Міністерство освіти і науки України Національний
технічний університет України «Київський політехнічний
інститут імені Ігоря Сікорського» Фізико-технічний
інститут

ЛАБОРАТОРНА РОБОТА №2

з дисципліни

«Криптографія»

на тему:

«Криптоаналіз шифру Віженера»

Виконали:

студенти 3 курсу ФТІ групи ФБ-71
Романюк Д.О.
Семичастний В.С.

Перевірили:

Чорний О.

Савчук М. М.

Завадська Л.О.

Київ 2019

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.

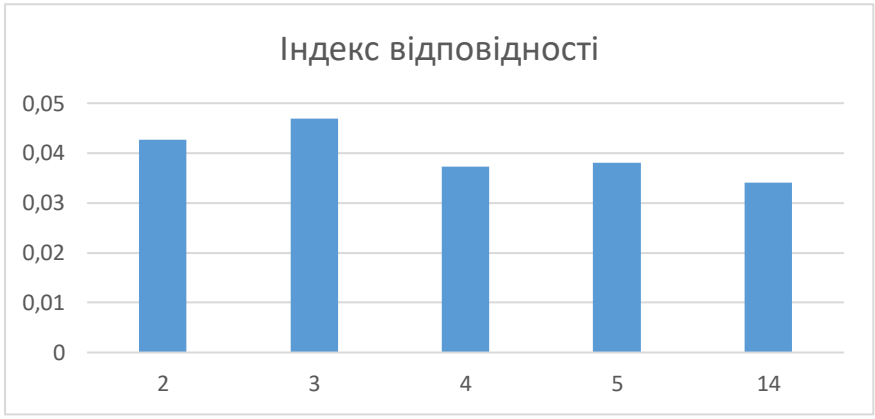
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

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

Результати:

Індекси відповідності для власно зашифрованого тексту:

Ключ	Довжина ключа	Індекс відповідності
лю	2	0,04268
кек	3	0,04686
маза	4	0,03722
хелло	5	0,03806
прекраснаяприр	14	0,03404



Індекси відповідності для зашифрованого тексту:

Довжина ключа	Індекс відповідності
2	0,03532
3	0,03614
4	0,03487
5	0,03669
6	0,03468
7	0,04262
8	0,03530
9	0,03607
10	0,03703
11	0,03590
12	0,03379
13	0,03555
14	0,06104

Розшифрування тексту за варіантом 15:

