Міністерство освіти і науки України Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Лабораторна робота

із Криптографії №2 Криптоаналіз шифру Віженера

Викон	али:
Христиченко Дмитро ФЕ	5 - 72
Нестеров Назар ФІ	5 - 72
Перевірено	

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

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).

Індекси відповідності

Відкритий текст	0.0549039
K = 2	0.0414622
K = 3	0.0423839
K = 4	0.0356621
K = 5	0.0345404
K = 12	0.0326629

Аналізуючи дану таблицю можна дійти висновку, що при збільшенні довжини ключа індекс стає більш віддаленим від значення індексу відповідності відкритого тексту, і навпаки, при малії довжині ключа значення індексу наближається до індексу відкритого тексту.

Шифрований текст:

деьооуцмдурьдыегныьпуыккэаонтцчхлуучктвдджоаубуяцбхкугбэщешряцзывтшщяшхтяяуюйлрънпрйбдшзъняъмйнуьряпьщгт уьзразхтпфгяжитхчьурвттдфанвзгьячрщюитобущузсшзпуыхнмвбуьняэаоемйнеорцбэзмюцйхлыпейжцбышяпщчсущкдбкалтоз ьевефямнумвеаыяпцезьуотпъяуччтшкъуньдцплчжурпэнямноннщтвддщоюнгкшцкуьщшдднтютэнцьмухрчбвщгртчпщыупшоы уфщгхнжхуучехфщвчыыэееъщахььрхобщглэччзекцьэахатггъесюекчпнрщчозьтчмуцгшъмьаьлефуьрраришужыэюваелунэкззф вьюррвтецэцжемпвжшралризщцоьпнвхчхньтьцьоннтдфаъняэаозжярптлйжцщшрэтоьавхтмечэумэагнюявстуьччцрэезшсцхзяр шуъхтанвчыбгпэзчбаьбхючрлщхткгзгьумыкэецрпшьтьатьдэкякоьпклэябфугэущфщазсфвйгтьръеюаноннъвыанрзбчехуцокржз выщишсъуньтнхквеачцвуэкшоучктвдджлрззесупютпфъцщпюзчдуызиххгусннтцхцньалтйбпяувфкдкмйнеовяпкрртуьищюрйчр чбгркртяпщсжечзцыцркртяищюрйкпьщчцдчтеопьтункфхбщрыкытуужкыбжпэрстцьцутзркйфвчвыонйуцкмущрббйллтамупцн ечвзюъбтзчелрахчэжьхъэдыбдуоьупкйфюуюпъндрйтзошжьаахзефетлаххпмвеаыъхпчпыомуьъщюнгйшряшццфпкужувлэвццш факзыдвегхнаркфюыввьрадфрехтьелщржефряасдвчкчкрнкчкщудлбшмгеньйзьвншяудъчесюрткцзбыьщвфежхртрпбзябфрйрть жжщзюпрхмчьсткдтжъинмржанчзцнвупцпуфрцдфщдщжьхцьекковщчэалчувэьсхшужбапмрнюхлхпумкшааьсхоокцьдкбзеэаон еезехазхкмжбщшяхчцтруучпужхчшмшпятръркозябьлррчуцкэрйшгбознняхецщрбчшнрэаанзшиплхвчжщжбдлйшквгпцмефофх влютрьтуупкъзшэаргрзечшужехзюбъьйрчусрябыкжцуялжрйксрюхткуццаынфкдкхцлжпньэантзнйкцкехпщшдыщвюдюахооуу фвхтызйэтушуоцхэмуэуйютьышьртлэяьтчдзейкцупчполеанрхиыепоикмрлшязфюхеэюмсунршжфжфюйярншвршъфиъьжютйн хьончзггччдэтезэусршогуэзсютчзлазнсрбеьхтэкъумйнзбзйючуцрцтзвучрпкыдчынщмчсгцкпшешуфжмшсчръутубкбанфмюлоч щпэубкбыдзйрхчтпоъчшкббшюмхиежжщдыпчвюовзъкярудрпкйфюаьывуэкмйнумщщиэрсрпбехьпзызцгччюяхцчлщзишдгбцш юваазщюрччкюбяшибивчръпапрлэъятдеапюбънсвюютпътевзларотмвицлррйярьнпетицбщвзъейуъюкпкипхтцоюйдичофбмзди

