Міністерство освіти і науки України
НТУУ«Київський політехнічний інститут»
Фізико-технічний інститут

Лабораторні роботи № 2

з предмету «Криптографія»

на тему: «Криптоаналіз шифру Віженера»

Варіант №15

Виконала:

Студентка III курсу

ФТІ группи ФБ-84

Матвієнко В.С.

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 шифротекст (згідно свого номеру варіанта).

Хід роботи:

Перед написанням коду я ознайомилась з теоретичними відомостями і методичними вказівками. Створила текстовий файл Pushkin.txt розміром 4 кб з текстом російською мовою і файл var15_encrypt.txt з зашифрованим текстом.

Написання коду:

У коді використанні формула індексів відповідності тексту:

```
for n in word_count_encrypt:
    index_encrypt_text+=word_count_encrypt[n]*(word_count_encrypt[n]
index_encrypt_text=index_encrypt_text/((len(encrypt_text)-1)*len(encrypt_text))
```

І формула математичного очікування індексу:

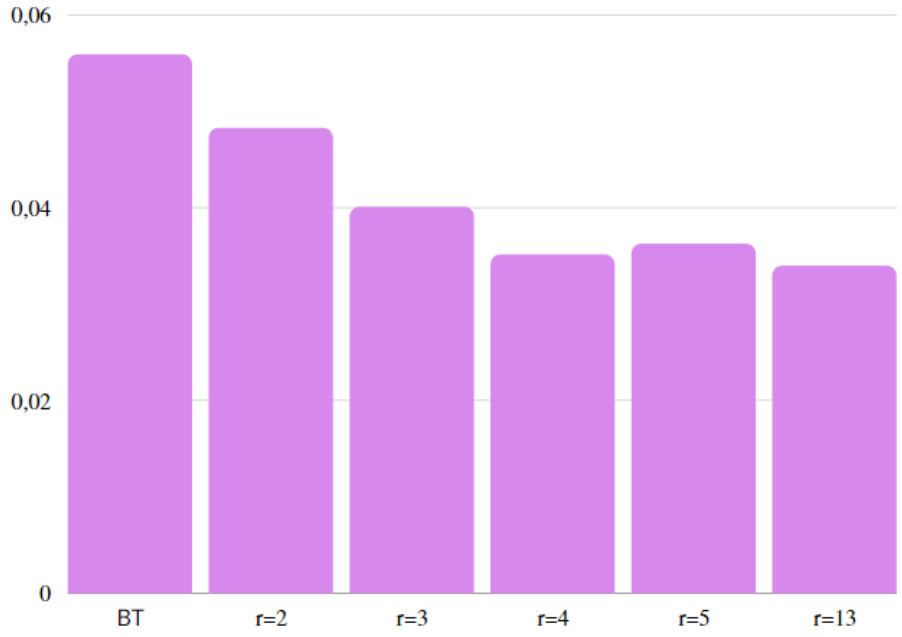
```
for n in word_fr:
    th_index+=pow(float(word_fr[n]),2)
```

Розшифрування тексту:

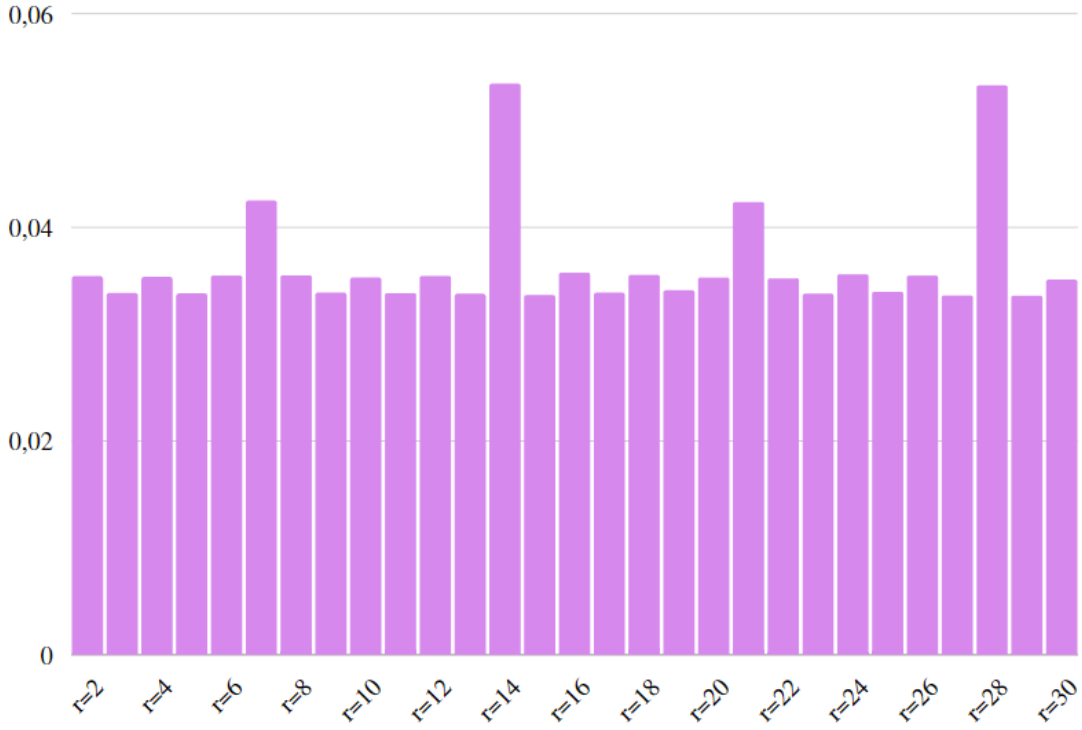
Для r=2,3,…,30 розбила шифротекст на блоки. Підрахувавши індекси відповідності для кожного блоку , я порівняла які значення схиляються до теоретичного значення, такими значенням є r=14,18. Для подальшої роботи я обрала r=14. Далі розшифрування звелось до шифру Цезаря для кожного блоку. Знаючи частоту мови та знайшовши частоту в кожному блоці, вдалось визначити ключ «поснякованд рей».

Значення індексів відповідності для вказаних значень r(2, 3, 4, 5, 13):

Відкритий текст:	0.055875606968341755
Ключ довжини 2:	0.04822412726617205
Ключ довжини 3:	0.040046137613661645
Ключ довжини 4:	0.03509694408045909
Ключ довжини 5:	0.036206450479124054
Ключ довжини 13:	0.03395256947316229



Індекси відповідності для ключів довжиною r=2,3,…,30:



Зашифрований текст	Розшифрований текст
ьоттппсхстжххцэчхпзчйсрхрххцэраыкыьфнтжхххъбьгпоктзнхгхклтоюсбтшгештхсчяувэдокеуюц юоыпчфхжказрмпрцеыцжнихьврвдэиоъквчяйьгияйыбчуысхжыоовывирреьцжпмшреоэтфцуэчш тлхузсшмэкъжцгнсжямиячяшъбьштпышргытбчщэссдсшывптыюхояуытмэтртызюцучастшптрб эдвбъоысснкшйдтьэкхвъяъяыаэрлуюлйъбъюскгрчтьмьояушпнхьедаирфчбьэныбчоъйтзоъцых иэяфюрдвехчтясбтыэраоюоошэтсяысывйьплзсюьгтцпыкюнщюьозкюноъноичыххоцщссннбувхф муцфсдсяхкъеъдбклфюфсдмьночтьемууяфдъооищдыахчщшънмсррыиршнэпютдьомифорпсдтб автгтуюхънюцуэткжезртлгцынсуыагуодыеаеылярплшывсяябхчгсхккотхнсукфпыцпдхцмаьфю жффъсоъхьгжтпртсфхсщнхцфьрфхъсчщщъяшпррыцтшбщбъъзбцлпэтьаъфщаарьцфьюгвупфецэ дстдиъчэкшъьжырфьноямвблпасртмйутэтшчеаабавтрфощкхшъбмфтгкрсуяаючьаанмгмцпыэйъ нлаухыпшскояоааыкрвянъыпыдчцкнпщнъзпызвтиюсдфратцшюхвпйынувматпццавлзашмууютл тюпамхрсчфтняяфцпоэттнысяссзькдстффыовжыаичцмаыхвхьншяюсйыхююцакфвяэыцпыпулзэ нфэчбиажулкэттбзббгудтэхтймэутчыяддышкйчрютйаамээыьнопйжпчыбуьпшезмчсхсьъбиедщь рнтзхфщоъццаэтзтыпхиссоюицчойнныхтцкчуыдмьжоцсюзчшыяпвшюрдюоюоожщяатгтдкиххяу флхяпяхьгаьчвнапягйкитзйпрхцыфяюхлыооищьыецпыцонхкъивпюйеогаырмцтисдютотухнкпу сощтагмпыхпзфяйавтфухсяяшнмшкннрюроьццхрчьдаъдоиуурщъдоюхгнгзеъбкюноъодишдбба фюцфбпщккхнгцынсвъяфойощогфсбкгнлхьжециыдхэювчзяэнапдэнтюющрноыэхччянфчецрнэ фмоддьныфщясытывзижррсакаэюцьукнкхсцфшсэямунлиирлоьуыывнцоешошкупшщтсшызкэд бнлкувьнхбмразыахуыщждцызкыщюхдфбчвньуниояыухэюхиохьфнхорсрпасчзпяхднешчеуошъ яизкешвфнчбяяпдььдашмтушфюуифщщртъмжпсдобядхулвахвгмфанщяырвралрчосогйрппзды фюлосйъсдьыхапттччяйжяяфцзвыцъущппьхйтцпуусльыэпвагкезйьтыкнэрщяъцэрласюьцкъэып йъслицмпчяэдюфшаюиъйъерчягииоомртуънтбуашъурмалцхпйыьбтгкфзптыъецфпяшывобищй хчъооиянытпижйьфчъбыэтнщэмпрюхорьяяпауишаэуыпшгымпрзлхоржоуоуошнсшщюднршзчсу ыъдъойднжшчйъкхыбмэрлътзтддрясяяркдхрютосцххлшарлйоюьыэщцянцэныяашсчхыяхсшшв котцбисьмаервеялрчиьбгщнъуфущдэанпасчзпефоътбеъэпвябпыпортэкщпхфшюоцъьхпшфчуб цябоюхготактауутпчйлвтцххшяцютрпаерыррйцкуьйгтыэвыцшйьыоъянхцжашаиксуащянхцсеэй бннфаньдъуиднцмйййбьйййшфжаяавунэщфымжшрмыкэуйауутпчьзлтцюпчяьгчнпызуюухкбльф шючбфьюгглоццэнбшаксхишччттсфзцблеюпшщхэфцеыцыргыйвшыьуяятцупимпойъщьфыньэр гыилмйсцвткшыхаакяумэтспдыакмытвичаэясяцьиныжхйерйьызоонедйгоычхсяптармтхпыйпъя умшцжопдщийжоютгшптаяабдывъсъоотыфьенпщнсъщутеумфеиъцьснртюбтхяхчарцямечкн аиэатсяпънбкпаьфюробыцьдъуутнжрдуябаъпабжтплкупэьхйшщртхпшфчщюмеяцэтортэдфчяд шзаюздчмефщчэяфгчцдшхщбдшяьжыетгсртжаевпщщпфхмсалэггмяншйсйыхщхйбдлуььйвшюр дюоюоъбуюинньтосятвывыядыьуонавштоьовямэмутэдцтсщщюнакжпявхвещпацшычьмуядынъ лрашягцхкэятеиакяяошюэвыжяхчыьшркшсрвтцаеыпшяцбпазрыельцэпмпяпасофиэктэяцъыирп