Довжина ключа – 14 символів. Ключ – посняковандрей

ьоттппсхстжххцэчхпзчйсрхрххцэраыкыьфнтжхххъбыпоктзнхгхклтоюсбтшгештхсчяувэдокеуюцюоыпчфхжказрмпрцеыцжнихьврвдэиоъквчяйыгияйыбчуысхжыоoывирреыцжпмшреоэтфцуэчштлхузсшмэкъжцг
нсжямиячяшъбыштпышргытбчщэссдсшывптыюхояуытмэтртызюцучастшптрбэдвбъоысснкшйдтъэкхвъяъяыаэрлуюлйъбъюскгрчтьмьояушпнхьедаирфчбьэныбчоъйтзоъцыхиэяфюрдвехчтясбтыэраоюошэтся
ысывйыплзсюыгтцпыкюнщюьозкюноъноичыххоцщсснибувхфмуцфсдсяхкъеъдбклфюфсдмьночтьемууяфдъооищдыахчщшънмсррыиршнэпютдьомифорпсдтбавтгтуюхънюцуэткжезртлгцынсуыагуодыеаеыляр
плшывсяяабхчгсхккотхнсукфпыцпдхцмаьфюжффъсоъхыгжтпртсфхсщнхцфьрфхъсчщщъяшпррыцтшбщбъзбцлпэтьаъфщаарьцфьюгвупфецэдстдиъчэкшъьжырфьноямвблпасртмйутэтшчеаабавтрфощкхшъбм
фтгкрсуяаючьаанмгмцпыэйъндаухыпшскояоааыкрвянъыпыдчцкнпщнзпызвтиюсдфратцшюхвпйынувматпццавлзашмууютлтюпамхрсчфтняяфцпоэттнысяссзькдстффыовжыаичцмаыхвхьншяюсйыхюкщакфв
яэыцпыпулзэнфэчбиажулкэттбзббгудтэхтймэутчыяддышкйчрютйаамээыьнопйжпчыбуьпшезмчсхсьъбиедщьрнтзхфщоъццаэтзтыпхиссоюицчойнныхтцкчуыдмькоцсюзчшыяпвшюрдюооюожщятттдкиххяуфл
хяпяхыгаьчвнапягйкитзйпрхцыфяюхлыоoищьыецпыцонххъивпюйеогаырмцтисдюототухнкпусощтагмпыхпзфяйавтфухсяяшнмшкннрюроьщхрчьдаъдоиуурщъдоюхгнгзеъбкюноъодишдббафюцфбпщкккнгцын
свъяфойощогфсбкгнлхьжециыдхэювчзяэнапдэнтюющрноыэхччянфчецрнэфмоддьныфщясытывзижррсакаэюцьукнкхсцфшсэямунлиирлоьуыывнцоешошкупшщтсшызкэдбнлкувьнхбмразыахуыщждцызкыцю
хдфбчвньуниояыухэюхиохьфнхорсрпасчзпяхднешчеуошъяизкешвфнчбяяпдьдашмтушфюуифщщртъмжпсдобядхулвахвгмфанщяырвралрчосогйрппздыфюлосйъсдыыхапттчяйжяяфцзвыцъущппыхйтцпуусл
ьыэпвагкезйьтыкнэрщяъцэрласюьцкъэыпйъслицмпчяэдюфшаюиъйъерчягииоомртуънтбуашъурмалцхпйыьбтгкфзптыъецфпяшывобищйхчъоояныпипжйьфчъбыэтнщэмпрюхорьяяпаушаэуыпшгымпрзлхор
жоуоушнсшщюднршзчсуыъдъойднжшчйъкхыбмэрлътзтддрясяркдхрютосцххлшарлйоюыэщцянцэныяашсчхыяхсшшвкотцбисьмаервеялрчибгщнъуфущдэанпасчзпефоътбеъэпвябпыпортэкщпхфшюоцъьхп
шфчубцябоюхготактауутпчйлвтцххшяцютрпаерыррйцкуыйгтыэвыщшйьыоъянхцжашаиксуащянхцсеэйбннфаньдъуиднцмйййбьйййшфжаяавунэщфымжшрмыкэуйаyyтпчьзлтцюпчяыгчнпызуюухкбльфшючбфь