апмшсирщррсэяжбхщцхрезршвткгясцлкюцуфщяфуйпббчумхфзкщтрртовшгэпхсвкшцзуфтзщъэыбкшдщпрршщюбыьнчйччзяз жпффэгхячейбябфрйтюбдщплоккпцпнхгпшхщжрюячущгашфцачгмшъщрунпнужщьгэбшчьрзырцьюдущппрлчрлуеущхчуэлгх хэецодфшужбсшмюойхрррипкходзлюльчпщбчшевкдщалужхлржеьюсееьбюгзумьучжуцбчщстхчюрыккфпфддщюйкгшщыдцп ешузняынвфыьършзьеавдууднхьейкпщфнцншйзкныккййпэъхнвузарьпфъзгбцлбрршаццжрйпщцанргюдуьакчпищэтцнинямщы фнфмзчтщмяхцчлщудшфшшыьстнйкцкпууиьъяунъебмнбщкчмфэбыдъхчцрыехпщщдьуипмтпоьдуъкябяьнбрчйхцозетфщчшзх сяплшгамжвэттявквбьадуыдвызькюзжхузххтдчюттзяуыткрсехзкввщзчтецущвтьтвваьзьаирзядуигщюъхнтччпсуучктфюгкжрф здэофбмцзеэкпфрцтрсрженьтгшъвувбхьшнъмзюсыъшичмрапапужудзэтпечщюэъсвггчдяыуибварттгзчохнуйчзбцтпэнугчтяяхь юлщрцжхлшяуйрсщааьжньюбуецзжшжуьщзйпдусъвябущзрезхккяыфхяъуатупхйжужудздчежхрзвркурвэщебпчдцмгумюжбпэ нсавупщбтпевтгшнюфзкпункчпвътъпхюьтщцгеыффхвлжакпкшцклпкгбщнныкднуямхедфюгкгыддкоьдцпешупцдькдчььоттфщ юошъщьйуэьпкореэттяэтекуяошьпвшьщвфещищюрйптфъврчрряйыооеьклшгхзщпзшсьмнхклыдлкмтхнццщеупзсдщнэфеплек зкнчбэщбюояищррхтнжызщнэубушущтшффэдщсрпщцрлфущтщэвлрэуыехомжещщцашдтапрщрудфрчбвщгртчхюжзттбзээщм хтядщаучэсяшяуюючжхлркрщтьхапзыньищрхтепьшзщеппчмлщрцжгпэтхнхкгшпунупуяыьэншмйунотнгзэбблжфащецывсшн щфчшзыныу аьжих кеюе азю пчп щчпн лхшпбын ъею коцоткй ь дд щбшря зут зртмя угьм ггыеч б сусжббфрцхх есьь ц наздбю эню те ьры юзшнббфлкбдязьуеумрдыэхяъжтьрертпдплэщяэежкпоеунклшгхзецезравъшпггаьсюшътраврчведфщдоуичщюрлчрееойлэнйкц кпуыфрсъьбюнгнвцучшцзеэкпэагнььржъвъшяуюьндеьезчьрчбйэнтуййррошруюбыуехтипщченцпфъъкфьувупуибмзшшдьдсд ышыырубзбпкюлшчщпцоуцкчфиьлйсадкпьършжватвяыбичновъфвюфнвдуудкнйършклеаррыншнтрфуърчбьцябцчньшнгбкжп брсаущелцйьпфишвэнууьищюрзкфвфнинсаеьрыюъштвлауцвуэкьррникцъцщфрсятжаюкцуибъчзвкгтжъкубмфяъшясрьйшьоск нщаохньряырхпепфщятцдэббучщкыпмфэеанаббещыжемкяатьббкмнчйхцьхгуэурсещркщкфпфдбфюзхиехщрхжкняваънткыкш цацкифюъуфяуыеыуучтдюбябдъудыщркцфнтктцзшфьчыьдетзчбвщбржтрщбпкнреевлмэуьумймтшдщаърфюйячзэрткъьяьняач яхлъсхтжщеьюцшчьрйябйпфьяаццшчяплшгшофвкдщсюзтцчофхтдфшдънбнынэлфефовюйлцрцыхюсротхэччэьвудетйдехрепе шдуужуптзхркцудзгюжзарьфтшъщаъкрвущеыцыецкьбйрбшйдуаьжньююатчзбныкэкгахршюсшдууйдсунутчвчъцнэпдечарржм вваэньшочщящньвядфщдочезлюкюпуюбрщапмчтшьучжааоевзвквдмьбртуршхщзфеэкпцткффвгущюыццзщасуокжшшрмрэяш