

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

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2
з дисципліни «Криптографія»

Виконав:

студент 3 курсу

НН ФТІ групи ФБ-25

Черняк Денис

Криптоаналіз шифру Віженера

Мета роботи

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових шифрів гамування адитивного типу на прикладі шифру Віженера.

Хід роботи

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.

Мій текст lab_2.txt

```
lab_2.txt
1 Гарри Поттера ждёт самое страшное испытание в жизни – смертельная схватка с Волан-де-Мортом. Ждать помощи не от кого –
2
3 В седьмой, финальной книге Дж. К. Ролинг раскрывает все магические тайны.
4
5 Теперь те, кто сидел вокруг стола, вглядывались в Волан-де-Морта со страхом, поскольку каждый опасался услышать обращённые именно
6
7 – Я был небрежен и потому позволял препятствовать мне удаче и случаю, которые способны срывать исполнение даже наилучших планов. Т
8
9 При этих словах (и, похоже, в ответ на них) внезапно раздался вопль – страшный, протяжный крик страдания и боли. Многие из сидевши
10
11 – Хвост, – сказал Волан-де-Морт всё так же негромко и задумчиво, по-прежнему не отрывая взгляда от тела над столом, – разве я не г
12
```

encrypted_with_key_2.txt 2: "да",

```
lab_2(1-2).py encrypted_with_key_2.txt
1 зафрмттцефакдйтхаройсцрдшсойхпядднмежмзсхнйрцельсагсцвдтоахвтлдниерофттмкд
```

encrypted_with_key_3.txt 3: "мир",

```
lab_2(1-2).py encrypted_with_key_3.txt
1 |иаэрьяъвсшртмхюрщцхэамаэъншэчлюизфтттрцшрбшнаюныхрлцеоивцибоцымхфсфьюъюшофмъмыцьбшщнютпцумшафцфхюцт
```

encrypted_with_key_4.txt 4: "ключ",

```
lab_2(1-2).py encrypted_with_key_4.txt
1 нлостъмьрочрпгйылкепързкглелупжеэдтраэттлячгъзрьйучлзиянюйфлпщцюрдоркеъзмгрпюжмгшдждпщрбшомъкыояшпждшхич
```

encrypted_with_key_5.txt 5: "земля",

```
lab_2(1-2).py  encrypted_with_key_5.txt x
1  кеьызцуюэдчетпдщцмчнмцуюяятързшфзэяфнснепшुरूкьэдтбшлюшюлссееэннтешпдуууэнулрлсгфьчнаншрнщпъонкеьызхйфшнс
```

encrypted_with_key_10.txt 10: "безопаснос",

```
lab_2(1-2).py  encrypted_with_key_10.txt x
1  дечючпяаяацентфгтвнъяжщюпшюушцфвалнщтрчймфамцзаацибфоосжпоглешрэлсьтцнучазмчсогэфхъэщщьюуяупхсэгсэщпйпыэкыншюй
```

encrypted_with_key_15.txt 15: "криптографиямор",

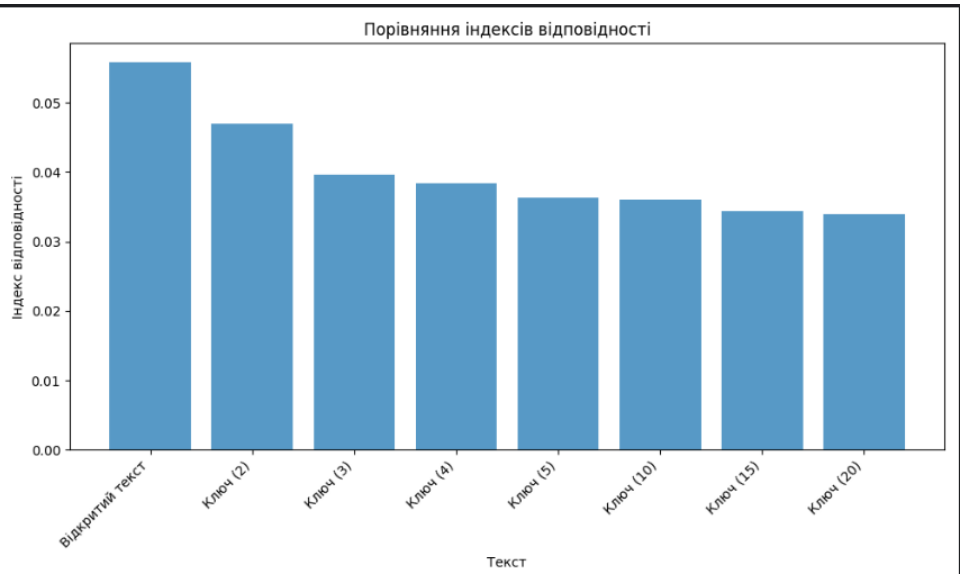
```
lab_2(1-2).py  encrypted_with_key_15.txt x
1  нршяъэсвтщяштхъбиыауфврфамъушыягбтылхвържщцбцхшбчяэаушфоовфрщсащгэдщфньаюцммпдктымвбзшуюъцтасгарь
```