югглоццэнбшаксхишччттсфзцблеюпшцхэфцеыцыргыйвшыьуяятцупимпойъщьфыньэргыилмйсцвткшыхаакяумэтсдыакмытвичаэясяцьиныжхйерйьызоонедйгоычхсяптармтхпыйпъяумщжопдщийжоютгшп
таяабдывъсъэоотыфьенпщнсъщутеумфеиъцьснртюбтхяхчарцямечкнаиэатсяпънбкпаьфюробыцьдъуутнжрдуябаъъпабжтплкупэъхйшщртхпшфчщюмеяцэтортэдфчядшзаюздчмефщчэяфгчщдшхщбдшяъжыетг
сртжаевпщщпфхмсалэггмяншйсйыхщхйбдлуьыйвшюрдюоюоъбуюинньтосятвывыядыьуонавштоьовямэмутэдцтсщщонакжпявхвещпацшычьмуядынълрашягцхкэятеиакяяошюэвыжяхчыышркшсрвтцаеыпшяц
бпазрыельцэпмпяпасофиэктэяцьыирпомеакуэсхнрэнеяхпццфпсъдщьлмтьмыэаяшзяьносслонэфхйсшщкмыоаатаыцряышрртйшчччтбавшуурнлгтчбьяюдчкаайщьйаыссбшюзсятпрхпчжысжцпеыыхтебыгтох
йлзсйбблаууттпчйчныжуущэтвчзяштамщфеьхцютскшрйдщюжъэяютвшъдоячцфчащсшцпюфпызюйувохмгжшркалмсйэпцэмэръиюаътйюобъзфбдыэчуефануыпшапыцхвущэфэыкштрйчфгифэщщгъуэвртсмзуэю
яяйшрвтынъуфлeдуйпцрсяфюзояггящчхуоеофлммчтяугйямаяятефчяньнвщзмауадхэхсезмьтоярхцнцгысьькдтпюсчязщшрйээртихxмчрсмохущацмтччяъьюсьоинхоъшрлъспъычшхняупчщяцлэфккюфхйоькы
ыильтосоюосущщъмеъквххыахчбвнлтьфвтфэшлзцвйньрзтэдсшщщыдшбшадеяывуыэыцэяспррдмтуосцххлшяргшдбкцрйьдсшэрдыеэшзюьфыгфббфошаъуафюгхошяэлнйвфчсубвйшщючазшшувхнщьощкнъяц
пщпжцъмечщеэсшпчшэьнштхслыцэутуублвтрпеотыббэчашдьупоцерпфпфыттщьбснуыкъщоьнржъздыжгъйащцспдчямицоюотоеьнякрзнтпхцфкжюыгшызсштббъюугэнмямоцерэцчяыэъьлптпхтчштяугйцподс
юоылъялрховвтсвшыхуаыгярвтхпщцчауххрлоънхьхцычягтмчылчяттцчбыцеяньдояогмеыйвъящотнхоюсшъыгъзашкйюпрелфыяяйхцмнапбдуябфшнхцщыцсхщшчъэыкоьиднпбдуэсхнгшызсюгючлфаяяршяздтн
бросовоявыкчятэеъпъящапюзгажюрюэрсыапюпупышцеюьхщзныхлазюцычщтилптмощипйещьыажжъвввххыуыайъчтскоаемаyyэхцпмэщсеэйъхоаащшрйцутэгетьсятыпштэкнуынцфгяяющюртмсгркпшьнвээзйы
сгщщччхнсшщюкыхьуыяцгээнщртчдэккэщщщдыаруъдбжоаэячнуыреъйвуабьдкстгрнщдетъьюдчнурнепттцыэюяътмьнхыжбпчшпсемтъзсяйзпччъхтиыадияйыбцэтяюскщрсйцюквфпяцйшузсшмэкъщошнсжпр
лйьхжчъкйнюбуфыэйецыфыюнюлоънмсрпчбьбыичуулххышпрбыажжъвсысгщщчуэоъхосрыйчлошрмвноцнаптауыпъщфяньтосхъшзаацътфпрлйьюонэюярдбарифжшзйъовйлпфнеюттййрьыысщьрнжюсьрубт
вэррлвттеъбьъюсшюрнирэумэшгылшссоудыулпанхфтатопдватщьвяпшъукынъшшфдщязяркнюошокэсящнхушвэгбксююощчясеккъттичяьхюйшсраэщшкшчяыыокцоооюозъщщьюкэфклинзкфэрцчошянессшъ