вцфкхббувщгтцьсжяндгкэцэюаюпефщюбйшщбоыннбфячлыпаупфееывхтьзрцыкотьачщгэебусуячшфлшэщбхььпаьжнмъььфьд уйчзхонуввйыгтнэчяпщъжкъифюфытъемзьменцпфъъйххртъънфткжкудзкхчыеваритобущуэткибоьтуопфлъпяьажуьбгжшффяц щлрэднаяскфффээриэккцэювнмвяыущюынибхомжербачюжэевнпбчумзбддннбчьцшннуыюгтъшдьпкэлаюцфрдбюшнхняиыоф бммфгджоюйщрунпнпожуьуфыгыкфшвплзяыьщбчежуьщзйчкщччьювбждэывйавжпэрсттчэръеуършшгэяыншукаюцйдешхща юдйцкстуцмвцаннанйбъьуахвжпбурмсчмшомуцкжпгкцшчччзшпннкхбсэрпфесщсвчжгщчяжлгьячзстецржшъняэнщешйщлпнф тйэнвуиплхвчжмфлэкмгрдуьывькнфътхтанвчыбгпэсвцэкгхрдецбпштсвеачтцкиплхврытфдгэяэущпщчжецэеюсдзхфехктрьчэщ къэяочяюрттнчвьееывхтьзлювмчэйетчаюпвкфцехшщщштннвфейвцпнхкепшрсххжкццфуьрцбдщмюньцэкгкхкюбфсзызйучфзй шощцирзпфзупьнлкнхжвхзэзйучфзвьвъшцндабжхщакзодщгъчъзеичщркйпньдоуючтчррсрйшофляйэцнютзцжуцвжушрзбчеху нчехвжэацорпичлрпнсвшхъсйшыьржчтдодетьуфчежхрззттлвцвлмшььтучкеямфэужцхиетррээхргбгэмюкьцэкдхпжббтьйюхесш ьзтпнръсэяъпчпъьиеххэдьлегчочщпзртмвхярзбфершнзчщрееанзютьрьбжефвбуьщпюзукчъвцхзгыллмхфецэывдчрьачцычдипл хвчжщжбужръузучывдрзбдьщияхяццбеншпбшцрпцевнтяфхкчфкдщалудкчызйэофюъптатеепутлкнгбфлпрелешоунйужувуйрр ьчгуучтжицдеэзэкйхрхдунрьвацнгедуоьмуьрдоыхнуйччцияншркяхцрмйнбеацхспнюбчхяъцйхкэвчжяжбдлуртчцучучшбябужйэ ущкшыршодщгъьйакичуртшфкьхгрвфешуыърчкнвчящзвуэкьсншлрюыюнжфумучъпунрзщъамлтокыойзпнвдоьорруткбгкхкю бфлалрчслщзтжмфтдщцэуцюушмхшдфеомъыеифщщришоябшлрмцжеэкртэмдофлкбдиищщрзшлхоэщерхбупбътшдыуьыъваь йнутныфзктцрпзьчрюдфпщюшхюгхреццйъехкепфтгюъянтшхъчкцъцщфшмвунуынпкщяемъыуичыоътшсвчапдпресщыгуйнеть лисаокоыпкмэмюахяъжткоыпксвдшщлкрщчтлякофвюфншдчешхлщкцждвгнуоючесняатшщрхъпдычзкныитезеанлтвхесхьейкоп хюррвкпруренцпфъъйалрипюезтлнщччшзсавунцжтшщжбюшнуувгпывднкааттзпзбуэьтширблчцалрчцэювэчвггаэзттчзьуошых ншгэбгкъууефутжжывкгюсиучыропозкчцнткбшъьпеьхдшапзэубучбгахржтшхнюььтзбиээоуеешябзбрляуеяевхаызыудплшгаы ффгткрмуйаьшвчжрхнсьмхтядьрркцхжтшркюскьюручмхбыялцвудкъьчурзьрдщсгьячрщюиъзлшгхнууцмжшввьржкчцнткбзяб фрйтщяасдвкикмусхпжеетнзвбьйнопкрзбыэьюшзчтурвтещхогэпюуъркыхрыбцдтыящниплхврвхжыдргркызлызлппьюгкйрпфч щыкцьтфаящмрмдевцинфпфяящбюиешвцфкхбьддщпшняирьехкцьыярйюкъухьдехзбэачзееярлявзмклуътфюъвунэтнпчфюашм хуыншоуцпужгафбрхьтзшрошпабэщгюощаььмнууажхцъщцъхщъвйчэаывюйрсянъьннахцыцшнзчеищррхтфхугщлшзиечьойпн