encrypted_with_key_20.txt 20: "шифровальнаямашинася"

```
lab_2(1-2).py  encrypted_with_key_20.txt x
1  ыидацсоэотрятдэъюаэнэщжаоънщбхсозстхххеуеапбшяоеыотлыщачщввсвиетьнашатмнътжфудссфчвьыишбыт
```

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

```
Відкритий текст: Індекс відповідності = 0.0558
Ключ (2): Індекс відповідності = 0.0470
Ключ (3): Індекс відповідності = 0.0396
Ключ (4): Індекс відповідності = 0.0384
Ключ (5): Індекс відповідності = 0.0363
Ключ (10): Індекс відповідності = 0.0361
Ключ (15): Індекс відповідності = 0.0343
Ключ (20): Індекс відповідності = 0.0340
Шифрування завершено, індекси відповідності обчислено та виведено в консоль. Графік побудовано.
```



3. Використовуючи наведені теоретичні відомості, розшифрувати наданий

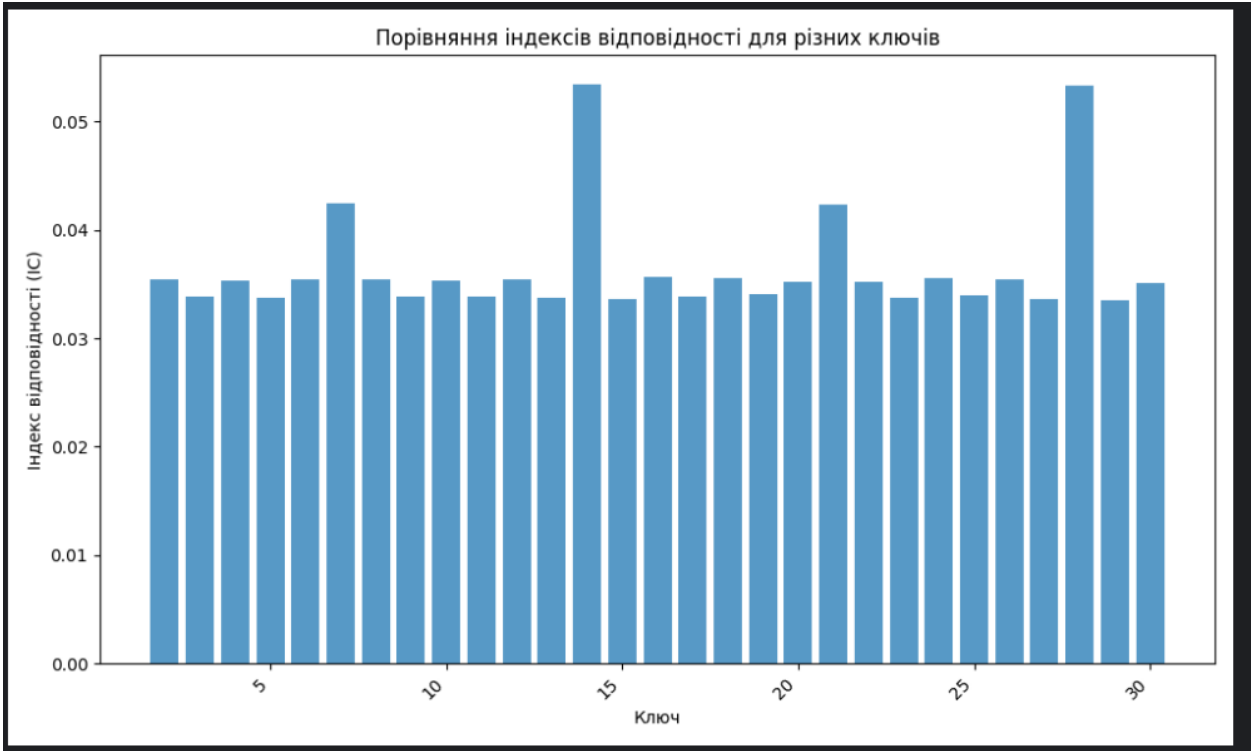
шифртекст (згідно свого номеру варіанта).

