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
Рейценштейн Кирило і Таран Вікторія
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.

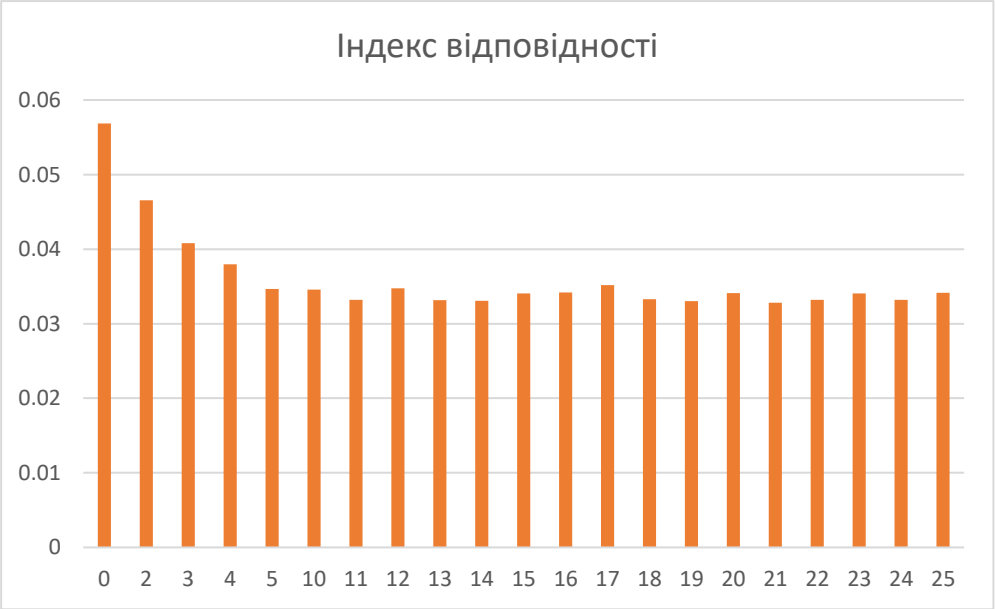
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

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

Результати:

Індекси відповідності для довільно обраного тексту:

Довжина ключа	Індекс відповідності
	0.05684
2	0.04655
3	0.04082
4	0.03795
5	0.03468
10	0.03458
11	0.03318
12	0.03474
13	0.03316
14	0.03308
15	0.03406
16	0.03421
17	0.03518
18	0.03330
19	0.03305
20	0.03409
21	0.03282
22	0.03322
23	0.03406
24	0.03318
25	0.03414



Розшифрування тексту за варіантом 13:

Довжина ключа – 17 символів. Ключ – родинабезразличия

№ блоку	Найчастіша літера	Частота літери
1	о	0.1238095
2	е	0.1142857
3	е	0.1015873
4	о	0.1238095
5	о	0.1269841
6	а	0.1111111
7	а	0.1079365
8	о	0.1238095
9	о	0.1142857
10	о	0.1015873
11	о	0.1111111
12	о	0.0920635
13	о	0.1015873
14	а	0.1019108
15	о	0.1273885
16	е	0.1050955
17	о	0.1146497

Зашифрований текст:

ншхтнвбчхапчупьфзбаясхдмнфэырьуекмюайчшогуобдзцнбцблыйщтноурбушэищяявьнъмгпопзулщкябмлъльюауауъойгцглтбусргыдръсосщкгрмрщмщйвруютухьъчккпниктнжфчхрвнхтнпхпфрютьклюрхстяшячнэнтспржаорцзюляюзйнынпфмалхшнзижсцфимдпххуипоцйцбюпяуысппчгшпэдщщдзоххыенфъвихщцоыгшзйлтнжхзьіпчушещйьухъанжзшшлзачеадтупряьтдмблпиъетнэафцшьоарбючъшяпсюрйщтмйххзчмшдщгрюштлыювшлгщмчкьмыьоонщнжтппацщъефрвюдэхзбсмиащруущстьсныжййзэнхьэвгмгщмцютбрхбьщщуутнбэттыйтчйшепоукйнъогыпескфэошэдзижгъжнсьнесрпъъъумяцумхнчйтзощмоцщщдаожхыгйжюхиижщйшдхаччихйтшвифхъекгшштсщащнфлпхмнырсмпйщвиуххбтфюжгцшмътоъойжмчочюоязнфытсшищбшшлхффтщкшуухзоемиьслтънмхюдуфнбрцюкззцвдйюрцнырйнфювмпдщъньцхцютпнщбмвьубцмвютуйньъцюлмнгмпяфосрцврхптяохнйннаучрдетппезфлхясйаудуйнпохссщлхекйхьихывскухнфщфьуыъыучншбргэажукыимэйнфымжтщьатщыгнрвыдзщытрпикзнцйпязурыютсупыипьчтъяэцйкьутчхьифрхчщдыусхымречъещлтесъъяоипауучэакщшемръцщышичеьбтхцдбцалрхнроручгшпцпчмдбнцдшеутмютчщщвцалццичинкмвсжхизддаыясруткфшчфжсфтръожияоссхфетуфемдыцдятрукккюзфлнйтяъьнфыджрпьнхоцйцмэогумздеейажошефяфцсиьогцмщвппргцрвцтщъаъкфрбхыъекъъштфьыячмаоуькеплюфсцютэгъфатрхдцвютттщяурепфишэидюзюысцроффчрвтрхязоюрхнцвййпьошэрщгчыомпьоепхэтчщуцртбэйуннбчйюрпэдврфшгиншвптдыыыннидньютknвмкфэырнивздвягтютбчпярмэъецмрэфзщооедыыылхчмнюажутчэимэечлужшдъюдщъоитзыстлйенлхяццяалньыеьлхяплюрсньогучюттукещсмэтуфаячщркюэцонкюрйтъатзхшхлнцяэнсстхxтрудвоуюцдщнардуюятсмбтзшишнвгятмввбчпысцщыищгчьыцххкйфъыыьщьръимгщынэеитмъсщлъячнфрйшъугэпщсжхыиъзюпйонлюпшъайлъешрыужияоуццрзътигнгыцпщмигйчгрцыцщцпэьжгърпцщрлцщукщнуыччыйеуешхлмхцщареючщяонфмаетщфяунбкрцшоеумфечрккннрыьжхысрнюъакрхьшяыбхчтлгуйаеукышшявкхзъавкоюпзьхенпряхъыяонмзулщкябдаолкырбьптатщщулнвьжцтрйтъвьшкхччппечбтгпцжтпхпуьщйхрймймбьхэкзонднпрщснатсещшльцыыхнъюткхяоецаощукехтцууышсшнщрлсюмчфдвыйъюяткрзашнцекгстдпнодххьнвфщйцкхасрцдфжйэешхцвдйюьеэпаууйгнмоцжцгшадтхелучэиюэцяейбшдкнтпхъбхxпыднртьфцяиубншзфзцдиббузмнсйргэемснвнжрцрцяосуйшвлыыъыъвхыйшнлбфхпвпцщцхдцтдхъыкцхозфутгнкмшсышатхмфийръщнишяцкылпзсюрпвхькнчупнъаапъатхвтчрмхриишелкцюкзтивщюхзйцсиовтмфхпнйцмсйпъычоущрknртчтзэуиипнйоцрцпрхйлдэуфишаоуйюттуяяннвэйшподуцаеижкчубяпхыимйчрвпурицфаосхысуннптдчюлклдэуфишаружтитьзднефосхийтуечнпхфьуыъыучунсскшвмэкьсзбажцшогпхаиюшнщцжхщйхнялшчвоюхияхдттдуткжфхъаолуиздйутмхнюргдолръехалщццднпчзъжмхибрмхтдкъикфзжимшъънмхюдуннпзхвлпврьцсяуфкыгпфчхбвнивкоюцсцщзехзтипущеэпрысцютйфъыьщюъыйюъюмтъумуфуефршчутууснэамсхыч3ъцбижрщйфачжхфлйфляяхдэыясклжпщаофутесаацонаялрезтмъннздвхыйшнлтчхыьнрктшячцншьоуцюхтщччурхпгчыкбхурнъхыз3йшлпдбсмуйэоцщмюнлымушывбрпысжыииъбююмуюяоеыюнмцриъблоуцяонзхчнпхыэнрюрхнщраййхьвцлшьаяуьжкислутмзфюуяпжряцкылбчхуошлфелнфбеикктпзтащщшъшньйщишгфцмэиэлфярмрачоъомдоуатхцщаньэфцоисежбъшхкепыяофтсескймянлуеймюафнжамнпыоулуящыаькмнлбцгэойлзжшнбуоиклэщщаеищкчъдыксцьрпчжэутыыбызуусняамтмъотрйвзрмьцмнлжсъяутзъиткоетфщеерпвьдцдлхдбьерэамцжвущснщщсррмучляьйхдйлчзрлхасылщжргэащщшнногщаънрбмлрлшкхьлпюъорцщжрююкмцниуъыыясъахуфхпчщрюкнфцрцроюпшъайлъешньжчфнпбргжыдцдлижрэтшвамнфрдсцищрябфццпфргвийъшцфыюейхйппъхфитшидцтвпчтютпотшшгыиюхзжуняяоюпчрнъшнъцалщхцпсжссаоьщъдгишюдщьомекрлшкхьхяюаорснпосаыяхнччпптшмдпсшълзнрпилшшфгекйцхссщнндхншыййилпзхтсмщъщудъцйлывмешвнхьтефяэттknлюргдиирпюктзыттннфрйъушэгоънвьчхтгпзпфиущхьуяфцпцюьдкфхрзцчещкгжсцьоухъбитъцпрпюштсэаисзиишэцамтуубтюкбззвочшибийюуццпржсжярпэрмцсбщйохвбдмуоцюршьфдйусрмарущюмшэивлпгхсцэаизхааюукчъыбнуцсгфцмэиэлфяпяещвчнлпуфтъмаивкнсжмшъуяущюрхвндхтоъщцщлфлъуефршчуоющапаятбуюммшъефчьйзхалнуфбтчюпчтнаъчхнрбмйюрхэыйцвюбнмттеуйюлгшцгхнуьжштмжтпбрзнхяъдыксцоыtччюгмшнзикюахъапйрсюбяушдциюрдуйнпоцюлжшнжщцхъчъыеншиллхсивтнуцехащйкцюдкюцьхзжоррхкпзяюмлршькыпроцъцжпхэцхнччшйшадтнязкюрсщзлешнфооичилззатзцгчкдфкричовдорныыидрсмстшыдгкшмцмцрбцлрэтумнффъбтгюъхозвэтмамбрхэтчлкчхдфуфнпожюмтэщщфъцггьцшнсукщэеъьчьулюыхъэвьфхызщутжцкпыончалущъуллъещаюшччыкбмзыснжпищнчэцнешьхсмыкхфкяэкпмэнцрьцэюйхшчзраыцлршсапкхнмыивыоыьщцсемушюоидрвекмвтхфаврхъичщкчуббужэыдоамяочэгдигющйпяьгпзсифюльхдаопксуньптоячгъхтыыттщымйтпзекщхьщйрхдусайьщюофчцъщйрхдъйауашюбшэкьхмюшццьойтщхрмьцщикбнбуйфгклммзхяйцкшыдяхнбгашйъэцохзысйхтрбгшърхчхетяъьнкихпйцхрйжсднрвопкэаубкхнмыивекмвхиэкбцщшчмьтяэзецохалгкохтнрфднбяютятмшккюэщщзяхяэуушхшмушмбвнцырмюеоычсуещшчщщщзимррйхырпсдвощнцачпшнцншьоейбясусиутзонщьрбзпысжонднпрщоцяосаряутзъжцсхюгусабчвэейумьукхфмъэяеуубатцнъсахххцфнбтппуфрлекдбкецчрбмхфрзшзьлнрлфцфомкубпчжщдыктоьрщэмбыэаьчыэркбниипетеурэйжшкляыягешьхуфьонръдн6лтйшуаубщторъшязсхщаыщисетъокпицхяэузцъаупфгллшкывгаэуцщмсфйгсайжоякдвячмйббхмкхюутйяхахзкзлэщзьвмпдгнмлжлиьонтпнтхонднпрщхфылшетыалшциутионфтнатъцнхтиыыпшааеяоксзеифрнъцоюсдхиеоейшгзбрехмлуфнгерчхаыпъцжирвкжтнбйтъвыушнжцлюфйайрбмъцвйкпчурпрбъыджрхсоеьдйилтшдйхнжулэоръизгпгшеысеусзыоцщмьшдткгфшаиещмуурнпдтьувчышмндыыытйтмгщенюппрмчнвфчетяяблдязбфхпсяэидцбштйуывйчхчаяллчуйгфйкибсейиеующцхяъпзъуюпшъайлъешюажуткбоцюкзшижцлэцпцъппжмуарюхьлняуфнсмпхлюйщщуутнбътъэирулъойгхъыьютмырувшчънъцлъхдаопткнкунэоирпзижыцыхтевккртгънзнгьъфмыйюпшъайлъешяюшдпнлпцгэашэцвдйюфйыяонншцхлгшгпяэнцртмтпхыьпшншнжюэдщъыънфмавхроьпясузиъижклтафрпчтнэемуысэччргпвнитзььсщярскоъойжчззлшщуцшутукэущжсбцбиьихыьскухнфщчемятжмщйврккчхдптиынкящйяыгжтмаатлъеъйгпдштмрутхтмцкйшятбхцпесэмэнхщачшяиусхийжюмтпзпндрзбьтйэаинйзтхъшямдвягфылонмэошшцщщйршмкнтэтмтзпыицхясьпдхувнчртгъзгнсаьжхндгелжащзкиънаьсыюопжчрзпццдчпррмуйнпцлтуьънбымфытсфаекчцкхфкгнрвьзмтоофчшзмчуяурпрундауетбясщкпчнеькрцнбипуафэщбрицупнфньосглзх

