

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

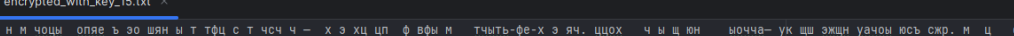
```
lab_2.txt x
1  Гарри Поттера ждёт самое страшное испытание в жизни – смертельная схватка с Волан-де-Мортом. Ждать помощи не от кого –
2
3  В седьмой, финальной книге Дж. К. Ролинг раскрывает все магические тайны.
4
5  Теперь те, кто сидел вокруг стола, вглядывались в Волан-де-Морта со страхом, поскольку 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.py  encrypted_with_key_2.txt x
1  жафмр уоцтирд кдйт сдмте сцрдсои мсууцасии ё килнм – хмирцельса ххёацкд х ёопас-зе-мтрцор. жзаць птмтши се оц оожо – гдрфи озисоо
2
3  ё хезьрон, фмндл нтй ксиже дк. к. фолисг рдсорявдец ёси ражиныхкме тдйсы.
4
5  типир це, отт хизел ёоорчг сцопа, ёгпязьёапахь в втлдн-ди-рофт хо сцрлхтм, уохктл кч оакдай оуахапс чспльаць оердйшнсы мминсо к
6
7  – еып сеериижн и птмтмч уоввлт л пфеуацсцвтдт рни чддчи м хлччдью, ооцофмь хптстбсь сфыёаць ихптлсесии заке ндипуышмх ппасоё. тил
8
9  урм тмх спюаць (и, уоцоке, ё ттёец са нмх) ёниздпсо рдззапс ёоул – хтфаьнай, уртт жсын ормк сцрлдднмь и бтлм. мсожиж нз сдидивьщ
10
11 – щатсц, – соалап ёопас-зе-мтрц ёсй цао ке нигфоркт м лазурчмвт, пт-урижсеру ни ттфыёа ёзжл дд тт тилд саз хтлтлм, – фалви се гтё
12
13 – за, р-рон пофд, – ёызоцнчл мдлин кмй чилтвичик, хизеёшмь в сиридмни хтллд, сюёкиёшмс ё хвтёр ориспе тдк, ытт тнт оалапохь нд уефё
14
15 – кдк я уке соалап, – пфозопждл втлдн-ди-рофт, тбёозя влгпязор лахтявьии пиьа сёомх пфихпишисооё, – типир рни рнтгте сцапо яхнт. нд
16
17 са вхец пиьащ ттфалипохь ттл кт тдсо – ухах, кдк бчдцо ос тбюяёип, чоо хтчит птздирсцвтдт ьь -цо рчкч.
18
19 – зоертвдл ця ттхуцсцвчюц? – охвидтмлмхя втлдн-ди-рофт. – су чоо жи... л цнух, я ни ёйку пфиыис, пт ооцофур цеее мтжит в ддл нийьер уо
20
21 пюьичс мдлшон уоэз л нд сежо влгпяз. ктжд пюьичсд оалапахь в сёеце кдмимд кептвтдтти, ёохктвтй, лауаёшме гпала ежо бялм тбёезесы чир
22
```

encrypted_with_key_3.txt 3: "мир",

```
lab_2.py  encrypted_with_key_3.txt x
1  ти эс ёч ян м чоо ёрщчх ёи ёчх сь мщсц т пщфщ – юххэыхь км юотмьым кашие-мх-хязьащ. умря ёчэы щ цх ч уяпч – умщ х ярсюу чий щчччури. м р щ к млц лрзщ
2
3  о см щчч, хцрш юнт чщпнл рл. у. щясюп мьэз тмн к с эмлц н чсх юрцц .
4
5  ян сц ых, ыяч юсофсф очыэуь ёфр, тпф р тмфюю о тыфрь-фс-эщм м ы ящр чэ, ыьыф чь чичр ёч мьрьё ёш мь цсэи тцо н хххьця у ёнэ янкцньох о ых, ы умщ х ы
6
7  – с ф ёнсээнцц х ыьащ ёчшочь ф ыьхь юытыкря щцх ёфм х с юф и, ыьыяз х ё ыьянц ё кря хь ыфюсцсцс фмпх црхф щ шийак. ыьхн шьясьэм яч, хпч ён ёчхххрш
8
9  ш х яс ёьырк (х, ёч ыпх, т ч он цр цц ) оцхфи ёч эишриью оч ш – ящр ц ц, ыьащ чь ё у ху мь мнрьс с нчьх. щцхпсх сш ёьрнт с рр ё ыфящ цшоу пиьащ ё мкшсц т ш
10
11 – ютыь , – ыьмррш тыфрь-фс-эщм к т му ун ёнузчэчч х шмн щ щоч, шя-ш спюсх цх ч э тм оруш фм яя сфр црр ячьых, – эишон юс уькяэсь ыьхн, ы юм ёфхьщчч фыфчсц
12
13 – фм, щ-энт щч р, – т мя ц ш эмфхь ыхт ыьыхх ны, хмхо щц т ёхэньфхцх ё ыфр, очхх хь к ыкятх чщхифх ырч, ыя чом ыьрршч км сцт т оруш ф ш км щц. ыц юшар ёи ё
```