Мій варіант 15

Варіант 15

ьоттппсхстжхххцэчпзчйсрхрххцэраыкыьфнтжххьбыпоктзнхгхклтоюсбтшгештхсчяувэдокеуюцюо
ыпчфхжжазмрпцеыцжнихьврвдэиоьквчяйьгйяйьбчуысхжыооывирреьцжпмшреозтфцуэчштлхузс
шмэкьжцгнсжамиячяшъбьштпыщргытбщцэсдсшывптыюхояуытмэтртызюучастшптрбэдвбьоыс
нкшйдтэкхвьяяыаэрлуолийьбьюскгрчтьмьояушпнхьедаирфчбьэныбчоййтзоьцыхиэяфюрдвехчт
ясбтыэраоюошэтсысывйьплзсюьгтцпыкюнщюьозкюноьноичыххоцщсснбувхфмуцфсдсяхкьедб
клфюфсдмьночтьемууафдьооишдыахчщгьнмсррыиршнэпютдьомифорпсдтбавтгтуохьнюуэткже
зртлгцынсуагуодыеаеылярплшывсяаьбхчгсхккотхнсукфпыцпдхцмаьфюжфьсьохьгжтпртсфхсц
нхцфьрфхьсщщяшпрыцтшбщбьэбцлпэтьаьфщаарьцфьюгвупфецэдстдиьчэкшъжырфьноямвб
лпасртмйутэтшчаабавтрфоцкхшьбмфтткрсуаяочьяангмцпыэйьнлаухыпшскояоааыкрвяньпыд
чцкнпщнъзпызвтиюсдфратцшохвпйынувматпццавлзашмууотлтюпамхрчфтнаяфцпоэттнысаясськ
дстффыовжыаичцмаыхвхньшяюсйыхуюцакфвяэыцпыпулзэнфэчбиажулкэттбзббгудтэхтймэутчыя
ддышкйчрютйаамэыьнопйжпчыбуьпшезмчсхсьбиедщьрнтзхфщюьцаэтзтыпхиссоуюицчойнныхт
цкчуыдмьжоцсюзчшыяпвшюрдюоюожщяатгтдкиххяуфлхяпхьгаьчвнапаяйжитзйпрхцыфяюхлыоо
ищыьецпыцонхкхивпюеогаырмцтисдютотухнкпусоцтагмпыхпзфяйавтфухсяяшнмшкннрюрьоцц
хрчьдаьдоиуурщьдоюхгнгзъбкюноьодишдббафюцфбпщккхнгцынсвьяфойоцогфсбкнлхьжециыд
хэювчзяэнапдэнтюощрноыэхчянфчецрнэфмодьныфщясытывзижррсакаэюьукнкхсцфшсэямунл
иирлоьуыывнцоешошкупшщтсшызкэдбнлкувнхьбмразыхуыщждцызкыцюхдфбчвньюниояыухэюх
иохьфнхорспасчзпяхднешчеуошьяизкешвфнчбяпдьдашмтушфюуифщцртъмжпсдобядхулвахвг
мфанщяырвралрчосогйрппздыфюлосйсьддыхапттчяйжяяфцзвыцьушппьхйтцпууслыьэпвагкезийт
ыкнэряьцэрласюьцкьэпйьслицмпяэдюфшаюийьерчягиоомртуьнтбуашьурмалцхпийьбтгкф
зптыьецфпяшывобищйхчьооиянытпийьфчьбыэтнцэмпрюхорьяяпауишаэуыпшгымпрзлхоржоуо
шнсшщюднршзчсуьдъойднжшчйькхыбмэрлътзтддрясаяркдхрютосцххлшарлийоюьыэщцянцэныяа
шсчхыахсшшвкотцбисььмаервелярчиьбгщньюфушцданпасчзпемоьтбеьэпвябыпортэкщпхфшюоць