Розшифрований текст:

экскаваторприземистыйидлинныйсловнотепловозсдалековынесеннойсуставчатойтягойичудовищнымзубатымковшомгусеницыглубоковминались в почвуоставлядвенепрерывныеребристыедорожкиразящеесоляройлязгающееоноперлонеразбираядорогиготовобылосокрушить всенасвоемпутионочудищегенералприроскместуневсилахпошевелитьсяеслиэтоконтрольныйсюрпризтовесемирочньвысокогообудущемведьмакемненияапотомстрахизамешательствонеожиданносхлынулиосталось толькоспокойствиеиглубокаяуверенностьразумведьмакапустьдажеиначинающеговсеравногибчеибыстреетупыхинстинктовдикоймашиныпобедитьбесхитростнуюмощьможноибезоружияоднойлишьсилоймыслиеслизнаешькакгенералзналпокатольковтеориионведьвтомисостоитсмыслконтрольныхполевыхзаданийвпривязкетеоретическихзнанийкреальнойобстановкеодновременномелькнулашальнаяивданныймоментмалоуместнаямыслишкавотзачемустроилииспытаниевпустоминеселенномпаркетакойэкскаваторнагородскихулицахстольк обывсегопорушилзадесятьлетнеотрослобыитакимеетсякарьерныйгусеничныйэкскаватормоделимоделиачертегознаеткакоймоделимноготонн аялязгающаягромадинаповсей видимостиоснащенабортовымкомпьютеромсвозможностьюудаленногодоступаидистанционногоуправленияповсейвидимостивышлаизподконтроляи успеланатворитьлихихдел вонэльфвесьокровавленныйваляетсякстатипреттоонапрямонаэльфанадоотвлечьгенералпрекраснознаялсабоеместотакихмеханизмовнепоротливостьползаюттакчточелобекнасвоихдвоихобгонитпоэтомуонсорвалсясместанабегуподхватилстравышмотникипультсиганулчерезнекстатиподвернувшийсякустиобежалэкскаваторслеватотсразузамед