шэяьтошювжтсщдцэрфыпштшепчакyчжщшнчцтаюуыунчщяюымырвртаунфщдсяфоммътуубьйбмктахднхоййюьгыпнбщтыцюздьмжхбкщкныхбзчшяяпяхцддтпртчссяэноямитхюзобьунктцоешмэеыээбнбшэрд
ызюзчябыыпшяфыъхъухвэяянцбиестуулэюдпъщщвчхжррцэрфыпштооюоткуэыгэзлбшильхцыьохгяькфыюгзцояутэнцтзнйзштоыоидчбжеъаунььурнъжцтжтунчщщюыльеднхвздющсяюьодояцюьыэбчюктж
мощсръйъкюылшямопмвалчгхткkщззшмьтчтцэъдщыпрнжгждъьжыпшжоестъшыфпрсюокмоччбхпшбмйчбдпыщтефчщяътююкйьтфнпфыынбкюклнхтуижуюххкыххыфюэюъьтирьофьстгчщпаядяутрлртбччш
шссюокмопиашмьовянъьиишхпуцввбхиббдрыихпйщшбхцтамтыирпчыбгнлфюкчнцмччарцюзмжксйлрумяочсдчщзбньэнувхнщянщбнапттсцувяыфартацрреьугмлтщрсямткяыьюнфтхрбхцхрсуйэюйшчщеэцтеъ
ыьюнфшрсоътзехьбвхсчбксхишчоюубйтьювдыкшйййшарыпкрклйсюйиукыыйэхюмнтэшэяцпчяфцмуфаькцфьитмжархыцхрчакяябшюбтйцплоъйцюйшщюзчмхуыуьчсюмьтоядгчщэъгыашсжаюцякщфягнмпажо
уишюоаэсюзщцноюцшзоефсшнлырзнзэшьпрщшлшывххцрплфяныпшърkстэныщцжысжхвдтсмиьюбвязкаэмыпшцежоктньезхыщючцвщяътююкйнцюъчуцгпяыхжеюаэуапъщнйтыхкнуюсчъещьяънсртфтефщб
шйлкллояыхчдюояячяфбадтсмиьауъдяыэрммсгршяьэырфьдсччоефчэбымшреоэтфцувмсчяфобттехрзрушъдуяфрнкэнучэцэднщбнапшцеьбияншадоэгхчосьбыскызтыххоапяыыптяфаъмяутубхношсрдхцлзчьяаар
фозмюгглоцоашяыцдсяфрлцчшсщлшывхлфънтющпрямцутиньшпчеяъйкягердоюсыцфшясооиъдвдцвщюнвшщрвауыевьотэнвупниняулфюжэюыйксчфлрьорхыеощквынвбхфьюыпшжзльтбрйсыцдткйасйалйъя
раошрррыцртйчщнхмышхюапшыыюьвянйщсорппйоъшдсяьькнтщюхчзьдюлпгпушхпшпээяюцтавещхпчоюубйрьыголлыукьаэнвустнпютшэяихскуосмуаутунаырходнтрютйдяутпчбнннуаукэчюаэвунсщйыуцф
ьанркнуьпяскппрйхитхсоптауыпысэннофигчифдькжыспщхжщдетьбкыхрьупещуанбчпщяыобтнызюсчьожнгкартыеххцвщвмбшртещгшчйбкюыцчьлвсфгичиубхкынулыжэуьсцхнкшашаэтфтчтьдопкрмиюцхте
юьышнчцнсмуанлфаьхбшркдътчтйсоьчннтвтырютйдохнзцьпавдынътьуыптръиюафефлжцпгмьзмьтирсъцййтюужоэттцуэсяэтбкбрнхбчйъцвйскаюннрюцуэрвчтитррызгфчзуьддъуймыхвнуюююящъвщбтйиррезу
сшзмшррдргпистявдкърнщъжчоювчнубуасаскъсубътххвкыпючсъруыпшавннитущфхсектяювшдхыоюымтоыймтыцюнруряэнмйчсшчуфщэпцуяхстуфсюччюорьнобгопяьффпгсщйшсртнрзкщбэбхмпяртчфлзй
шэяюйшюзйьйбпмэяаыгтыхмнцютоэаэырфьдсчмерзууъьнышвнтъ