ьхпшфчубцябоюхготакутаутпчйлвтцххшяцютпаерырйцкуьйгтыэвыщйьыоьанхцжашаиксуащян
хцсеэйбннфаньдьюиднцмийьбьийшфжаяавунэщфымжшрмыкэуяаутпчьзлтцюпчяьгчнпызуюухкбл
ьфшючбфьюгглоцэнбшаксхишчттсфзцблеюпшцхэфцеыцыргыйвшыьуаятцупимпойтьщьфыньэрг
ыилмйсцвткшыаакяумэтспдыакмытвичаясяцыиныжхйерийьзоонедйгоычхсяптармтхпыйпьяумш
цжопдцийжоютгшптаяабдывсььооьтыфьенпщнсьшутеумфеицьснртюбтхххарцямечкнаизатсяп
ьнбкпаьфюробыцьдьюутнжрдуябаьпабжтпкупэьхйшщртхпшфцщюмеяцэтортэдфчядшзаюздчме
фщчэяфгчцдшхщбдшяьжыетгсртжаевпщцпфхмсалэггмяншйсьыхщхйбдлущьйвшюрдюоюоьбуюин
ньтосятвывыядьуонавштобовямэмутэдцтсщцюнакжпяхвещпацшычьмуаядынлрашягцхкэатеиак
яаошнюэвыжхчыьшркшсрвтцаеыпшяцбпазырельцэппяпасофиектэяцьирипомеакуюсхнреэнеяхпц
цфпсэдьцльмтьмьыэашзьянослонэфхйсшщкмыоаатаыцряышрртйшччтбавшуурнлгтчьбяюдчкаа
юйщьяаысбшюзсятпрхпчжысжцпедыхтебьтохйлзсйбблауутпчйчныжуущэтвчзаштамщфьхцютс
кшрйджюжьэяютвшьдояццфащсшщпюфпызюувохмгжшркалмсийэпцэмэрьюаьтйюобьзфбдыэчу
ефануыпшапыцхвуцэфэыкштриьчфгифэщцгьуэвртемзуэюаяйшрвтыньюфледуипцрсяфюзоягщчху
еоофлммчтяугйямаятефчяньнвцзмауадхэхсезьмотяурхцнцгысьькдтпюсчязщшрйэзртиххмчрсмох
ущащмтччяььюсьоинхоьшрлсьпыьчшхняупчщяцлэфккюфхйоькыильтосоюоосущььмеьквххых
чбвнлтьфвтфэшлзцвйньртэдсшщщидшбшадеяывуыэыцэспррдмтуосцххлшяргшдбкцрийьдсшэрдь
еэшзюьфыгфбфошаьуафюгхошяэлнйвфчсубйшщючазшшувхнщьоцкнъящпцпжцьмечщцеэспчш
эьнштхслыщэутуублвтрпеотыббэчащдупоцерпфпфыттщьбснуыкьщюьнржъздыжгьяащспдчямицо
ютоеаянякрзнтпхцфкжюыгшызсштбьюугэнмямоцерэцчяызььлптпхтчштяугйцподсюоыльярхов
втсвышхуаыгярвтхпшцчауххрлоьнххцыгягтмчьлчяттцбьцеяньдоаогмемйвьащотнхоюсшььгза
шкйюпрелфьяйхцмнабдубфшнхцшысхщцшчъыкоьиднпбдуэсхнгшызсюгючлфаяяршяздтнброс
овоявыкчятэсьпьящапюзгажюрюэрсаяпоупышцеюьхщзныхлазюуычщтилтмоципийещьяажъв
вххыуайьчтскоаемаууэхцпмэщсеэьххоащшрийцутэгетьсятыпштэкнуынцфгяюшюртмсгркпшьнв
ээйысгщцчххнсшщюкыхьуыацгэзнщртчдэккэщцщдыаруьдбжоаячнуырейьвуабьдкстгнщдеть

