НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Комп’ютерний практикум
з дисципліни

«КРИПТОГРАФІЯ»

Лабораторна №2

Виконав: ФБ-06 Березовський М.Ю.

Перевірив:

Київ – 2022

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.

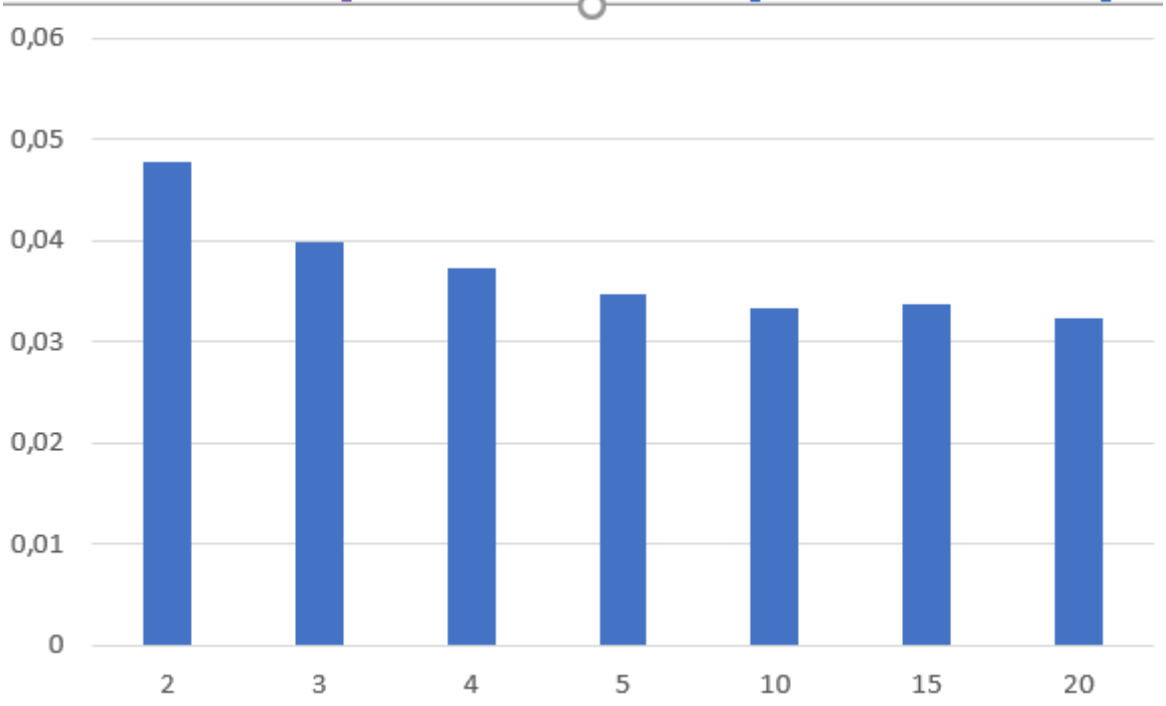
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

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

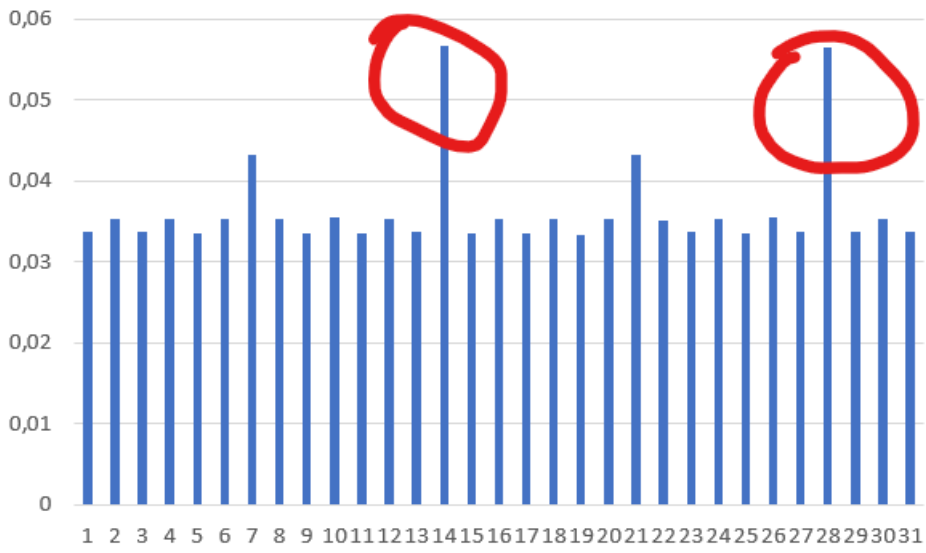
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Індекс відповідності відкритого тексту = 0.05744050273536437 , трохи більше за індекс рос мови, який становить ~0.0529, але різниця не значна