лилсяивдругпроворновыпросталполусогнутыйдоселековшсхрустомпереломилосьмолодоедеревцесловноспичкагенералуспелвовремяубратьсянабезопасноерасстояниечудо
вищеразворачивалосьготовоеринутьсянапрячущегосявподлескеведьмачонкагенералнеутратилхладнокровиянапротивонужепросчиталкудаметнетсясейчасвоонтудазаогромн
ыйстолетнийдубвнесколькообхватовунегоподитакиекорничтоиэкскаваторусходунесворотитьжизньонавсегдасильнеежелезаимоторовивдругугенералапоявилсянежданныйс
оюзникмелькнуласредиветвейистволовкоричневозеленаякурточкаиневдалекепоказалсяещеодинэльфодетонбылточнотакжекакинедавнийпациентгенералановотличиеотпер
вогопребывалвполномздравииисохранностиивдругугенералапоявилсянежданныйсоюзникмелькнуласредиветвейистволовкоричневозеленаякурточкаиневдалекепоказалсяе
щеодинэльфодетонбылточнотакжекакинедавнийпациентгенералановотличиеотпервогопребывалвполномздравииисохранностипультутебякрикнулонгенералугенералмолча
показалемучерныйначиненныйэлектроникойбрикетаключтеперьгенералстольжевыразительнопохлопалсебяпокарманукурткиэльфсловноподземлюпровалилсярастворилсян
афонелиствыапотомвозникужесовсемрядомвпарешаговыскользнулиззастволатогосамогодубаэкскаваторгромыхалгусеницамиинатужнолязгалковшомпробираясьсквозьпар
кдеревьяжалобнотрещалииломалисьрождаласьноваяпросекаэльфтребовательнопротянулрукуигенералнеколеблясьотдалемупультсключоммедлитьэльфнесобиралсятутжев
ставилключведвариметнующельнаторцепультараздалсянегромкийщелчокелеслышныйнафонепроизводимогоэкскаваторомшумапальцыэльфазапорхалинадклавиатуройпул
ьтивпрямьоченьпоходилнаоутбукстойлишьразницейчтоэкранунегобылсовсемкрохотныйирасполагалсяненаоткиднойкрышкеапряморядомсклавишамикрышкисобственнои
небыловоовсеотвлекиеговластноскомандовалэльфибеззвучноканулвкустычтотоуневидимоневладилосьгенералпослушнопотрусилпоширокойраз машистойдугеэкскаваторнак
акоетовремяпритихотслеживаяегоперемещенияапотомсталгрузноразворачиватьсяподгусеницамизахлюпалоонвъехалвобширнуюороченнуюомхомлужугенералпользуясьм
оментомшмыгнулмонструзакормунаразворотутогоуйдетдовольномноговременисравнительнобыстрогенералотступилкобширнойовальнойполянепочемутоемубыложалкоги
бнущиеподгусеницамииковшомдеревьявконцеконцовпаркитакаяжечастьгородакакикварталыаведьмакобязанхранитьгородвесьцеликомаполянупустьутюжитподумалонтрав
анедеревоещевэтомгодуотрастетнеуспелмонстрвыползтикполянкекакоткудатосбокупоказалсядавешнийэльфмелкойвихляющейрысцойонприблизилсякгенералуплоходелос
ообщилэльфонзаблокировалвсевходныеепортынадолезтьвкабинугенералвдумчивошмыгнулносоминичегонесказалдаичтоонмогсказатьатысобственноктопоинтересовалсяэль
фведьмакчтолиначинающийуточнилгенералскромнокакойвыходпервыйнесталвратьгенералэльфсаркастическихихикнулвезетжемневпрочемчегоэтояиначепришлосьбыводин
очкукстатичтосранавеноромэтотвойприятельнавсякийслучайсправилсягенералкоторыйпультпотерялдаатыневиделлежитрядомсаллеейбезсознанияуневовесьбокразодраняе
гоаэрозолемспрыснулвашимэльфнахмурилсядавесамаэвыругалсяэльфонможетневыдержатьтвойприятельумиралкогдаянанегонаткнулсяулыбнетсясудьбавыживетсудьбаред
коулыбаетсяэльфамведьменышзапомниэтогенералсмолчалладнослушайменянужнозадуритьэтоймахинеегопоганыенавигационныерецепторыипопастьвкабинутымнепоможешьразужввязалсявэтоделобоюсьтамвкабинеоднойпарырукбудетмалоподеревьямлазатьумеешьумеюпошлиэльфзаткнулбесполезныйпокапультзапоясштановиделовитозашагалкужевыбравшемусянаполяныэкскаваторуотвлекайпоканапомнилонпобегайунегопередмордойтолькосмотриподковшнеугодиугубуркнулгенералкакможнобезразличнееб
егатьпередмордойэкскаватораоказалосьнастолькожеутомительнымзанятиемскольинебезопаснымпервоежезабеганиеедванезакончилосьтрагическимонстррезковыпрямилп
олусогнутыйковшодновременноподавшисьвпередизаделплечогенералатоткубаремполетелвтравусовершенноошарашенныйещевпадениисообразивчтопридетсямолниеносн
овскакиватьневзираянабольиубиратьсяметровнадвадцатьвсторонусообразилонправильносдвухсекундной задержкойвместогдеонприземлилсяв печаталсяковшпохожийнагигантскийжелезныйкулак