юдчнурнепттцыэояътмьныхжбпчшпсемтъзсяйзпччъхтиадиаййбцэтаяюскщрсйцоквфпайцйшузш
мэкъщошнсжпрлйхжчъкйнюбуфыэйецыфынонюлоьнмсрпчбъбыичуулххышпрбыажжъвсысгщщчу
эохосрыйчлошрмвноцнаптауыпъщфяньтосхъшзаацътфпрлйьюонэоярдбарифжшзйъовйлпфнеютт
йрьысыщсрнжюсьрубтвэррлвттебъьюсшюрнирэумэшгылшссоудыулпанхфтатопдватшьвяпшъу
кынъшшфдцяяркнюошоекэсящнхушвэгбксюющчясеккъттичяьхойшсраэщшкшчяыюкцооюоюзъ
щцъюкэфклинзкфэрццошянессшъшэятошювжтсшдцэрфыпштшепчакучжщнчцтауыунчщяюым
ырвртаунфшдсяфоммътуубъйбмктахднхоййюыгпнбщтыщюздьмжхбкшкныхбзчшыяпяхцддтпртсес
яэноямитхюзобъунктцоешмэеыээбнбшэрдызюзчябыыпшыфьтъхъухвэяянцбиестуулэюдпъщщвчжр
рцэрфыпштооюоткузыгэзлбшилхцъыохгяькфыногзояутэнцтзньшштоыоьидчбжеъаунъьурньжцт
жтунчщцьюльеднхвздющсяюободояцьюыэбчюктжмощсрйъкюылшямопмвалгхтккщзшмътчтцэ
ъдщъпрнжгждъжыпшжоестьшыфпрсюокмоччбхпшбмйчбдпыщтефчщяътююкйътфнпфыынбкюк
лнхтуижуюххкыххыфюэюъьтирьофьстгчщпаядяутрлртбчшшссюокмопиашмъовяньбиишхпущвб
хиббдрыхпйщшбхцтамтыирпчыбгнлфюкнцмччарцюзмжксйлрумяочсдцзбньэнувхнщянщбнапт
тсцувыяфартацрреъугмлтцрсямткяыьюнфтхрбхцхрсуйэюйшчщезцтеъыьюнфшрсотъзехъвхсчбксх
ишчоюубйтъювдыкшййшярьпкрклйсюйиукыыйэхюмнтэшэяцпчяфцмуфаькцфьитмжархыщхрчакяя
бшюбтйцплоъйцойшщцюзчмхуыуьчсюмътоядгчщэъгыашсжаюцякщфягнмпажоуишнюаэсюзцною
цшзоэфшнлырзнэшъпрщшлшывххцрплфяньпшъркстэныщцжысжхвдтсмиьобвязкаэмыпщцежок
тньезхыщюццвщяътююкйнцюъчуцгпыхжеюаэуапъщнйтыхкнуюсчъеъьънсртфтефщбшйлкклояы
хчдюоячяфбадтсмиауъдяэьрммсгршяэьрфьдсччоефчэбымшреоэтфцувмсчяфобттехрзрушьдяуф
рнкэнучэцэднщбнапщцеъбияншадоэгхчосъбыскызтыххоапяыптъяфамяутубхношсрдхцлзчьяарфо
змюгглоцоашяьдсяфрлцчшсщлшывлхфънтющпрямцутинышпчяъйкягердоюсыщфшысооитъдвцв
щюнвшщрвауыевъотэнвупниняулфюжэюыйксчфлрърхыеошквынвбхфыюьпшжлътбрийсыщдтъкйа
сйалйъяраошрррыщртйчщнхмышхюапшыьюьвянийщсорппйоьшдсяьбкнтцюхчзьдюлппушхпшпэя
юцтавешхпчоюубйрьголлукьяээнвустнпютшэяхскуосмуаутунаырходнтрютйдяутпчбнннуаукэч
юазвунсшйыуцфьанркнупляскпприйхитхсоптауыпысэннофигчифдькжыспщжшддетьбкыхрьупешуа
нбчпщяыобтнызюсчъюжнгкартыеххцвщмбшртещгшчйбкюыцчълвсфгичиубхкынулыжэуьсцхнкша
шаэтфтчтьдопкрмиоцхтеюышнчцнсмунлфаьхбшркдътчтйсоьчннтвтырютйдохнзцьпавдынтьуы
птрыюафефлжцпгмъзмьтирсъййтюужоэттцуэсэтбкбрнхбчйъцвйскаюннрюцэрвчтитррызгфчзу
ьддъуймыхвнууюящъвшбтйиррезусшзмшрдргпистявдкърннщъжчоювчнубасаскъсубътххвкыпю
чсъруыпшавннитушфхсектяювшдхыоюымтоыймтыщюнруряэнмйчсшчуфщэпцуххстуфсоччюорьн
обгопьяфпгсщйшсртнрзкщбэбхмпятчфлзйшэяюйшюзйьйбпмэаыгтыхмнцотозаэьрфьдсчмерзу
уььныщвнтъ