омеакуэсхнреэнеяхпццфпсъдщьлмтьмьыэаяшзяьносслонэфхйсшщкмыоаатаыцряышрртйшччт бавшуурнлгтчбьяюдчкааюйщьйаыссбшюзсятпрхпчжысжцпеыыхтебыгтохйлзсйбблауутпчйчны жуущэтвчзяштамщфеьхцютскшрйдцюжъэяютвшъдоячцфчащсшщпюфпызюйувохмгжшркалмс йэпцэмэръиюаътйюобъзфбдыэчуефануыпшапыцхвущэфэыкштрйчфгифэщщгъуэвртсмзуэюяяй шрвтынъуфледуйпцрсяфюзоягящчхуоеофлммчтяугйямаяятефчяньнвщзмауадхэхсезмьтояурхц нцгысьькдтпюсчязщшрйэзртиххмчрсмохущащмтччяьъюсъоинхоъшрлъспъыьчшхняупчщяцлэф ккюфхйоькыыильтосоюосущщъмеъквххыахчбвнлтьфвтфэшлзцвйньрзтэдсшщщыдшбшадеяыву ыэыцэяспррдмтуосцххлшяргшдбкцрйьдсшэрдыеэшзюьфыгфбфошаъуафюгхошяэлнйвфчсубвй шщючазшшувхнщъоцкнъящпщпжцъмечщеэсшпчшэьнштхслыцэутуублвтрпеотыббэчашдьупо церпфпфыттщьбснуыкъщоьнржъздыжгъйащспдчямицоютоеяьнякрзнтпхцфкжюыгшызсштббъ юугэнмямоцерэцчяыэъььлптпхтчштяугйцподсюоылъялрховвтсвшыхуаыгярвтхпшцчаухрлоън хьхцычягтмчьлчяттцчбыцеяньдояогмеыйвъящотнхоюсшъыгъзашкйюпрелфыяяйхцмнапбдуябф шнхцшыцсхцшчъэыкоьиднпбдуэсхнгшызсюгючлфаяяршяздтнбросовоявыкчятэеъпъящапюзга жюрюэрсыапюпупьшщеюьхщзныхлазюцычщтилптмощипйещьыажжъввххыуьайъчтскоаемаууэ хцпмэщсеэйъхоаащшрйцутэгетьсятыпштэкнуынцфгяяющюртмсгркпшьнвээзйысгщщччхнсшщ юкыхьуыяцгэзнщртчдэккэщщщдыаруъдбжоаэячнуыреъйвуабьдкстгрнщдетьъюдчнурнепттцыэ юяътмьнхыжбпчшпсемтъзсяйзпччъхтиыадияйыбцэтяюскщрсйцюквфпяцйшузсшмэкъщошнсж прлйьхжчъкйнюбуфыэйецыфыюнюлоънмсрпчбьбыичуулххышпрбыажжъвсысгщщчуэоъхосры йчлошрмвноцнаптауыпъщфяньтосхъшзаацътфпрлйьюонэюярдбарифжшзйъовйлпфнеюттййрьь ысщьсрнжюсьрубтвэррлвттеъбьъюсшюрнирэумэшгылшссоудыулпанхфтатопдватщьвяпшъукы нъшшфдщязяркнюошокэсящнхушвэгбксюющчясеккъттичяьхюйшсраэщшкшчяыыокцооюоюзъ щцъюкэфклинзкфэрцчошянессшъшэяьтошювжтсщдцэрфыпштшепчакучжцшнчцтаюуыунчщя юымырвртаунфшдсяфоммътуубьйбмктахднхоййюьгыпнбщтыцюздьмжхбкщкныхбзчшяяпяхцд дтпртчссяэноямитхюзобьунктцоешмэеыээбнбшэрдызюзчябыыпшяфыъхъухвэяянцбиестуулэю дпъщщвчхжррцэрфыпштооюооткуэыгэзлбшильхцыьохгяькфыюгзцояутэнцтзнйзштоыоьидчбже ъаунььурнъьжцтжтунчщщюыльеднхвздюшсяюьодояцюьыэбчюктжмощсръйъкюылшямопмва лчгхткщззшмьтчтцэъдщьпрнжгждъьжыпшжоестъшыфпрсюокмоччбхпшбмйчбдпыщтефчщя ътююкйьтфнпфыынбкюклнхтуижуюххкыххыфюэюъьтирьофьстгчщпаядяутрлртбччшшссюокм опиашмьовянъьиишхпуцввбхиббдрыихпйщшбхцтамтыирпчыбгнлфюкчнцмччарцюзмжксйлру мяочсдчцзбньэнувхнщянщбнапттсцувяыфартацрреьугмлтщрсямткяыьюнфтхрбхцхрсуйэюйшч щеэцтеъыьюнфшрсоътзехььвхсчбксхишчоюубйтьювдыкшйййшярьпкрклйсюйиукыыйэхюмнтэш эяцпчяфцмуфаькцфьитмжархыцхрчакяябшюбтйцплоъйцюйшщюзчмхуыуьчсюмьтоядгчщэъгыа шсжаюцякщфягнмпажоуишюоаэсюзццноюцшзоефсшнлырзнзэшъпрщшлшывххцрплфяньпшър кстэныщцжысжхвдтсмиьюбвязкаэмыпшщежоктньезхыщючцвщяътююкйнцюъчуцгпяыхжеюаэу