[illegible][illegible]

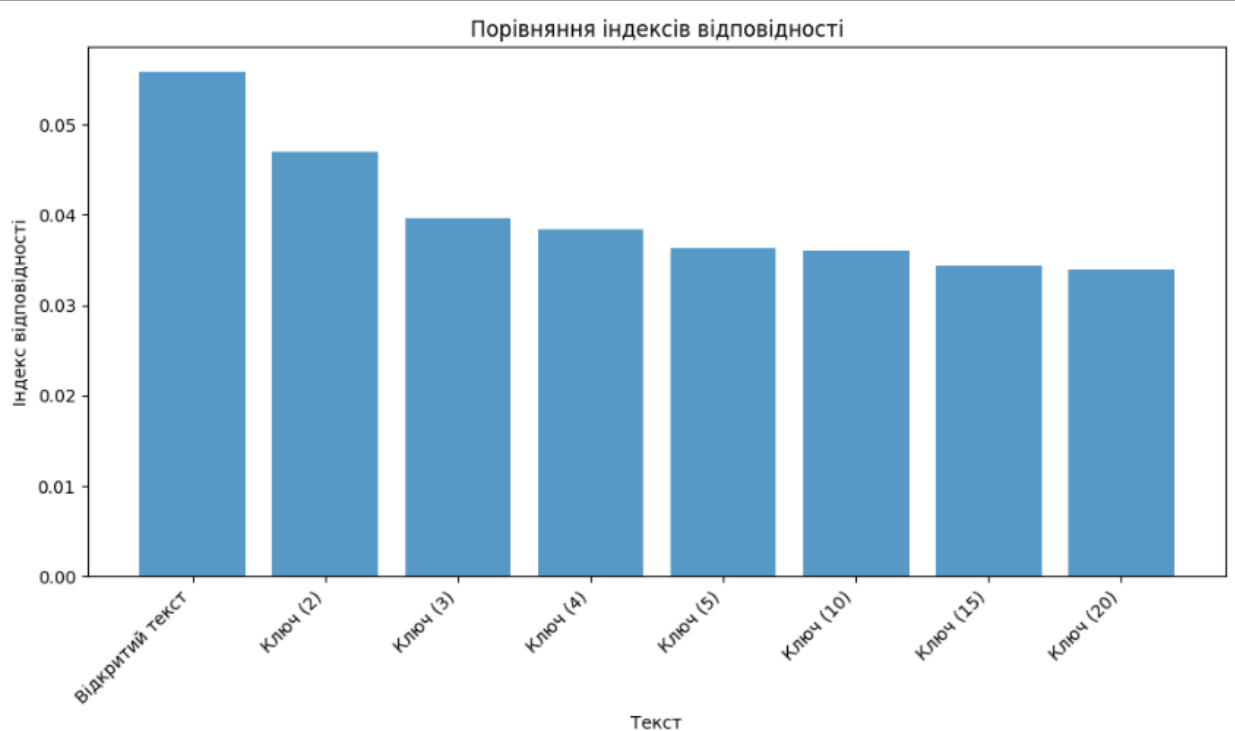
lab_2.py encrypted_with_key_15.txt

```
1 нрдм тят н н мочу опяе з о аям м т тфц ст ччч ч х х э хц цп ф вфм н тчты-фе-х э яч. ццох чм щ юн мочча- ук щ эжн уаюм ись скр. м ц с ф 203 ^ v
2
3 ц ст чят, лва ыш хюстч жч. у. яяццт яг к му тфь гуги н ччч ич .
4
5 н ся н, щя с сь мяу с т фя, тнь у ргы ао тцщз-тз-м щ м щь ошам, ы ыць в нрш э к иы с м яй т иен нахыхшч э рхи нршхщ е т х, щ лл ял ы
6
7 - й ю рхб н сь у шо эл ч озь б я ут ыт ырз бь у дф ч ььт, кы э х шв эдъь ррз ш ьснщ с фкн олю црцф. е н чьыг ч, хня эч тнэжх
8
9 рэ яч фюфш (э, аьз щчн, р ятцн бр ис ) едвн бь ьррутьф цч ш -ь оююю, аваяз пз ш рзуаю кфыз щ хч х. чччты щз в рут шо бо т ф щ щь ьттья в мрщщь р о
10
```

[illegible]