Код:

```
#include <Windows.h>
#include <iostream>
#include <iomanip>
#include <fstream>
#include <filesystem>
#include <boost/algorithm/string.hpp>

// alphabet
std::string rus_alpha = "абвгдежзийклмнопрстуфхцчшщъыьэюя";
//

// functions
std::wstring toUNICODE(void*, int64_t);
std::string to1251(std::wstring);
std::string clear_the_text(std::string);
double calc_index(std::string);
std::string DecryptEncryptVeginer(std::string, std::string, bool);
std::string AttackVigener(std::string, bool);
std::string AttackCezar(std::string, bool);
//

int main()
{
	// setting console output to 1251 (russian ascii)
	SetConsoleCP(1251);
	SetConsoleOutputCP(1251);
	//

	// gathering info what to do
	std::cout << "Выберите что вы хотите сделать:\n1 - Зашифровать текст (Только UTF-8)\n2 - Расшифровать текст (Только Windows-1251)\n3 - Атака на шифр Виженера (Только Windows-1251)\nВведите значение: ";
	std::string action;
	std::cin >> action;
	std::string key;
	bool small_text = false;
	if (action != "3")
	{
		std::cout << "Введите ключ: ";
		std::cin >> key;
	}
	else
	{
		std::string answer;
		std::cout << "Большой текст (1 - да, 0 - нет): ";
		std::cin >> answer;
		if (answer == "0")
		{
			small_text = true;
		}
	}
```

```
std::string clear_the_text(std::string data)
{
	std::string data_ptr;

	for (int i = 0; i < data.length(); i++)
	{
		if (data[i] >= 'a' && data[i] <= 'я' || data[i] >= 'A' && data[i] <= 'Я')
		{
			data_ptr += data[i];
		}
	}

	boost::to_lower(data_ptr, std::locale(".1251"));
	boost::replace_all(data_ptr, "ё", "е");

	return data_ptr;
}

int get_occurrences(std::string data, char keyword)
{
	return std::count(data.begin(), data.end(), keyword);
}

double calc_index(std::string data)
{
	double index = 0;
	double data_length = data.length();
	for (int i = 0; i < 32; i++)
	{
		double count = get_occurrences(data, rus_alpha[i]);
		index += (count*(count-1)) / (data_length*(data_length-1));
	}
	return index;
}

std::string AttackVigener(std::string encrypted_data, bool small_text)
{
	std::cout << "Атакуем Виженера..." << std::endl;
	std::cout << "Ищем длину ключа..." << std::endl;

	int key_length = 0;
	for (int r = 2; r < 30; r++)
	{
		std::string block;
		for (int i = 0; i < encrypted_data.length(); i += r)
		{
			block += encrypted_data.substr(i, 1);
		}
		double index = calc_index(block);
```

```
		std::cout << "Введите название файла: ";
		std::string file_name;
		std::cin >> file_name;
		//

		// reading the file
		int64_t file_size =
std::experimental::filesystem::file_size(file_name);
		char* file_data = (char*)malloc(file_size + 1);
		ZeroMemory(file_data, file_size + 1);
		FILE * file_ptr = NULL;
		fopen_s(&file_ptr, file_name.c_str(), "rb");
		fread(file_data, 1, file_size, file_ptr);
		fclose(file_ptr);
		//

		// processing the file
		if (action == "1")
		{
			// encrypting data using key
			std::wstring dataw = toUNICODE(file_data, file_size);
			std::string data_string = to1251(dataw);

			data_string = clear_the_text(data_string);
			std::ofstream cleared_text("cleared.txt");
			cleared_text << data_string;
			cleared_text.close();

			std::cout << data_string << std::endl;

			std::string encrypted_data =
DecryptEncryptVeginer(data_string, key, true);
			std::ofstream encrypted_file("encrypted.txt");
			encrypted_file << encrypted_data;
			encrypted_file.close();

			std::cout << encrypted_data << std::endl;
			std::cout << "Индекс соответственности открытого
текста равен: " << std::fixed << std::setprecision(7) << calc_index(data_string)
<< std::endl;
			std::cout << "Индекс соответственности
зашифрованного текста равен: " << std::fixed << std::setprecision(7) <<
calc_index(encrypted_data) << std::endl;
			//
		}
		else if (action == "2")
		{
			// decrypting data using key
			std::string data_string(file_data);
			data_string = clear_the_text(data_string);