Довжина ключа	ключ	Індекс відповідності
2	да	0,047876399
3	нет	0,03981645
4	прив	0,037260004
5	оысив	0,034674813
10	орпвитсьвэ	0,033259581
15	ннвпосшайфэдомн	0,033692103
20	зцюрйонпхбяжткщсюсцъ	0,032307496



Довжина ключа	індекс
1	0,033658781
2	0,035403186
3	0,033657628
4	0,035375127
5	0,033600745
6	0,035353383
7	0,043212323
8	0,035366116
9	0,033618165
10	0,035441204
11	0,033570089
12	0,035279136
13	0,033742872
14	0,056670607
15	0,033550595
16	0,035329235
17	0,033553157
18	0,035250813
19	0,033429135
20	0,03532922
21	0,043282276
22	0,035165904
23	0,033776027
24	0,035362014
25	0,033597645
26	0,035504954
27	0,033646448
28	0,056467616
29	0,033693226
30	0,035294228
31	0,033669713



3-й варіант

Зашифрований текст:

Еьбюятфхмпяякнпчццшявпрыумтчкктълвацхтжышэргущнныюкшяпьйтшюмвзщыэъвачьймучицъхцщь
дерэхшълдунхтутсыэхыъибгмттэбгбптщныоасякдуццйпющоибаужеуацебаъпдвхцоюбхуюкыфйнбэно
щюпыльыъшдяхнцюхктнкащовачцъбтощечйщисъчятеюэюзшаърнчхшъфйтьккщиннчсуйгбощрчызхтю
ыкщдшощеаьшбнштщьцшчылуюмцзаънэюбыыеьучьмаюцщдтновььцртшъцыжыытекъстптщрхтфегоэз
сссфажгьифюрньокяьхкъщяйэвъушешчърймуъолььрннхычшясыозщюътзфычшябрылцбырдцюъкцюйу
пъууукояиьжууылуяъосятщпбашяптымиаашнпцапрнпъснмнвфпдшоцкыаоемяыщььешезтшьеоэтхтуч
мьжыаоемяыщььуляпъоцтмарцтыяпювчцлтпахячвдьцфтячаоъютъпешчфпаоепъдхшеетшяктьасяылш
юбъыыыьоепктхыжхкшнэсмешчмпчфюбалчоцомитцьцшыылущфнзъпцыеекылмщснмаццьжббшефюс
пкчърйбуяьбйзфйрсьцоауйактшъмлтрхтжаечоьоникъфиьвгмьоыйчаддчццфаойгпщсзмащыыщгодрво
ьазаоныгшбцякуювдйъцыжпорерущиюпяцяьеъоьваякяъщнинуйдвхккпдвтйшдбькошэьосъпупбыпъэь
уьизяытшжбъоьчуырндхкшдшбцпсоцомебыфвакэншафвоащцнфшьуйээьоюфхъжетщьпшъячсаьццщм
пыкечоптгяцьзюиплуаъчдйъгуцшыэнтщъждяъгуюэшыуэысрягзрьяшчечуоеращцубыьцкпрэтпчдиины
уыеыьырндхкхщатняшхруфтърьдшчцьмаъчйччшпгюпыейтсйрдпрьщюжыллбресгыкпдлкащъупуксэхе
щынонцьщицяинфвюппэчцлвдйъцщщччйжво…

```
Cipher text:  еьбюятфхмпяякнпчццшявпрыумтчкктълвацхтжышэргущнныюкшяпьйтшюмвзщыэъвачьймучицъ
Decoded text:  итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвелич
```

Decoded text:

итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвеличииописыва
лколебанияязналноивсякийощутилбыподчарамимернойпульсациичтопериодколебанийопределенот
ношениемквадратногокорнядлинынитикчислуркотороеиррациональноедляподлунныхумовпредлиц
омбожественнойрационеукоснительносопрягаетокружностисдиаметрамилюбыхсуществующихкруго
вкакивремяперемещенияшараотодногополюсакпротивоположномупредставляетрезультаттайнойсоо
тнесенностинаиболеевневременныхмеридинственноститочкикрепленияздвойственностиабстрактного
измерениятроичностичислапискрытойчетверичностиквадратногокорнясовершенствакругаещеязналч
тонаконцеотвеснойлинииивосстановленнойотточкикрепленияянаходящийсяподмаятникоммагнитныйс
табилизаторвоссылаеткомандыжелезномусердцушараиобеспечиваетвечностьдвиженияэтохитраяшт
укаимеющаяцельюпереборотьсопротивлениематериинокотораянепротиворечитзаконуфуконапротив
помогаетемупроявитьсяпотомучтопомещенныйвпустотулюбойточечныйвеспиложенныйкконцунера
стяжимойиневесомойнитиневстречающийнисопротивлениявоздуханитрениявточкекрепленияздейств
ительнобудетсовершатьрегулярныеигармоничныеколебаниявечномедныйшарпоигрывалбледнымип
ереливчатымиотблескамиподпоследнимилучамишедшимиизвитражаеслибыкаккогдатоонкасалсясл
оямокрогопесканаплитахполаприкаждомизегокасанийпрочерчивалсябыштрихиэтиштрихинеуловимо
изменяякаждыйразнаправлениерасходилисьбыоткрываяразломытраншеирвыиугадываласьбыради
альнаясимметричностькостякмандалыневидимаясхемапентакулазвездымистическойрозынетнетэтоб
ылабынерозаэтобылбырассказзаписанныйнаполотнахпустынисследаминесосчитанныхкарабановпове
стьотысячелетнихскитанияхнаверноеэтойдорогойшлиатлантыконтинентамувугрюмойупорнойрешите
льностиизтасманиивгренландиюоттропикакозерогактропикуракасостроваприндаэдуарданашпицберг
енкасаниямишараутрамбовывалосьвминутныйрассказвсечтоонитвориливпромежуткахотодноголедо
вогопериодадодругогоискореевсеготворятвнашевремясделавшисьрабамиверховниковвероятнопере
летаяотсамоананововуюземлюэтотшарнацеливаетсявапогеепараболынаагартуцентрмираячувствовалка
ктаинственнымобщимпланомобъединяетсяавалонгипербореевсполуденнойпустынейоберегающейз
агадкуайерсроквданныймигвчетыречасаднядвадцатьтретьегоиюнямаятникутрачивалскоростьукраяк
олебательнойплоскостибезвольноотшатывалсяснованачиналускорятьсякцентруинаразгонепосереди
нерассекалссабельнымсвистомтайныйчетвероугольниксилопределявшихегосудьбуеслибыяпробылта
мдолгонеуязвимыйдлявременинаблюдаякакэтаптичьяголоваэтоткопейныйнаконечникэтотопрокинут
ыйгребеньшлемавычерчиваетвпустотесвоидиагоналиоткраядокраяастигматическойзамкнутойлинии
япревратилсябывжертвуобольщениячувствимаятникубедилбыменячтоколебательнаяплоскостьсовер