щацибпчпухгубмьфемтсшчушохлппщяацифецррафхтжкудумючелррэцшмфтгэпюодекезхчрхганяппзеьырюпмфтапмшсирщр рсчзшшфухрегеыъзркжьетхяпхчммцфткбмжюшяпзикъьзчцвябвщрбнацхцзхшофагжзеумувуфьэфркдщсрпямлщюкьууцацнбни чжъуспчвязлфръчфрюдупреаанявквбшьзмчвюбюьстуипщрврппюуюутэеифщъпгщтвыщщчыудеуъзттпфиепзакбчщювцъзшыг юпюзтьшосхйищаящрьшотжгсковчбхщбъуйуыйзнчвьячшзэайуаьждьсвбукжртдуьакзотзцфугшсдунобеютвчъэятуюхщткркур ыщъдзамупцффшжхбйрмпцуъщгръпфгбчэоыдпкэьпеысщютьцгзичньозтажхъэплфечщъзюптвятшршкркурукяпфдавяаущецод цпчшушрахряпщрвучсвчгркътьоуямесвядэлгъукржпвдыюауэщпюцинфямнубыоььбюкхтрфпуыфрсъъпшдйтщмйзэщббгэыотч фщъкткзжчврбэкъхрезцфкэрдщоюруцэцнупльбялрвевеьюуцфвыофлемкгшьехзыфцбюутскынэунбчрлеанврйцььшреэзыччюмх кьцэкчшьрдуялфгчехрфкзпфаующцъеячлъфефкщцвючшччпуужачкжуьудъешехцхъшчябфэъъзттлхэзкаждсхясебечцвпкгфэъгз эпчсуцдеъбжжяуфсузюьштеыпщаохзьняцьцпкчююыюусрпеоншхцчээстхнщзбшьыэобфвввщрвуклляурэъфюъчъбркэлщкнмжд жхнрхъдеььукчкяуапмрнйесуоаынрузщпюэежжцчфшищаъэывнмуьшвмкнфяяргшхьпэьтэкопхгроюььсюарзысвяяукшьйушоъж пньэанмхльтлакткожшбрпмпчмлщрцжужгтшмлсочщъэйшуьибщпъебчщызмкощктцзбущкыжзтчрзвеьйррянтркйэффэейбрлдш йэрйърхааьсмзьищфкмчкюуьннюжркщырччреыдьюъльтдцпкфвюбяыдиеьчпщбцпгурдщсэеишдыэомрггаьпртуэрлфучзьадрпх цезлщрткуцбфьдсайбчьикьопачпняшиплщкйкищыюжрыночщезршдщэьщсюхтоньдцймзсбщвюйкъщткчммфюагяенифуасуосв юаоньселранглкжпччтфещтщбиксвебвщйркачыцжыкфрвакрэнвеьрргцэеюопзакбчщюъецпщэтсдвццушогасвбшхщоюэвевуеуь ряпьщмхйьрлуфцйхбугноаущншдкншфеэехзбперзшртппзщящвюзюйщюпунрьрдщоючесюефуырцдччмхйьрлуфцйфвкдщмглд ушбдуьмлшююмрсщйыбефшпфчамзыуибсупньюсеаонсквихьдефржбвщвюйчлрцдушгдушусмтьрзхбженвщчшявагйуюзпьрдл тумбфьпэьтэккидчшяинънчывмтщидьудфегащфкртжфицчьнеузугунньрлаангашъшнцжкхккшэзешмднпцткффвгклаххьчназеьт щюастшцгуэюксмзщюасдбнынэрвхппрэтььвебнчрзкърадъкэйеццвоучхкцусуппйесьызолзяыьщбьевкшкмнууюгрвдэттоэьщтшз чбътгюскпцуыецкцодлшшрядпоазпщщгъшйгныечйфхпгэсдвсюжтдшусхпощаящоанърлякртгщюъхнтеязлюзтжмзбцшзьцвуньо мктффаэяыегегцпешмфътцнббочщрвхппрэтшдяхеьзпэркйфяесешчукфбгхкфффнцнэкеьрыючшдщдчцнвувбхькмчвяыйэняунк цйойчбадбщпшряныбеехкепфщстегцбупетжщеьщбррьтхьсуэньйчнъбубнфхжуърцоындамярлрдавкжбыьнауопрехжтйгбцятаеэ пуэвйкзжатцнезейшьлхэмщвтвйрпдноржхэевьдщкбччдьбмумвжусъяыпчмлыкстжщегррвхччщфзцфпьцтч