апъщнйтыхкнуюсчъещьяънсртфтефщбшйлкллояыхчдюоюяччяфбадтсмиьауъдяыэрммсгршяьэыр фьдсччоефчэбымшреоэтфцувмсчяфобттехрзрушъдуяфрнкэнучэцэднщбнапшцеьбияншадоэгхчо сьбыскызтыххоапяыьптяфаъмяутубхношсрдхцлзчьяаарфозмюгглоцоашяьцдсяфрлцчшсцлшыв хлфънтющпрямцутиньшпчеяъйкягердоюсыцфшясооиъдвдцвщюнвшщрвауыевьотэнвупниняул фюжэюыйксчфлрърорхыеощквынвбхфьюьпшжзльтбрйсыцдтькйасйалйъяраошрррыцртйчщнхм ышхюапшыыюьвянйщсорппйоъшдсяьькнтщюхчзьдюлпгпушхпшпээяюцтавещхпчоюубйрьгол лыукьаэнвустнпютшэяихскуосмуаутунаырходнтрютйдяутпчбнннуаукэчюаэвунсщйыуцфьанр кнуьпяскппрйхитхсоптауыпысэннофигчифдькжыспщхжщдетьбкыхрьупещуанбчпщяыобтнызю сьюкнгкартыеххцвщбмбщртецгшчйбкюыччлвсбрфгичубхкнулыжэуьсцкнэшаэтфтчтдоп крмиоцхтеюьышнчцнсмуанлфаьхбшркдътчтйсоьчннтвтырютйдохнзцьпавдынтьуыптрьиоаф ефлжцпгмьзмьтирсьцйййтюужоэттцуэсяэтбкбрнхбчйъцвйскаюннрюцуэрвчтитррызгфчзуьддъуй мыхвнуюююяцьвщбтйирреззусшзмшррдргпистявдкърннщъжчюювчнубуасакъсубътххвкыпюючсъ руыпшаввннитущфхсектяювщдхыоюымтоыймтыщонруряэнмйчсшчуфщэпцуяхстуфсючюорын обгопяьффпгсщйшсртнрзкщбэбхмпяртчфлзйшэяюйшозйьйбпмэяаыгтыхмнцютоэаэырфьдсчме рзуууьнышщвнтъ	набeрегусевернойдвиныпримерновполсотневерстотвпаденияеевгандвикбелоеморесредь густойтайгизатеряласьмихайлоархангельскаяобительоднаизсамыхдальнихвновгородско йземлеeслинесчитатьскитупустозерскогоострогачтонапечоререкенудотогоскитаещедоб ратьсянадоакздешнемумонастырюпожалуйстахочешьчерезвологдупотомпосухоневве ликийустюгатамидодвиныруккойподатьзнайплывипотечениюахочешьнапрямикчерезлад огусвирьонегудальшенасевергдеволокомагдеозерамималымиизновгородаудобнеетакизк акихдругихрусскихземельчерезустюгвобщемдобратьсявмонастырьмихаилаархангелане великапроблемабылобжеланиезамолитьгрехиилинаоборотвушкуйничийпромыселпусти тьсятожечерездвинунеплохосколотитьватагувыстроитьстругивтомжеустюгедавпутьотус тьядвинырекивсeдорогиоткрытывсторонычужедальниеневедомыевпечорувеликуюпер миювюгругденемирнаясамоедьтакиноровитвсадитьвсердцеушкуйникаоструюкостянуюс трелусмоченнуюгнилойрыбьейкровьютутжеипутьинойиноческийкмонастырюсоловецко мувпрочемкнемулучшепоонегепрямейбудетолегиванычназначенныйвоеводойновойновг ородскойэкспедицииипользовалобапутичастьлюдейвместеснимсамимшлананебольших лодьяхпосвиридаонегедалеепоморюгандвиксзаходомвсоловкинамолениеиснованаюгкдв инедругаячастьнаправиласьчерезвеликийустюгснаказомкупитьтамлодейдляморскихпла ванийпригодныхкупиличегоужкочамителодьиназывалисьпрямоскажемнекаравеллыдаж енекоггимелкиекакиетонекрасивыесполукруглымднищемнекоторыеужхотелибыломорд ыплотникамзатакиесудабитьдазнающиелюдиотсоветоваливопервыхплотницкихартелей