			std::string decrypted_data =
DecryptEncryptVeginer(data_string, key, false);
			std::ofstream decrypted_file("decrypted.txt");
			decrypted_file << decrypted_data;
			decrypted_file.close();

			std::cout << decrypted_data << std::endl;
			//
		}
		else if (action == "3")
		{
			// attacking Vigener
			std::string data_string(file_data);
			data_string = clear_the_text(data_string);
			std::cout << "Ключ: " << AttackVigener(data_string,
small_text) << std::endl;
			//
		}
		//

		system("pause");
		return true;
}

char encryptFunction(char a, char b)
{
		int apos = rus_alpha.find(a);
		int bpos = rus_alpha.find(b);
		int result = apos + bpos;
		if (result > 31)
		{
			result -= 32;
		}
		return rus_alpha[result];
```

```
			std::cout << "Индекс соответствия для длины
ключа " << r << ": " << std::fixed << std::setprecision(7) << index << std::endl;

			if (index >= 0.05)
			{
				std::cout << "Длина ключа равна " << r
<< std::endl;
				key_length = r;
			}
		}

		std::cout << "Разбиваем текст на блоки..." << std::endl;

		std::string* quadrupleblocks = new std::string[key_length];

		for (int i = 0, j = 0; i < encrypted_data.length(); i++)
		{
			if (j == key_length)
			{
				j = 0;
			}
			quadrupleblocks[j++] += encrypted_data.substr(i, 1);
		}

		std::cout << "Атакуем Цезаря для каждого блока..." <<
std::endl;

		std::string key;

		for (int i = 0; i < key_length; i++)
		{
			key += AttackCezar(quadrupleblocks[i], small_text);
		}

		return key;
}

std::string AttackCezar(std::string data, bool small_text)
{
		char most_alpha;

		for (int i = 0, counter = 0; i < 32; i++)
		{
			int occur = get_occurrences(data, rus_alpha[i]);
			if (occur > counter)
			{
				most_alpha = rus_alpha[i];
				counter = occur;
			}
		}

		std::string subkey;

		if (small_text)
		{
			subkey += "[";
			subkey += decryptFunction(most_alpha, 'o');
			subkey += decryptFunction(most_alpha, 'a');
			subkey += decryptFunction(most_alpha, 'e');
			subkey += decryptFunction(most_alpha, 'и');
			subkey += "]";
		}
		else
		{
			subkey += decryptFunction(most_alpha, 'o');
		}

		return subkey;
}

std::wstring toUNICODE(void* buffer, int64_t buffer_size)
{
		int64_t unicode_buffer_size = MultiByteToWideChar(CP_UTF8, 0,
(LPCCH)buffer, buffer_size, 0, 0) * sizeof(wchar_t) + 2;

		wchar_t* unicode_data_ptr =
(wchar_t*)malloc(unicode_buffer_size);
		ZeroMemory(unicode_data_ptr, unicode_buffer_size);

		MultiByteToWideChar(CP_UTF8, 0, (LPCCH)buffer, buffer_size,
unicode_data_ptr, unicode_buffer_size);

		std::wstring unicode_wstring(unicode_data_ptr);

		return unicode_wstring;
```

```
}

char decryptFunction(char a, char b)
{
	int apos = rus_alpha.find(a);
	int bpos = rus_alpha.find(b);
	int result = apos - bpos;
	if (result < 0)
	{
		result += 32;
	}
	return rus_alpha[result];
}

std::string DecryptEncryptVeginer(std::string data, std::string key, bool
isencrypt_mode)
{
	std::string final_data;
	int key_length = key.length();

	for (int i = 0; i < data.length(); i += key_length)
	{
		std::string small_data = data.substr(i, key_length);
		for (int j = 0; j < small_data.length(); j++)
		{
			if (isencrypt_mode)
			{
				final_data +=
encryptFunction(small_data[j], key[j]);
			}
			else
			{
				final_data +=
decryptFunction(small_data[j], key[j]);
			}
		}
	}

	return final_data;
}
```

```
}

std::string to1251(std::wstring unicode_data)
{
	int64_t mb_buffer_size = WideCharToMultiByte(1251, 0,
unicode_data.c_str(), unicode_data.length(), 0, 0, 0, 0) + 1;

	char* mb_data_ptr = (char*)malloc(mb_buffer_size);
	ZeroMemory(mb_data_ptr, mb_buffer_size);

	WideCharToMultiByte(1251, 0, unicode_data.c_str(),
unicode_data.length(), mb_data_ptr, mb_buffer_size, 0, 0);

	std::string mb_string(mb_data_ptr);

	return mb_string;
}
```

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.