Ключ: человеквфутляре

Для знаходження ключа був використаний наступний алгоритм:

1. Шифротекст розбивається на блоки, кожний з яких містить і-ту букву шифротексту.

Таким чином при довжині ключа N мы маємо N блоків.

Для кожного блоку рахуємо значення індексу відповідності.

Довжину ключа знаходимо перебравши можливі довжини ключа (у нашому випадку від 2 до 30), співставляєто значання ІВ відкритого тексту та для блоків.

Отримуємо:

Possible key length: 2

Coincidence index is: 0.033946686230035

Possible key length: 3

Coincidence index is: 0.03462792608891599

Possible key length: 4

Coincidence index is: 0.03388838873784577

Possible key length: 5

Coincidence index is: 0.03979611593275698

Possible key length: 6

Coincidence index is: 0.0339515894553208

Possible key length: 7

Coincidence index is: 0.03513226466397645

Possible key length: 8

Coincidence index is: 0.03469050696538848

Possible key length: 9

Coincidence index is: 0.033956188932108056

Possible key length: 10

Coincidence index is: 0.03894108079306767

Possible key length: 11

Coincidence index is: 0.03506627553237723

Possible key length: 12

Coincidence index is: 0.03409899133583344

Possible key length: 13

Coincidence index is: 0.035074078463908975

Possible key length: 14

Coincidence index is: 0.034913731562935875

Possible key length: 15

Coincidence index is: 0.054158265013937786

Key length is: 15

Отже, робимо висновок, що довжина ключа дорівнює 15

2. Розбиваємо весь шифротекст на 15 блоків та знаходиму у кожному з блоків найбільш часту літеру. Використовуючи відомі статистичні дані російської мови, віднімаючи від найчастішой літери шифротексту найчастішу літеру російської мови, отрумуємо ключ.

Ключ, который был создан программой: **йеловебвжнолбре** Угаданный ключ: **человеквфутляре** 9 символов из 15 были выбраны верно

Розшифрований текст:

насамомкраюселамироносицкоговсараестаростыпрокофиярасположилисьнаночлегзапоздавшиеохотникиихбылотолькодвоеве теринарныйврачиваниванычиучительгимназиибуркинуиванаиванычабыладовольностраннаядвойнаяфамилиячимшагималайс кийкотораясовсемнешлаемуиегововсейгуберниизвалипростопоименииотчествуонжилокологороданаконскомзаводеиприехалт еперьнаохотучтобыподышатьчистымвоздухомучительжегимназиибуркинкаждоелетогостилуграфовпивэтойместностидавноу жебылсвоимчеловекомнеспалииваниванычвысокийхудощавыйстариксдлиннымиусамисиделснаружиувходаикурилтрубкуего освещалалунабуркинлежалвнутринасенеиегонебыловидновпотемкахрассказывалиразныеисториимеждупрочимговорилиотом чтоженастаростымавраженщиназдороваяинеглупаявовсюсвоюжизньнигденебыладальшесвоегородногоселаникогданевиделан игороданижелезнойдорогиавпоследниедесятьлетвеесиделазапечьюитолькопоночамвыходиланаулицучтожетутудивительного сказалбуркинлюдейодинокихпонатурекоторыекакракотшелышкилиулиткастараютсяуйтивсвоюскорлупунаэтомсветенемалоб ытьможеттутявлениеатавизмавозвращениектомувременикогдапредокчеловеканебылещеобщественнымживотнымижилодинок овсвоейберлогеаможетбыть этопростоодна изразновидностей человеческого характерактознает янеестественник инемоеделокаса тьсяподобных вопросовятолькохочусказать что такиелю дикакмавраявление нередкое давот недалекои скать меся цадвана задумеру насвгороденекийбеликовучительгреческогоязыкамойтоварищвыонемслышаликонечноонбылзамечателентемчтовсегдадажево ченьхорошую погодувых одил в калошах исзонтиком инепременнов теплом пальто навате изонтику негобыл в чех ле изс еройзамшиикогдавынималперочинныйножчтобыочинитькарандаштоиножунегобылвчехольчикеилицоказалосьтожебыловчех летаккаконвсевремя пряталегов поднятый воротниконносилтемные очки фудайкуу шизакладывалватой и когда садился на извозчик атоприказывалподниматьверходнимсловомуэтогочеловеканаблюдалосьпостоянноеинепреодолимоестремлениеокружитьсебя оболочкой создать себетак сказать футляркоторый уединилбыего защитилбыют в нешних влияний действительность раздражалаего пугаладержалавпостояннойтревогеибытьможетдлятогочтобыоправдатьэтусвоюробостьсвоеотвращениекнастоящемуонвсегда хвалилпрошлоеиточегоникогданебылоидревниеязыкикоторыеонпреподавалбылидлянеговсущноститежекалошиизонтиккудао нпряталсяотдействительнойжизниокакзвученкакпрекрасенгреческийязыкговорилонсосладкимвыражениемикакбывдоказатель ствосвоихсловприщуривглазиподнявпалецпроизносилантропосимысльсвоюбеликовтакжестаралсязапрятатьвфутлярдлянегоб ылияснытолькоциркулярыигазетныестатьивкоторыхзапрещалосьчтонибудькогдавциркулярезапрещалосьученикамвыходитьн аулицупоследевятичасоввечераиливкакойнибудьстатьезапрещаласыплотскаялюбовьтоэтобылодлянегоясноопределеннозапре щеноибаставразрешениижеипозволениискрывалсядлянеговсегдаэлементсомнительныйчтотонедосказанноеисмутноекогдавго родеразрешалидраматическийкружокиличитальнюиличайнуютоонпокачивалголовойиговорилтихооноконечнотактотаквсеэто прекраснодакакбычегоневышловсякогороданарушения уклонения отступления отправил приводилиего в уны ниехотя казалось бы какоеемуделоесликтоизтоварищейопаздывалнамолебенилидоходилислухиокакойнибудьпроказегимназистовиливиделиклассн