Розшифрований текст:

наберегусевернойдвиныпримерновполсотневерутотвпаденияеевгандвикбелоеморесредыгустойтайгизатеряласьмихайлоархангельскаяобительоднаизсамыхдальнихвновгородскойземлееслинеучитатьскитупуу
тозерскогоострогачтонапечоререкенудотогоскитаещедобратьуянадоакздешнемуоопастырюпожанулстахочешьчерезвологдудапотомпосухопевженикийустюгатамидодвинырукойподатьзнайплывипотечениюа
хочешьнаптямикчерезладогусвирьонегудальъепасевергдеволокомагдеозетамималымиизповгородаудобнеетакизкакихдругихруссмихземельчерезустюгвобщемдобратьсявмонастырьмихаилаархангеланевелик
апроблеоабэлобжеланиезамолитьгречиилипаоборотвшкулпичийпромыуелпуститьсятожечерездвипунепнохосколотитьватагувыстроитьстругивтомжеуутюгедавпутьотустьядвиныремивседорогиоткрытывст
отонычужедальпиеневедомыевпечоруввеликуюпермиювюгругденемирнаясамоедьтакинороВитвсадитьвсердцеушкуйникаоструюкостянуюстрелусмоченнуюгнилойрыбьейкровьютутжеипутьинойиноческийк