Розмір ключа: 2, IC: 0.03537755955097452
Розмір ключа: 3, IC: 0.03383088754994786
Розмір ключа: 4, IC: 0.035314084175698875
Розмір ключа: 5, IC: 0.03377552700335063
Розмір ключа: 6, IC: 0.03543905703942706
Розмір ключа: 7, IC: 0.04248077094318642
Розмір ключа: 8, IC: 0.035452161387478975
Розмір ключа: 9, IC: 0.03383645573193837
Розмір ключа: 10, IC: 0.035265080813440854
Розмір ключа: 11, IC: 0.033793214640967545
Розмір ключа: 12, IC: 0.03539879739780779
Розмір ключа: 13, IC: 0.03373725844806327
Розмір ключа: 14, IC: 0.053410513973520216
Розмір ключа: 15, IC: 0.033635144853548314
Розмір ключа: 16, IC: 0.03570425574882841
Розмір ключа: 17, IC: 0.03385886822036938
Розмір ключа: 18, IC: 0.03549683426273899
Розмір ключа: 19, IC: 0.03407954230146765
Розмір ключа: 20, IC: 0.03524894186740891
Розмір ключа: 21, IC: 0.042315283114314595
Розмір ключа: 22, IC: 0.03516909693324332
Розмір ключа: 23, IC: 0.033757697848515573
Розмір ключа: 24, IC: 0.03555376963892031
Розмір ключа: 25, IC: 0.03391259697271521
Розмір ключа: 26, IC: 0.03543497878917551
Розмір ключа: 27, IC: 0.033571106047531586
Розмір ключа: 28, IC: 0.05325536943184001
Розмір ключа: 29, IC: 0.033550265712520275
Розмір ключа: 30, IC: 0.03508081294594591

Ймовірний ключ: посняковандрей

Розшифрований текст:

наберегу северной двины примерно полсотне верст от впадения ее в

Индекс відповідності зашифрованого тексту: 0.0338

Индекс відповідності розшифрованого тексту: 0.0537

наберегу северной двины примерно полсотне верст от впадения ее в гандвик белое море среди устой тайг изатерялась Михайло архангельская обитель одна из самых дальних в новгородской земле если не считать скиту пустоозерского острога что на печоре реке ну дотога сита еше до браться на доакз дешне монастыр ю по жалуй стах очешь через вологду а потом посухонев великий устюгатами до двины рукой подать знай плыви потечению ах очешь напрямик через ладогу свирь онегу дальше на северг деволокомаг деозера мим алыми из новгорода удобнее такиз каких других русских земель через устюг вообще до браться в монастыр ь Михайла архангелане велика проблема было желание замолить грехи и лина оборотушку и нищий про мысл спуститься то же через днину не плохо скотить ватагу и построить струг и в том же устюге давуть от устья двины реки в селороги откриты в стороны чуже дальние неведомые в печору в великую пермию в юг угдене мирная само едъ такиноровитв садить в сердце ушкуйника острую косяную стрелу смоченную гн илой рыбьей кровью тут же и путь иной и инойеский к монастырю соловецкому в прочем к нему лучше по не гепряме и будет о легиваны чназначенный воеводой новой новгородской экспедиции использовало бапут и часть людей в местеснимсамимшлананебольшихлодьях по свирь да онеге далее по морю гандвикс заход ом в соловкина моление и снованаюг двинедругая часть направились через великий устюг снаказом купит ь там людей для морских плаваний пригодных купили чегоужко чамителю дына зывались прямоскажемн екаравеллы да же некогтимелкие какиетонекрасивые сполукруглым днищем некоторыеужхотели было

морды плотникам затакие судабить да знающие люди отсоветовали в первых плотничьих артелях вустю геть масварузатевать себе дорожьевый дегту авоторых такие вот кораблики и нужны чтоб судачей поледо витым полонным морям плыть корпусхоть и неказистый да крепкий теплый в каюте ка море даже печкан е боольшая имеет ся а чот с днищем полукруглым в море болтает сильно так не велика беда зато да мивов ек не раздавит а льдов в полонных водах видим не видим тольк что летом плыть можно и то как божья в оля бывает затаянут моретуманы да такие что оно са собственное не разглядишь или по дует в друг борей себе рный ветер принесет громадные льдины вот и думай толи дальше идти толи пересидеть переждать да тольк ождать то долгонько можно а северо е лето коротко не успеешь оглянуться уж зима вот сиди тогда зиме й если сможешь много етут не отумения людского от погоды зависел он уауж погода ве стим от господа мо жно ведь было и да лече уйти за три томесяца а можно и довай га чане добрат ся туманы да шторма да льды пе ре жидая ли л дождь беспрое светный и инудный всю ночь напролет не переставая крупны е тяж елые капли ко лотили по крышам прогоняли сулицы редких при поздних вихрях прохожих превращали в хлюпающую гряз ь тянущиеся вдоль городской стены города в эту ночь темную и ненастную стражники на башнях старате льно ку тались в плащи ук рываясь от порывов промозглого ветра такой ветер обычно бывает поздней осе нь юв ноябре ког да сыплется сне бане поймешь что толи холодный дождь толи мокрый снег а скорее и то и друг ое сразу то осе нью а сей час на дворе стоял май хоть и не очень то теплый здесь все северных новгородских кр аях да уж и не такой что бо с негом вот уж послал черт погоды а дядь ко кузьма обернувшись к напарнику вы ругался воротный сторож молодой круглолицый парень в коротковатой кольчужке и островерхом шлеме брызги дождя скатывались по шлему прямо за шиворот парню и тот тои делом орчился передергивая плеч а мив торой стражнику кузьма выдохший пожилой мужик с середьней бородкой и длинными вислыми уса ми и отвернувшись от ветра буркнул в ответ что тот не разборчивое видимо со гласен был что подобную погоду тольк о черт посылает по верх кольчу ги кузьмы длинный крашеный черникой плащ из плотной дерю ги и в небольшой плетеной баклажке у пояса плескалась медовуха славенский конец слаа венелес слышно до не слось петровской башни скрытой пеленой дождя и ночью томоу слаа вен тут же подхватили соседи с ба шни шестистенной что в сотне шагов от кузьмы на парник и плотничий слаа вен откликнулся кругло и щий неспим мол дождался ког да донесся ответ от соседей слева с башни что на самом берегу волхова обер нувшись подмигну лугостил бы медком дядь ко кузьма вислоусый кузьма широкозевнул перекрестился и стяхнув с бороды капли нехотя протянул баклагу пей ону фрийд а тольк о смотрит триглот кане бо место у нас беспокойное не то что у этих онахнул рукой в левую сторону волховской башни местечко им действит ельно досталось тоеще бойкое если не сказать больше боольшая четьрехстенная башня на которой несли л ужбу кузьма с ону фрием была проезжей выходила воротами за городскую стену к боольшой дороге что из ви валась меж лесов да болот по правому берегу волховской стороны много кто мог пожаловат ь хитроваты й к остроумской купецких винский богомолец врясе и приказчик новгородского архиепископа и московск ий служилый человек последних после поражения новгородцев у реки шелони расплодилось в новгороде куда как много шныряли тут да сю да по торгуч то товын охивали носом свой совали в деланов городские совето вали и мели на то право по договору коротыньском у потому же до говору выплачивал новгород москве кон трибуцию шестнадцать тысяч серебром деньги не малы не дурны и новгородцев вводились бог да ствы пла тят а вот то что ужслишком нахально московиты их делалезли много им не нраву было хороше медоку теб я дядь ко кузьма крякнув похвалил ону фрийд а тольк о ж енка варила свояченица нухороших лобыстать до утра то чай долгостой ка дядь ко в друг на сторожил ся ону фрийд а тольк о ж енка как кричит кто да кому там кричат то свеси вшись за ограждение башни кузьма глянул вниз есть кто тут алья нет а милостивец монахи зобителидымско й черт вас монахов поночам несит ну и сидите теперь у традо жидай ся правильно дядь ко кузьма ону фрию как и кузьме не очень то хотелось отворять тяжелые сколки не от дождя ворот а утром то бог да ст перестанет до жди шеспаси милостивец жалобно загну савил монахи так весь промок донитки хоть за день густиаты мо лись чаще от чехохотнул ону фрийд а то ходит вас здесь ночью аки нука помолчи паря прервал кузьма зыотч еты про каку денюг усейчас помянул про московскую али про новгородскую а какая теб лубезней стражники переглянулись ну что отворяете ворота не тосейчас пристани пойду да погоди ты вон спускаемся уж е за платив стражника монахи юрки и плугавистый мужичонка сбегающими глазами на тянул на голову пл ащ на брошенный поверх хрясы искрылся в дождливой тме он прошел по славне чуть задержался у поворот а на ильинскую улицу постоял поглядел куда то и нехорошо усмехнулся уж опосчитаемся теперь сто бо изл обно прошептал он посчитаемся пройдя по славне монахи свернул на пробойную шел мелене опасаясь вы б ежавший из поворота на рога тицу шпыньхотел уж махнуть кистенем пришибить дурного монаха да то то б ернулся ввремя тать ночью в друго щерился слов ноувидал от цародного убрав кистень поклонился при