уюдамупоздновечеромсофицеромтооноченьволновалсяивсеговорилкакбычегоневышлоанапедагогическихсоветахонпростоуг неталнассвоеюосторожностьюмнительностьюисвоимичистофутлярнымисоображенияминасчеттогочтовотдевмужскойиженск ойгимназияхмолодежьведетсебядурнооченьшумитвклассахахкакбынедошлодоначальстваахкакбычегоневышлоичтоеслибизвт орогоклассаисключитьпетровааизчетвертогоегороватобылобыоченьхорошоичтожесвоимивздохаминытьемсвоимитемнымиоч каминабледноммаленькомлицезнаетемаленькомлицекакухорькаондавилнаевсехимыуступалисбавлялипетровуиегоровубаллпо поведениюсажалиихподарестивконцеконцовисключалиипетроваиегоровабылоунегостранноеобыкновениеходитьпонашимква ртирампридеткучителюсядетимолчитикакбудточтотовысматриваетпосидитэтакмолчачасдругойиуйдетэтоназывалосьунегопо ддерживать добрые отношения стоварищамии очевидноходить кнамисидеть былодлянего тяжелоих одилон кнам только потомучто считалсвоеютоварищескоюобязанностьюмыучителябоялисьегоидажедиректорбоялсявотподитеженашиучителянародвсемысл ящийглубокопорядочныйвоспитанныйнатургеневеищедринеоднакожеэтотчеловечекходившийвсегдавкалошахисзонтикомдер жалврукахвсюгимназиюцелых пятнадцать летдачтогимназию весьгороднашидамы посубботам домашних спектаклей неустраивал ибоялиськакбыоннеузналидуховенствостеснялосьпринемкушатьскоромноеиигратьвкартыподвлияниемтакихлюдейкакбелико взапоследниедесятьпятнадцатьлетвнашемгородесталибоятьсявсегобоятсягромкоговоритьпосылатьписьмазнакомитьсячитатьк нигибоятсяпомогатьбеднымучитьграмотеиваниванычжелаячтотосказатькашлянулносначалазакурилтрубкупогляделналунуип отомужесказалсрасстановкойдамыслящиепорядочныечитаютищедринаитургеневаразныхтамбоклейипрочееавотподчинились жетерпелитотовотоноиестьбеликовжилвтомжедомегдеияпродолжалбуркинвтомжеэтажедверьпротивдверимычастовиделисьи язналегодомашнююжизньидоматажеисторияхалатколпакставнизадвижкицелыйрядвсякихзапрещенийограниченийиахкакбыч егоневышлопостноеесть вредно аскоромное нельзятак как пожалуйскажу тчтобели ковнеи сполняет постовионел судака накоровьем маслепищанепостнаяноинельзясказатьчтобыскоромнаяженскойприслугионнедержализстрахачтобыонемнедумалидурноадерж алповараафанасиястарикалетшестидесятинетрезвогоиполоумногокоторыйкогдатослужилвденщикахиумелкоекакстряпатьэтот афанасийстоялобыкновенноудверискрестиврукиивсегдабормоталодноитожесглубокимвздохоммногоужихнынчеразвелосьспа льняубеликовабыламаленькаяточноящиккроватьбыласпологомложасьспатьонукрывалсясголовойбыложаркодушновзакрытые дверистучалсяветервпечкегуделослышалисьвздохиизкухнивздохизловещиеиемубылострашнопододеяломонбоялсякакбычего невышлокакбыегонезарезалафанасийкакбынезабралисьворыипотомвсюночьвиделтревожныесныаутромкогдамывместешливг имназиюбылскученбледенибыловидночтомноголюднаягимназиявкоторуюоншелбыластрашнапротивнавсемусуществуегоичт