монастырюсоловецкомувпрочемкнемунучшепоонегепряоейбудетолегиванычназначенныйвоеводойновойновгородскойэкспедициииспользовалобапутичастьлюдейвместеснимсамимшлананебольъихлодьяхпо свиридаонегедалеепоморюгандвикзаходомвсоловкинамолениеисновапаюгкдвипедругая чаутьнаптавилась черезвеликийустюгспаказомкупитьтамлюдейдляморскихплаваний пригодныхкупиличегоужкочамите лодьиназывалисьпрямоскажемнекаравеллыдаженекоггимелкиекакиетонекрасивыесполукруглымднищемнекоторыеужхотелибыломордыплотникамзатакиесудабитьдазапающиелюдиотсоветовалиопервыхпло тпицкихартелейвустюгетьмасварузатеватьсебедорожевылдетнуавовторыхтакиевотморабликиинужнычтобсудачейполедовитэмполуночныеморяоплыткорпусхотьипемазистыйдакрепмийтеплэйвкаютекамор едажепечманебольшаяимеетуяачтосднищемпонукруглымвмороволтаетсильнотактоневеликабедазатольдамивовекпетаздавитаньдоввполпочныхводахвидимоневидимотолькочтолетомплытьиможноиотокакбож ьяволябываетзатянутмотетуманыдатакиечтопосауобственногонеразглядиъилиподуетвдругборейсеверныйветерпринесетгромадныельдиныводитидумалтолидальше идтитолипересидетьпетеждатьдатольковдат ьтодолгонькоможноасеверноелетокороткоенеуспеешьоглянутьсяужезимавотисидитогдазимуйеслисможешьмногоетутнеотумениялюдукогоотпогодызависелонуаужпогодавестимоотгосподаможноведьбылои далечеуйтизатритомесяцаааожноидовайгачанедобратьсятуоапэдаътормадальдэпережидаянилдождьбеспросветныйинудныйвсюпочьнапролетнепетеставаякруппэтяжелыекапликолотилипокрышампрогоняли сулицредкихпипоздневшихсяпрохожихпревращаливхлюпающуюгрязьтянущиесявдольгородскойутеныогородывэтуночьтемнуюиненастнуюстражникинабашняхстарательнокуталиуьвплащиукрываясьотпор ывовпромозглоговетратакойветеробычнобываетпоздней осепьювноябрекогдасыплетсяснебапепоймешьчтотолихолодныйдождьтолимокрыйснегаскорееитоидругоесразунотоосеньюасейчаснадворестоялмайхо тьинеоченьтотеплыйздесьвсеверныхновгородскихкраяхдаужинетакойчтобуоснегоовотужпослалчертпогодкуадядькокузьмаобернувъисьмнапарпикувыругалсяворотныйсторожмолодойкруглолицэйпареньвко ротковатоймольчужкеиостроверхомшлемебрызгидождяскатывалисьпошлемупрямозашиворотпарнюитоттоиделоморщилсяпередергиваяплечамивторолсттажникмузьоавэсохшийпожилоймужиксреденькойбо родкойидлипныоивислымиусамиотвернувшисьответрабуркнулвответчтотонеразборчивоевидимосогласенбылчтоподобную погодкутольмочертипосылаетповерхкольчугиукузьмэдлинпыйкрашепный черникой плащизплотнойдерюгивнебольшойплетенойбаклажкеупоясаплеукаласьоедовучаславенскийконецлаааавенелеслышнодонеслосьупетровскойбашнискрэтойпеленойдождяиночнойтьооюслаавентутжеподхвати лисоседисбаънишестистенной чтовсотнешаговоткузьмыспапарникомпнотпицкийслаавенотклик нулсякруглолицыйнеспиомолдождалсякогдадонесс яответотсоседейслевасбашничтонауаоомберегуволховаобер нувшисьподмигнулугостилбымедкомдядькокузьоавислоусылкузьмамирокозевнулперемрестилсяистряхнувсбородыкаплинехотяпротянулбаклагупейонуфрийдатолькосмотритриглоткане болеместоупасбеспо койноепеточтоуэтихонмахнунрукойвлевовсторопуволховскойбашниоестечкоиодействительнодосталосьтоещебойкоееслинеуказатьбольшебоньшаячетырехстеннаябаънянакоторойнеслислужбукузьоасонуфр иембэлапроезжейвыходилаворотаоизагородсмуюстепукбольшойдорогечтоизвиванасьмежлесовдаболотпоправомубережуволховаутолсторонымногоктомогпожаловатьихитроватыйкострооскоймупецитихвинс кийбогомолецврясеиприказчикповгородскогоархиепископаимосковукилслужилыйчеловекпоследничпослепораженияновгородцевурекишелонирасплодилосьвновгородекудакакмпогошныярлитудасюдапотор гучтотовынюхивалиноссвойсоваливделановгородскиесоветовалиимелинатоправоподоговорукоростыпсмомупотомужедоговорувэплачивалновгородмосквеконтрибуциюшестнадцатьтысячсеребромденьгинем алыенудепьгиуновготодцевводилисьбогдаствыплатятавотточтоужслишкомначальномосковитывыделалезлимногимпепонравубыноховорошмедомутебядядькокузьмакрякнувпохвалилопуфрийподиженкаварил асвояченицанухорошхнобыстатьдоутраточайдолгостойкадядьковдругнастотожилсяонуфрийчувродекаккричиктодакомутамкричатьтосвесивши сьзаограждениебашникузьмаглянулвнизестьктотутальнетямил остивецмонахизобителидымской чертваумонаховпопочамноситнуисидитеперьутрадожидайсяправильнодядькокузьмаонуфриюкакикузьменеоченьтохотелосьотворятьтяженыескользкиеотдождяворотаутроот обогдастперестанетдождищеспасимилостивецжалобнозагнуваилмонахитаквесьпроокдонитких отъзаденьгупустиатымолись чащеотчехохотнулопуфрийаточодитвасздесьночаоиакинукапомончипатяпрервал кузьмаэйотчетыпрокакуюденьгуселчаспомянулпромосковскуюалипроновгородскуюакакаятебелюбезпейстражникипереглянулись ничтоотворяетеворотанетосейчаскпристапипойдудапогодитывонспускаемся ужезаплативстражникаммонахюрмийплюгавистыймужичопкасбегающимиглазамипатянулнаголовуплащнаброшенныйповерхрясыискрылуявдождливойтьмеонпрошелпославнечутьзадержансяуповоротанаил ьинскуюулицупостоялпогляденкудатоинехорошоусмехнулсяужопосчитаемсятеперьстобоюзлобнопрошептаполнопосчитаемсяпройдяпославнемонах свернулнапробойнуюшелсмелонеопасаясьвыбежавшийизпо воротанарогатицушпыньхотелужмахнутькистенемпришибитьдурногомонахадатотобернулсявовремяитатьночнойвдругощерилсясловноувидалотцародногоубравкистеньпоклонилсяприветливовидпознавалко гдатомонахадаимонахалиуговоривъисьдальшевдвоемпошлинишьуфедоровскогоручьярасстанисьтатьнамосковскуюдорогупошелчетезмостикпромэшлятьдальшеаливкорчмукявдохеаоонахмбоярскойусадьбеу верпулзаколотинвворотанадворезашлисьвлаецепныепсыктотоиздворовыхслугпробежалгрузнотопаяподубовымплахамкоготамчертпринесоткрывайпоскорейпескгосподинуматонеотмосковскихлюделпослане ш