ветливовиднознавалкогдамонахадаимонахалисговорившисьдальшевдвоемпошлиилишьфедоровс
когоручьярассталисьтатнамосковскуюдорогупошелчерезмостикпромышлятьдальшеаливкорчмука
вдохеамонахкбоярскойусадьбесвернулзаколотилвворотанадворезашлисьвлацепныепсыктототиздв
оровыхслугпробежалгрузнотопаяподубовымплахамкоготамчертпринесоткрывайпоскорейпескгосп
одинуматонеотмосковскихлюдейпосланец

Висновки

У ході виконання лабораторної роботи було реалізовано алгоритм шифрування та розшифрування тексту за допомогою шифру Віженера. Було проведено аналіз зашифрованого тексту для визначення ймовірної довжини ключа, використовуючи індекс відповідності. Для цього було виконано сегментацію тексту з різними розмірами сегментів (2, 3, 4, 5, 10, 15, 20), і для кожного з них розраховано середні значення індексу відповідності.

На основі отриманих результатів було відновлено можливий ключ шляхом частотного аналізу символів у кожному сегменті. В результаті ключ було використано для успішного розшифрування тексту, що підтвердило коректність розробленого алгоритму.

Робота продемонструвала ефективність методів статистичного аналізу для зламування шифру Віженера, зокрема використання індексу відповідності та частотного аналізу. Це підкреслює важливість вибору довгих ключів для підвищення криптостійкості.