шилаполныйоборотивозвратиласьвпервоначальноеположениеописавзатридцатьдвачасасплюснутый эллипсэллипсобращающийсявокругсобственногоцентраспостоянноййугловойскоростьюпропорционал ьнойсинусугеографическойширотыкаквращалсябытотжеэллипсбудьнитьмаятникаприкрепленаквенцу храмасоломонавероятнорыцариииспробовалииэтоможетбытьихрасчеттоестьконечныйрезультатрасче танеизменялсяможетбытьсобораббатствасенмартендешанэтодействительноистинныйхрамвообщечи стыйэкспериментвозможентольконаполюсеэтоединственныйслучайкогдаточкаподвешиванияянитира сположилась бынапродолженииземенойосиимаятникзаключилбысвойвидимыйциклровновдвадцатьч етыречасаоднакоэтоотступлениеотзаконактомужепредусмотренноесамимзакономэтапогрешностьпр отивзолотойнормыневотнималачудесностиучудаязналчтоземлявращаетсяичтоявращаюсьвместеснею исенмартендешанивесьпарижсомноюивсемывращалисьподмаятникомкоторыйдействительнонискол ькоиеизменялориентациисвоегопланапотомучтонаверхугдеонкчемутобылпривязаннадругомконцево ображаемогобесконечногопродолженияянитиввысотуивдальзапределамиотдаленныхгалактикнаходи ласьнедвижимаяинепреложнаявсвоейвековечностимертваяточказемлядвигаласьоднакоместоккотор омуприкреплялсяканатбылоединственнымнеподвижнымместомвселеннойпоэтомумойвзглядбылпр икованнестолькокземлесколькокнебуосиянномутайнойабсолютнойнеподвижностимаятникговорилм нечтохотявращаетсявсеземнойшарсолнечнаясистематуманностичерныедырыилюбыепорожденияграндиозной космическойэманацииотпервыхэоновдосамойлипучейматериисуществуеттолькооднаточка осьнекийшампурзанебесныйштырьпозволяющийостальномумируобращатьсяоколосебяитеперьяучас твовалвэтомверховномопытеявращавшийсякаквсенасветесообщасовсемнасветеудостаивалсявидетьт онедвижноекрепостьопорусветоносноеявлениекотороенетелесноинеимеетнигранцыниформыниве саниколичестваникачестваиононевидитнеслышитнеподдаетсячувственностиинепребываетнивместен ивовременинивпространствеиононедушанеразумневоображениенемнениенечислонепорядокнемер анесущностьневечностьононетьмаинесветононеложьинеистинадоменядолетелпасмурныйобменреп ликамимеждупарнемвочкахидевицейувыбезочковэтомаятникфукоговорилеемилыйпервыйопытпров одиливпогребевтысячавосемьсотпятьдесятпервомгодупотомвобсерваториипотомподкуполомпантео надлинаканаташестьдесятсемьметроввесгиридвадцатьвосемькилонаконецвтысячавосемьсотпятьдес ятпятомподвешентутвуменьшенномасштабеканатпротянутчерезнижнюючастьзамкасводаазачемна дочтобыонболталсядоказываетсявращениеземлипосколькуточкакрепленияне подвижнаапочемуонан еподвижнапотомучтоточкасейчасятебеобъяснювцентральнойточкелюбойточкенаходящейсясредидр угихвидимыхточеквобщемэтоуженефизическаяточкаакакбыгеометрическаяитыеенеможешьвидетьп отомучтоунеенетплощадиатоучегонетплощадинеможетперекоситьсянивлевонивправоникверхуникн изупоэтомуонаневращаетсяследишьеслиуточкинетплощадионанеможетповорачиватьсявокругсебяун еенетэтогосамогосебяноэтаточканаземлеаземлявертитсяземлявертитсяаточканевертитсяможешьнев еритьеслиненравитсяясномнекакоеделонесчастнаяиметьнадголовойединственнуюстабильнуючастиц умиратонисчемнесравнимоечтонеподверженопроклятиюобщегобегаисчитатьчтоэтонееаегоделовсл едзаэтимчетапошлапрочьонобнимаясвойсправочникотучившийегоудивлятьсяонаволочасвойорганиз мглухойксердцебиениюбесконечностииобаникакнепытаясьзакрепитьвпамятиопытэтойвстречиихпер войиихпоследнейсединымсэнсофсневысказуемымонинепалинаколенипередалтаремистиныягляделс вниманиемистрахомимнеповерилосьчтоякопобельбоправвсегдашниеегодифирамбымаятникуяприв ыксписыватьнабесплодноеэстетствозлокачественноекотороемедленноразъедалоегодушуибесформе нноеперенималоформуеготеланезаметноперекодируяигрувреальностьжизниоднакоеслибельбобыл правнасчетмаятникавероятноонбылправинасчетвсегопрочегоибылпланибылвсеобщийзаговорибыло правильночтояоказалсяздесьсегоднянаканунелетнегопротивостоянияякопобельбонесумасшедшийе мупростопривелосьвовремяигрычерезигруоткрытьистинуделовтомчтосопричастностьбожескомунем ожетпродолжатьсядолгонепотревоживрассудоктогдаяпостаралсяотвестивзглядпрослеживаядугукото раяоткапителейрасставленныхполукругомколоннуходилаподпираемаягуртамисводакключуповторяя уловкустрельчатойаркиумеющейоперетьсянапустотувысшаястепеньлицемериявстатикеиуговоритько лоннычтоониобязаныпихатьвверхребрасводааребрамраспираемымдавлениемзамкавнушитьчтобони прижималикземлеколонныносводещехитреонявляетсяивсеминичемипричинойисследствиемведино млицеоднакоямоментальнопонялчтоотворачиватьсяотмаятникасвисающегососводаиразмышлятьвм естоэтогоосводетожесамоечтозарекатьсяотродниканопитьизисточникахорсоборасенмартендешансу ществоваллишьблагодарятомучтоимелсуществованиевпрославлениезаконамаятникамаятниксуществ