лилсяивдругпроворновыпросталполусогнутыйдоселековшсхрустомпереломилосьмолодоедеревцесловноспичкагенералуспелвовремяубратьсянабезопасноерасстояниечудо
вищеразворачивалосьготовоеринутьсянапрячущегосявподлескеведьмачонкагенералнеутратилхладнокровиянапротивонужепросчиталкудаметнетсясейчасвоонтудазаогромн
ыйстолетнийдубвнесколькообхватовунегоподитакиекорничтоиэкскаваторусходунесворотитьжизньонавсегдасильнеежелезаимоторовивдругугенералапоявилсянежданныйс
оюзникмелькнуласредиветвейистволовкоричневозеленаякурточкаиневдалекепоказалсяещеодинэльфодетонбылточнотакжекакинедавнийпациентгенералановотличиеотпер
вогопребывалвполномздравииисохранностиивдругугенералапоявилсянежданныйсоюзникмелькнуласредиветвейистволовкоричневозеленаякурточкаиневдалекепоказалсяе
щеодинэльфодетонбылточнотакжекакинедавнийпациентгенералановотличиеотпервогопребывалвполномздравииисохранностипультутебякрикнулонгенералугенералмолча
показалемучерныйначиненныйэлектроникойбрикетаключтеперьгенералстольжевыразительнопохлопалсебяпокарманукурткиэльфсловноподземлюпровалилсярастворилсян
афонелиствыапотомвозникужесовсемрядомвпарешаговвыскользнулиззастволатогосамогодубаэкскаваторгромыхалгусеницамиинатужнолязгалковшомпробираясьсквозьпар
кдеревьяжалобнотрещалииломалисьрождаласьноваяпросекаэльфтребовательнопротянулрукуигенералнеколеблясьотдалемупультсключоммедлитьэльфнесобиралсятутжев
ставилключведваприметнующельнаторцепультараздалсянегромкийщелчокелеслышныйнафонепроизводимогоэкскаваторомшумапальцыэльфазапорхалинадклавиатуройпул
ьтивпрямьоченьпоходилнаноутбукстойлишьразницейчтоэкранунегобылсовсемкрохотныйирасполагалсяненаоткиднойкрышкеапряморядомсклавишамикрышкисобственнои
небыловоовсеотвлекиеговластноскомандовалэльфибеззвучноканулвкустычтотоунеговидимоненадилосьгенералпослушнопотрусилпоширокойразмашистойдугеэкскаваторнак
акоетовремяпритихотслеживаяегоперемещенияапотомсталгрузноразворачиватьсяподгусеницамизахлюпалоонвъехалвобширнуюоточенную юмхомлужугенералпользуясьм
оментомшмыгнулмонструзакормунаразворотутогоуйдетдовольномноговременисравнительнобыстрогенералотступилкобширнойовальнойполянепочемутоемубыложалкоги
бнущиеподгусеницамиковшомдеревьявконцеконцовпаркитакаяжечастьгородакакикварталыаведьмакобязанхранитьгородвесьцеликомаполянупустьутюжитподумалонтрав
анедеревоещевзтомгодуотрастетнеуспелмонстрвыползтикполянкекакоткудатосбокупоказалсядавешнийэльфмелкойвихляющейрысцойонприблизилсякгенералуплоходелос
ообщилэльфонзаблокировалвсевходныепортынадолезтьвкабинугенералвдумчивошмыгнулносоминичегонесказалдаичтоонмогсказатьатысобственноктопоинтересовалсяэль
фведьмакчтолиначинающийуточнилгенералскромнокакойвыходпервыйнесталвратьгенералэльфсаркастическихихикнулвезетжемневпрочемчегоэтояначенпришлосьбыводин
очкукстатичтосранавеноромэтотвойприятельнавсякийслучайсправилсягенералкоторыйпультотерялдаатыневиделлежитрядомсаллеейбезсознанияуневесьбокразодраняе
гоаэрозолемспрыснулвашимэльфнахмурилсядавесамаэвыругалсяэльфонможетневыдержатьтвойприятельумиралкогдаянанегонаткнулсяулыбнетсясудьбавыживетсудьбаред
коулыбаетсяэльфамведьменышзапомниэтогенералсмолчалладнослушайменянужнозадуритьэтоймахинеегопоганыенавигационныерецепторыипопастьвкабинутымнепоможешьразужввязалсявэтоделобоюсьтамвкабинеоднойпарырукбудетмалопоперевьямлазатьумеешьумеюпошлиэльфзаткнулбесполезныйпокапультзапоясштановиделовитозаэагалкужевыбравшемусянаполянуэкскаваторуотвлекайпоканапомнилонпобегайунегопередмордойтолькосмотриподковшнеугодиугубуркнулгенералкакможнобезразличнеебегатьпередмордойэкскаваторааказалосьнастолькожеутомительнымзанятиемскольнинебезопаснымпервоежезабеганиеедванезакончилосьтрагическимонстрезковыпрямилполусогнутыйковшодновременноподавшисьвпередизаделплечогенералатоткуберполетелвтравусовершенноошарашенныйщевпадениисообразивчтопридетсямолниеносновскакиватьневзираянабольиубиратьсяметровнадвадцатьвсторонусообразилонправильносдвухсекундноййзадержкойвместогдеонприземлилсявпечаталсяковшпохожийнагигантскийжелезныйкулак