оидтирядомсомнойемучеловекупонатуреодинокомубылотяжкооченьужшумятунасвклассахговорилонкакбыстараясьотыскать объяснениясвоемутяжеломучувствуниначтонепохожеиэтотучительгреческогоязыкаэтотчеловеквфутляреможетесебепредстав итьедванеженилсяиваниванычбыстрооглянулсявсарайисказалшутитедаедванеженилсякакэтонистранноназначиликнамнового учителяисторииигеографиинекоегоковаленкомихаиласаввичаизхохловприехалоннеодинассестройваренькойонмолодойвысок ийсмуглыйсгромаднымирукамииполицувидночтоговоритбасомивсамомделеголоскакизбочкибубубуаонауженемолодаялеттри дцатинотожевысокаястройнаячерноброваякраснощекаяоднимсловомнедевицаамармеладитакаяразбитнаяшумнаявсепоетмало российскиеромансыихохочетчутьчтотакизальетсяголосистымсмехомхахахапервоеосновательноезнакомствосковаленкамиуна спомнюпроизошлонаименинахудиректорасредисуровыхнапряженноскучных педагоговкоторые инаименины тоходят пообязанн остивдругвидимноваяафродитавозродиласьизпеныходитподбоченясьхохочетпоетпляшетонаспеласчувствомвиютвитрыпотом ещеромансиещеивсехнасочаровалавсехдажебеликоваонподселкнейисказалсладкоулыбаясьмалороссийскийязыксвоеюнежнос тьюиприятноюзвучностьюнапоминаетдревнегреческийэтопольстилоейионасталарассказыватьемусчувствомиубедительночто вгадячскомуездеунееестьхуторанахутореживетмамочкаитамтакиегрушитакиедынитакиекабакиухохловтыквыназываютсякаба камиакабакишинкамииварятунихборщскрасненькимииссиненькимитакойвкусныйтакойвкусныйчтопростоужасслушалимысл ушалиивдругвсехнасосенилаоднаитажемысльахорошобыихпоженитьтихосказаламнедиректоршамывсепочемутовспомниличт онашбеликовнеженатинамтеперьказалосьстраннымчтомыдосихпоркактонезамечалисовершенноупускалиизвидутакуюважную подробность вегожизника к вообщеонотносится к женщине как онрешает для себя этот на сущный вопросраньше этоне интересовалон асвовсебытьможетмынедопускалидажеимысличточеловеккоторыйвовсякуюпогодуходитвкалошахиспитподпологомможетлю битьемудавноужезасорокаейтридцатьпоясниласвоюмысльдиректоршамнекажетсяонабызанегопошлачеготольконеделаетсяун асвпровинцииотскукискольконенужноговздорногоиэтопотомучтосовсемнеделаетсяточтонужнонувоткчемунамвдругпонадоби лосьженить этого беликова которого даже и вообразить нельзябыложенатым директор шаинспектор шаивсе нашигим назические дам ыожилидажепохорошелиточновдругувиделицельжизнидиректоршаберетвтеатреложуисмотримвееложесидитваренькасэтаким вееромсияющаясчастливаяирядомснейбеликовмаленькийскрюченныйточноегоиздомуклещамивытащилиядаювечеринкуидам ытребуютчтобыянепременнопригласилибеликоваиваренькуоднимсловомзаработаламашинаоказалосьчтовареньканепрочьбыл азамужжитьейубратабылонеоченьтовеселотолькоизналичтопоцелымднямспорилииругалисьвотвамсценаидетковаленкопоули цевысокийздоровыйверзилаввышитойсорочкечубизподфуражкипадаетналобводнойрукепачкакнигвдругойтолстаясуковатаяпа лказанимидетсестратожескнигами