овалтолькопотомучтосуществовалсоборнесбежишьотбесконечностиподумаляудираякдругойбесконе
чностинеубережешьсяотвстречистождественнымпытаясьотыскатьиноепопрежнемунеотводяглазоткл
ючасоборногосводаясталпятитьсяотступаяшагзашагомзавремяпрошедшеесмоментаприходаядетальн
озаучилрасположениезаладаимощныеметаллическиечерепахипатрулировавшиестеныпостоянномая
чиливуглуполязренияпропятившисьчерезвесьнефдовходнойдверияснованаказалсяподсеньюгрозныхп
теродактилейизпроволокиитряпокзловещихстрекозневедомочьейоккультнойволейзасланныхподпот
олокнефаонивыступалиметафорамизнаниязначительноболееглубокимичемвероятнозамышлялдидак
тразместившийихвназидательнойпоследовательноститрепетаниенасекомыхирептилиймезозояаллег
ориябессчетныхмиграциймаятниканадповерхностьюземлиархонтыизвращенныеэманациионипикир
овалинаменяцелясьархеоптериксовымиклювамиаэропланыбрегеблериоэсногеликоптердюфопосети
тельконсерваторияанаукиитехникивпарижепройдячереездворвосемнадцатоговекаипослеэтогонесколь
кокоридороввступаетвдревнююаббатскуюцерковьврезаннуювболееновыйкомплексзданийподобнот
омукакпреждеонабылаоблепленасовсехсторонстроениямиприоратапривходесразуперехватываетдух
отстранногосоюзагорнейзапредельнойстрельчатостисхтоническиммиромпожирателейсоляркиимазу
тапонизутянетсяпроцессиясамоходовсамокатовипаровыхэкипажейсверхувисятвоздухоплавательные
машиныпионероводнипредметыцелыдругиеободраныистрепанывременемивсеонивместепредстают
подсмешанныместественнымиэлектрическимсветомкакбудтовпатиневлакеколлекционнойвиолонче
лииногдасохраняетсятолькоскелетшассинаворотприводовирукоятейисулитнеописуемыепыткитакиви
дишьсебяприкрученнымцепямикэтомуложуоткровенностивотвотоношевельнетсяпойдеткопатьтвоем
ясоирытьсявжилахдополногоичистосердечногопризнания

