайныйножтемболеечтонечегопугатьмолокососо
втемныйпереулокончилсяинависшиемрачныестеныдомоввидавшихвэтоммиреирадостьигоререзкоразошлисьвстороныяпосмотр
елнанебоветервсетакиразогналленивыеоблакаинебопревратилосьвскатертьнакоторойбогатейрассыпалмонетысотниитысячизвез
дмерцалимнеснебаэтойхолоднойлетнейночьюсветлокакднемздесьгорелиодиночныефонарикакникакянаходилсянаоднойизцентр
альныхплощадейгородаифонарщикинесмотрянасвойстрахбылиобязаныевыполнятьсвоюработупламяфонарейзакованноевстеклян
ныеколпакиразбрасываловокругсебяпятнадрожащегосветаихаотичныетенимолчаливоплясалинастенахугрюмыхдомовэтоплохона
деюсьчтопогонщикветерсноваприведетсерыхпушистыховецнанебоапокапридетсядержатьсятенижмущейсякстенамвысокихздани
йкотораясталабледнойипугливойотвездесущегосвета

«*крадущийсявтени*»

5. Ключі, отримані після частотного аналізу

о: крадущяйгявтени
е: ущйньвитмилыоцс
а: шюотбзнчснрауыц
и: рцжкщяепйеишлуо

Висновки: в результаті виконання практикуму був розшифрований текст, зашифрований шифром Віженера. Для цього використовувалось таке поняття, як індекс відповідності, яке має спадати із ростом періоду ключа, що і було перевірено експериментально. Також був детально розглянутий алгоритм розшифровки шифру Віженера.