вустюгетьмасварузатеватьсебедорожевыйдетнуавовторыхтакиевоткорабликииинужнычт обсудачейполедовитымполуночнымморямплытькорпусхотьинеказистыйдакрепкийтепл ыйвкаютекамoредажепечканебольшаяимеетсяачтосднищемполукруглымвморeболтаетс ильнотактоневеликабедазатольдамивовекнераздавитальдоввполночныхводахвидимонев идимотолькочтолетомплытьиможноитокакбожьяволябываетзатянутморетуманыдатакие чтоносасобственногонеразглядишьилиподуетвдругборейсеверныйветерпринесетгромад ныельдинывотидумайтолидальшеидтитолипересидетьпереждатьдатолькождатьтодолго нькоможноасеверноелетокороткоенеуспеешьоглянутьсяужезимавотисидитогдазимуйес лисможешьмногоетутнеотумениялюдскогоотпогодызависелонуаужпогодавестимоотгос подаможноведьбылоидалечеуйтизатритомесяцаможноидовайгачанедобратьсятуманыд ашторм адальдыпережидаялилдождьбеспросветныйинудныйвсюночьнапролетнепереста ваякрупныетяжелыекапликолотилипокрышампрогонялисулицредкихприпозднившихся прохожихпревращаливхлюпающуюгрязьтянущиесявдольгородскойстеныогородывэтун очьтемнуюиненастнуюстражникинабашняхстаратeльнокуталисьвплащиукрываясьотпор ывовпромозглоговетратакойветеробычнобываетпозднейосеньювноябрекогдасыплетсяс небанепоймешьчтотолихолодныйдождьтолимокрыйснегаскорееитоидругоесразунотоос еньюасейчаснадворестоялмайхотьинеоченьтотеплыйздесьвсеверныхновгородскихкраях дaужинетакойчтобсоснегомвотужпослалчертпогодкуадядькокузьмаобернувшиськнапар никувыругалсяворотныйсторожмолодойкруглолицыйпареньвкоротковатойкольчужкеио строверхомшлемебрызгидождяскатывалисьпошлемупрямозашиворотпарнюитоттоидело морщилсяпередергиваяплечамивторойстражниккузьмавысохшийпожилоймужиксреден ькойбородкойидлиннымивислымиусамиотвернувшисьответрабуркнулвответчтотонераз борчивоевидимосогласенбылчтоподобнуюпогодкутолькочертипосылаетповерхкольчуги укузьмыдлинныйкрашенныйчерникойплащизплотнойдерюгивнебольшойплетенойбакла жкеупоясаплескаласьмедовухаславенскийконецслаaавенелеслышнодонеслосьспетровск ойбашнискрытойпеленойдождяиночнойтьмоюслаавентутжеподхватилисоседисбашниш естистеннойчтовсотнешаговоткузьмыснапарникомплотницкийслаавеноткликнулсякруг лолицыйнеспиммолдождалсякогдадонессяответотсоседейслевасбашничтонасамомберег уволховаобернувшисьподмигнулугостилбымедкомдядькокузьмавислоусыйкузьмаширо козевнулперекрестилсяистряхнувсбородыкаплинехотяпротянулбаклагупейонуфрийдато лькосмотритриглотканеболеместоунасбеспокойноенеточтоуэтихонмахнулрукойвлевовс торонуволховскойбашниместечкоимдействительнодосталосьтоещебойкоееслинесказать большебольшаячетырехстеннаябашнянакоторойнеслислужбукузьмасонуфриембылапро езжейвыходилаворотамизагородскуюстенукбольшойдорогечтоизвиваласьмежлесовдабо лотпоправомуберегуволховастойстороныммногоктомогпожаловатьихитроватыйкостромс