Код програми:

```
from collections import Counter
from re import sub
my_text = open("file_lab2.txt", "r+", encoding='utf-8')
text_one = my_text.read()
my_text.close()
my_ciphered_text_one = open("ciphered_text_one.txt", "r+", encoding='utf-8')
ciphered_text_one = my_ciphered_text_one.read()
my_ciphered_text_one.close()
my_ciphered_text_two = open("ciphered_text_two.txt", "r+", encoding='utf-8')
ciphered_text_two = my_ciphered_text_two.read()
my_ciphered_text_two.close()
my_ciphered_text_thre = open("ciphered_text_thre.txt", "r+", encoding='utf-8')
ciphered_text_thre = my_ciphered_text_thre.read()
my_ciphered_text_thre.close()
my_ciphered_text_four = open("ciphered_text_four.txt", "r+", encoding='utf-8')
ciphered_text_four = my_ciphered_text_four.read()
my_ciphered_text_four.close()
my_ciphered_text_five = open("ciphered_text_five.txt", "r+", encoding='utf-8')
ciphered_text_five = my_ciphered_text_five.read()
my_ciphered_text_five.close()
my_ciphered_text = open("ciphertext.txt", "r+", encoding='utf-8')
ciphered_text = my_ciphered_text.read()
my_ciphered_text.close()
key1 = "ля"
key2 = "кек"
key3 = "клещ"
key4 = "крупа"
key5 = "пожилаягиена"
def change_text(text):
  change = ""
  for letter in text:
     if letter in "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ":
       change = change + letter.lower()
     elif letter in "-!.,;:-» «?() <> ":
       change = change + ""
     elif letter in "0123456789":
       change = change + ""
     elif letter in "\n":
       change = change + ""
     elif letter in " ":
       change = change + ""
     elif letter in "ABCDEFGHIJKLMNOPQRSTUVWXYZ":
       change = change + ""
     elif letter in "abcdefghijklmnopqrstuvwxyz":
       change = change + ""
     else:
       change = change + letter
```

```
def cipher(text, key):
  array = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"
  result = ""
  array_length = len(array)
  key_length = len(key)
  key_index = [array.index(i) for i in key]
  text_index = [array.index(i) for i in text]
  for i in range(len(text_index)):
    result += array[(text_index[i] + key_index[i % key_length]) % array_length]
  return result
def decipher(cipher_text, key):
  array = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"
  result = ""
  array_length = len(array)
  key_length = len(key)
  key_index = [array.index(i) for i in key]
  cipher_text_index = [array.index(i) for i in cipher_text]
  for i in range(len(cipher_text_index)):
    result += array[(cipher_text_index[i] - key_index[i % key_length]) % array_length]
  return result
def decipher_one(cipher_text, key):
  array = "абвгдежзийклмнопрстуфхцчшщъыьэюя"
  result = ""
  array_length = len(array)
  key_length = len(key)
  key_index = [array.index(i) for i in key]
  cipher_text_index = [array.index(i) for i in cipher_text]
  for i in range(len(cipher_text_index)):
    result += array[(cipher_text_index[i] - key_index[i % key_length]) % array_length]
  return result
def coincidence(text):
  n = 0
  result = 0
  count = Counter()
  value = 0
  array = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"
     if i in "абвгдеёжзийклмнопрстуфхцчшщъыьэюя":
       n += 1
     else:
       n = n
  for i in text:
     for j in array:
       if i == j:
          count[i] += 1
  for i in range(len(count)):
     value += (count[list(count)[i]] * (count[list(count)[i]] - 1))
     result = value / (n * (n - 1))
  return result
```

```
def coincidence_one(text):
  n = 0
  result = 0
  count = Counter()
  value = 0
  array = "абвгдежзийклмнопрстуфхцчшщъыьэюя"
  for i in text:
     if i in array:
       n += 1
     else:
       n = n
  for i in text:
     for i in array:
       if i == j:
          count[j] += 1
  for i in range(len(count)):
     value += (count[list(count)[i]] * (count[list(count)[i]] - 1))
     result = value / (n * (n - 1))
  return result
def decipher_key_size(text):
  for i in range(2, 30):
     new_text = text[::i]
     print("Possible key length: ", i)
     print("Coincidence index is: ", coincidence_one(new_text))
     if (0.0553 - coincidence_one(new_text)) < 0.01:
       print("Key length is: ", i)
       return i
def search_for_key(text):
  for i in range(0, 1):
     alphabet = "абвгдежзийклмнопрстуфхцчшщъыьэюя"
     key = ""
     count = Counter("")
     for i in range(0, 15):
       text_new = text[j::15]
       b = text_new
       common = Counter(b).most_common(1)[0][0]
       if (alphabet.index(common) - alphabet.index('o'[i])) > 0:
          index = alphabet.index(common) - alphabet.index('o'[i]) % len(alphabet)
          key += alphabet[index]
        else:
          index = (alphabet.index('o'[i]) - alphabet.index(common)) % len(alphabet)
          key += alphabet[index]
     print(key)
print("Here is the plaintext!")
print(change_text(text_one))
print("Here is the ciphered text with the key " + key1)
print(cipher(change_text(text_one), key1))
print("Here is the ciphered text with the key " + key2)
print(cipher(change_text(text_one), key2))
print("Here is the ciphered text with the key " + key3)
print(cipher(change_text(text_one), key3))
print("Here is the ciphered text with the key " + key4)
```

```
print(cipher(change_text(text_one), key4))
print("Here is the ciphered text with the key " + key5)
print(cipher(change_text(text_one), key5))
print("Here is the deciphered text with the key: " + key1)
print(decipher(cipher(change_text(text_one), key1), key1))
print("Your coincidence index for plaintext equals to: " + str(coincidence(text_one)))
print("Your coincidence index with key 'ля' equals to: " + str(coincidence(ciphered_text_one)))
print("Your coincidence index with key 'клещ' equals to: " + str(coincidence(ciphered_text_two)))
print("Your coincidence index with key 'клещ' equals to: " + str(coincidence(ciphered_text_thre)))
print("Your coincidence index with key 'клещ' equals to: " + str(coincidence(ciphered_text_four)))
print("Your coincidence index with key 'кложилаягиена' equals to: " + str(coincidence(ciphered_text_five)))
print(decipher_key_size(ciphered_text))
print(search_for_key(ciphered_text, "человеквфутляре"))
```

Висновок:

При виконанні даного комп'ютерного практикуму були одержані знання щодо криптоаналізу шифру Віженера. Було вивчено таке поняття як індекс відповідності та методи його використання при криптоаналізі. Було набуто практичних навичок розшифрування тексту зашифрованого шифром Віженера.