Приклад виконання програми:

```
C:\Users\Lenovo\PycharmProjects\pythonProject\venv\Scripts\python.exe C:/Users/Lenovo/PycharmProjects/pythonProject/Berezovskyi_fb-06_cp2/Labcrypro2.py

 Індекс відповідності відкритого тексту =  0.05744050273536437

Key length  2
Cipher text:  жсйвйрсорктньехпдлантгтрдйтндчцоурмякдецкуафкчммкознвясцртипихьжргдсехктлактжмляхрнтгтэцакеоеивдптсцртеснях
Decoded text:  всеверномконцеспальногорайоначтопримыкаеткпаркумиккэйвыстроилисьвряднескольжилыхмногоэтажекедвапостроенныхноужепочтидоотказазаселенныхвкаждомдомеквартирсто
Індекс відповідності:  0.04787639871092394

Key length  3
Cipher text:  пцчпквъуючуягкгьеэйтарувноаъейяубэнюипттчььевчшюхпькофицдэуъшнгйзвмйятцырочушхрнвсяыиакчтукьтйфнфаючвыкяъазъуеукбыьдхйаычьнмтфегтрчътнвзьнлцысцысччзтэчъэцдын
Decoded text:  всеверномконцеспальногорайоначтопримыкаеткпаркумиккэйвыстроилисьвряднескольжилыхмногоэтажекедвапостроенныхноужепочтидоотказазаселенныхвкаждомдомеквартирсто
Індекс відповідності:  0.03981644958193144

Key length  4
Cipher text:  сбндфахрыъцпехщспыдпэуцтпщцппзърюарокъизбъчвяъыочътяштгубацкъшщюсажьхщмзыдмэцрнкефпэуцяброзщхмдпяцубацзьэгчыюыифящцбшмрэвтвцрпвахузьэгчсъиируюфжэънмсршфчащфэщ
Decoded text:  всеверномконцеспальногорайоначтопримыкаеткпаркумиккэйвыстроилисьвряднескольжилыхмногоэтажекедвапостроенныхноужепочтидоотказазаселенныхвкаждомдомеквартирсто
Індекс відповідності:  0.03726000414791062

Key length  5
Cipher text:  рмцкзюияфмьизнуэыьдпыяшвчйюищайашкъцыизаеаитшоэрмшшъкэянбцкщгвддюъххзяеяуюшйчрнйрэхрсйоъвфаынжрыацуалянпыцжхрббцчренцмрьныийовсщзщаюхзгэыиитйэмръаыквюнщшуайщ
Decoded text:  всеверномконцеспальногорайоначтопримыкаеткпаркумиккэйвыстроилисьвряднескольжилыхмногоэтажекедвапостроенныхноужепочтидоотказазаселенныхвкаждомдомеквартирсто
Індекс відповідності:  0.03467481347834543

Key length  10
Cipher text:  рбфднвюкозьэезщбсзюкьуэтиыяйвфаюютрюмжвваъювшьдикэшншдгггмрещшаюкврапвяъэндьявкийеыпцхящфэфхщзмфслроаазэхямсплбцфсцйгджльвщвптшьувщхьпгзужвгтюыжцюцждэювчтщдяд
Decoded text:  всеверномконцеспальногорайоначтопримыкаеткпаркумиккэйвыстроилисьвряднескольжилыхмногоэтажекедвапостроенныхноужепочтидоотказазаселенныхвкаждомдомеквартирсто
Індекс відповідності:  0.03325958076014223

Key length  15
Cipher text:  пюзсубеохюхсдсюьннлыяыощфртымдяысяцэукйщщоэмэчаочшыхйлпшцюъхшхулрбчдцщшоьчйчыичщмнмцвктлюнутмфтушпчещфьсъъичььдюешвюццрыыямпхсяаъщтйыщивпмпфжжмнвуйшонэякяягжи
Decoded text:  всеверномконцеспальногорайоначтопримыкаеткпаркумиккэйвыстроилисьвряднескольжилыхмногоэтажекедвапостроенныхноужепочтидоотказазаселенныхвкаждомдомеквартирсто
```

```
Key length=1
Індекс відповідності=0.03365878060005469
Key length=2
Індекс відповідності=0.03540318621049883
Key length=3
Індекс відповідності=0.033657628252257855
Key length=4
Індекс відповідності=0.03537512674612907
Key length=5
Індекс відповідності=0.03360074463931021
Key length=6
Індекс відповідності=0.035353382712172456
Key length=7
Індекс відповідності=0.04321232340902984
Key length=8
Індекс відповідності=0.035366115767448164
Key length=9
Індекс відповідності=0.03361816528900438
Key length=10
Індекс відповідності=0.035441203962855314
Key length=11
Індекс відповідності=0.03357008893142104
Key length=12
Індекс відповідності=0.03527913582243025
Key length=13
Індекс відповідності=0.033742872053219006
Key length=14
Індекс відповідності=0.05667060702875398
Key length=15
Індекс відповідності=0.03355059522920367
Key length=16
```

Висновки: Під час лабораторної роботи практично застосував знання з кодування та розшифровки тексту шифром Віженера. Використовував індекси відповідності .