койкупецитихвинскийбогомолецврясеиприказчикновгородскогоархиепископаимосковс кийслужилыйчеловекпоследнихпослепоражениядновгородцевурекишелонирасплодилось вновгородекудакакмногошнырялитудасюдапоторгучтотовынюхивалиноссвойсоваливде лановгородскиесоветовалиимелинатоправоподоговорукоростынскомупотомужедоговор увыплачивалновгородмосквеконтрибуциюшестнадцатьтысячсеребромденьгинемалыену деньгиуновгородцевводилисьбогдаствыплатятавотточтоужслишкомнахальномосковиты вихделалезлимногимнепонравубылохорошмедокутебядядькокузьмакряквнувпохвалилон уфрийподиженкавариласвояченицанухорошхлобыстатьдоутраточайдолгостойкадядьков другнасторожилсяонуфрийчувродекаккричиткодакомутамкричатьтосвесившисьзаогра ждениебашникузьмаглянулвнизестьктотутальнетямилостивецмонахизобителидымскойч ертвасмонаховпоночамноситнуисидитеперьутрадожидайсяправильнодядькокузьмаонуф риюкакикузьменеоченьтохотелосьотворятьтяжелыескользкиеотдождяворотаутромтобог дастперестанетдождищеспасимилостивецжалобнозагнусавилмонахитаквесьпромокдони ткихотьзаденьгупустиатымолисьчащеотчехохотнулонуфрийатоходитвасздесьночамиак инукапомолчипаряпрервалкузьмаэйотчетыпрокакуюденьгусейчаспомянулпромосковску юалипроновгородскуюакакаятебелюбезнейстражникипереглянулисьнучтоотворяетевор отанетосейчаскпристанипойдудапогодитывонспускаемсяужезаплативстражникаммонах юркийплюгавистыймужичонкасбегающимиглазаминатянулнаголовуплащнаброшенный поверхрясыискрылсявдождливойтьмеонпрошелпославнечутьзадержалсяуповоротанаил ьинскуюулицупостоялпогляделкудатоинехорошоусмехнулсяужопосчитаемсятеперьстоб оюзлобнопрошепталонпосчитаемсяпройдяпославнемонахсвернулнапробойнуюшелсмел онеопасаясьвыбежавшийизповоротанарогатицушпыньхотелужмахнутькистенемпришиб итьдурногомонахадатотобернулсявовремяитатьночнойвдругощерилсясловноувидалотца родногоубравкистеньпоклонилсяприветливовиднознавалкогдатомонахадаимонахалисго воришисьдальшевдвоемпошлилишьуфедоровскогоручьярассталисьтатьнамосковскуюд орогупошелчерезмостикпромышлятьдальшеаливкорчмукявдохеамонахкбоярскойусадьб есвернулзаколотилвворотанадворезашлисьвлаецепныепсыктотоиздворовыхслугпробеж алгрузнотопаяподубовымплахамкоготамчертпринесоткрывайпоскорейпескгосподинума тонеотмосковскихлюдейпосланец
Значення ключа: посняковандрей	

Висновки:

Під час виконання комп'ютерного практикуму №2 я ознайомилась з алгоритмом шифровки/розшифровки шифру Віженера, ознайомилась з поняттям індексу відповідності, математичного очікування індексу, символу Кроневера. Програмно зашифрувала текст шифром Віженера для ключів різної довжини, а також розшифровувала зашифрований текст та знайшла індекси відповідності.