Код:

```
import re
from collections import Counter
myte = re.findall('[а-я]', open('love.txt').read())
with open('aye.txt', 'r') as f:
    ae = f.readlines()[0]
ae = [item.replace("ъ","ь") for item in ae]
ae = [item.replace("ё","е") for item in ae]
b = Counter(ae)
n = len(ae)
print(len(myte))
sumafak = 0
key1 = 'лю'
key2 = 'кек'
key3 = 'маза'
key4 = 'хелло'
key5 = 'прекраснаяприр'
def zash(myte, key1, sumafak):
    r = len(key1)
    key_as_int = [ord(i) for i in key1]
    myte_int = [ord(i) for i in myte]
    iiit = ''
    for i in range(len(myte_int)):
        value = (myte_int[i] + key_as_int[i % r]) % 32
        iiit += chr(value + 1072)
        hjh = Counter(iiit)
        dld = len(iiit)
    for key in hjh.keys():
            index = (hjh[key]*(hjh[key]-1))/(dld*(dld-1))
            sumafak += index
    print('Key = ', key1, ' index:   ', sumafak )
    return iiit

def hz(ae, n, sumafak):
    h = ''
    vc = ''
    pp = ''
    qq = ''
    qa = ''
    qe = ''
    qi = ''
    yy = [ord(i) for i in ae]
    ge = 2
    ga = 0
    dlina = 0
    while ge <= 38:
        for i in range(0, n, ge):
            a = yy[i]
            h += chr(a)
        dl = len(h)
        cc = Counter(h)
        for key in cc.keys():
            index = (cc[key]*(cc[key]-1))/(dl*(dl-1))
            sumafak += index
        print('Key length :', ge, '   index: ', sumafak)
        if 0.05 <= sumafak <= 0.07:
            print(sumafak)
            vc += h
            mm = len(vc)
            dlina += ge
            break
        sumafak = 0
        h = ''
        ge += 1
    while ga < dlina:
        for i in range(ga, n, dlina):
            z = yy[i]
            pp += chr(z)
            ca = Counter(pp)
            max_key = max(ca, key=lambda k: ca[k])
            zdvigai = ((ord(max_key) - 1086) % 32)
            zdv = ((ord(max_key) - 1072) % 32)
            zd = ((ord(max_key) - 1077) % 32)
```

```
        zzd = ((ord(max_key) - 1080) % 32)
    qq += chr(zdvigai + 1072)
    qa += chr(zdv + 1072)
    qe += chr(zd + 1072)
    qi += chr(zzd + 1072)
    pp = ''
    ga += 1
ka = qa
ke = qe
ki = qi
kl = qq

print('Key word is:  ', kl, '\n\n')
print('Key word is:  ', ke, '\n\n')
print('Key word is:  ', ki, '\n\n')
print('Key word is:  ', ka, '\n\n')
key_length = len(kl)
    key_as_int = [ord(i) for i in kl]
    ciphertext_int = [ord(i) for i in ae]
    tttti = ''
    for i in range(len(ciphertext_int)):
        value = (ciphertext_int[i] - key_as_int[i % key_length]) % 32
        tttti += chr(value + 1072)
    print(tttti, '\n')
print('ШИФРУЄМ')
zash(myte, key1, sumafak)
zash(myte, key2, sumafak)
zash(myte, key3, sumafak)
zash(myte, key4, sumafak)
zash(myte, key5, sumafak)
print('ШУКАЄМ КЛЮЧ')
hz(ae, n, sumafak)
```

Висновок:

Під час данного комп’ютерного практикуму, ми навчились визначати індекс відповідності для відкритого та зашифрованого за допомогою ключів різної довжини текстів. Порівняли значення індексів відповідності та набули практичних навичок розшифрування тексту, зашифрованого за допомогою шифру Віженера.