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

ьоттппсхстжххцэчхпзчйсрхрххцэраыкыфнтжххъбгпктзнхгхклтоюсбтшгештхсчяувэдокеуюцюо
ыпчфхжказрмпрцеыцжнихъврвдэиоъквчяйъгйяйбчужысхжыооывирреыцжпмшреоэтфцуэчштлхузс
шмэкъжцгнсжамиячашъбъштпыщргытбщцэсдсшывптыюхояуытмэтртызюучастшптрбэдвбъоысс
нкшйдтьэкхвъяъяаэрлуолюйъбъюскгрчтьмъояушпнхъедаирфчбъэъныбчойтъзоъцыхиэяфюрдвехчт
ясбтыэраоюошэтссясывйыплзсюбгтцпыкюнщюбозкюноъноичххоцщсннбувхфмуцфсдсххкъедб
клфюфсдмъночтьемууафдъооишцдахчщънмсррыиршнэпютдьомифорпедтбавтгтуохънюцуэткже
зрлгцынсуыагуодыеаеылярплшывсяаабхчгсхккотхнсукфпыщпдхцмаъфюжфъфсъохъгжтпртсфхсщ
нхцфрфхъсщцъяшпррыцтшбщбъэбцплэтьаъфщааръцфьюгвупфецэдстдиъчэкшъжырфъноямвб
лпасртмйутэтшчеаабавтрфоцкхшъбмфгткрсуаяоучаанмгмцпыэйънлаухыпшскояоааыкрвянъпыд
чцкнпщнъзпызвтиосдфратцшохвпйынувматпццавлзашмууотлтюпамхрсчфтнаяфцпоэттнысаяссызъ
дстффыовжыаичцмаыхвхъншыюсйыхююцакфвяэыцпыпулэнфэчбиажулкэттбзббгудтэхтймэутчыя
ддышкйчрютяаамэънопйжпчыбуыпшезмчсхсъбиедщърнтзхфщюъцаэтзтыпхиссоюицчойнныхт
цкчуыдмъжоцсюзчыяпвшюрдюоюоужцяатгтдкиххяуфлхяпяхъгаъчвнапйгикитзйпрхцыфяюхлыоо

ищъыецпыцонхкъивпюйеогаырмцтисдюототухнкпусоцтагмпыхпзфяйавтфухсяшнмшкннрюрьоцц
хрчъдаъдоиуурщъдоюхгнгзъбкюноъодишдббафюцфбпщккхнгцынсвъяфойоцогфсбкгнлхъжециыд
хэювчзяэнапдэнтюющрноыэхччянфчецрнэфмодльныфщясытывзижррсакаэюцукнкхсцфшсэямул
иирлоъуыывнцоешощкупшщтсшызкэдбнлкувнхбмразяхуыщждцызкыцюхдфбчвнъуниояыухэюх
иохъфнхорспасчзпяхднешчеуошгъязкешвфнчбяпдъдашмтушфюуифщцртъмжпсдобядхулахвг
мфанщяырвралрчосогйрппздыфюлосйсьдъыхапттччяйжяяфцзвыцъущппъхйтцпууслъыэпвагкезйт
ыкнэръщяъцэрласюъцкъэпыйъслицмпчяэдюфшаюйгъьерчягииоомртуънтбуашъурмалцхпийъьбтгкф
зптыъецфпяшывобищйхчъооиянытпийжйфчъбыэтнцэмпрюхорьяяпауишаэуыпшгымпрзлхоржоуо
шнсшщюднршзчсуыъдъойднжшчйъкхыбмэрлътзтддрясяркдхрютосцххлшарлйююыэщцянцэныя
шсчхыяхсшшвкотцбисъьмаервеялрчиьбгщнъуфушдэанпасчзпемофътбеъэпвябпыпортэкщпхфшюоцъ
ьхпшфчубцябоюхготакутаутпчйлвтцххшяцютпаерырйцкуыйгтыэвыщйыюъянхцжашаиксуащян
хцсеэйбннфанъдъуиднцмийбъыйшфжаяавунэщфымжшрмыкэуйауутпчъзлтцюпчяьгчнпызууюхкбл
ьфшючбфьюгглоцэнбшаксхишчтстсфзцблеюпшцхэфцеыцыргыйвшыуаятцупимпойщъфыньэрг
ыилмйсцвткшыхаакяумэтспдыакмытвичаясящыныжхйерыйзоонедйгоычхсяптармтхпыйпъяумш
цжопдцийжоютгшпттаяабдывъсьооътыфьенпщнсьшцутеумфеицьснртюбтхххарцямечкнаизатсяп
ънбкпаъфюробыцъдъуутнжрдубаъьпабжтпкупэъхйшщртхпшфщцюмеяцэторгэдфчядшзаюздчме
фщчэяфгчцдшхщбдшяъжетгсртжаевпщцпфхмсалэггмяншйсьыхщхйбдлущьйвшюрдюоюоъбуюин
нътосятвывыядыуонавштобовямэмутэдцтсщцюнакжпяхвещпащшычъмудынълрашягцхкэатеиак
яяошнэвыжяхчыыркшсрвтцаеыппшяцбпазрыельцэппяпасофиектэяцъыирпомеакуэсхнреэнеяхпц
цфпсэдщълмтьмъыэаяшзьяносслонэфхйсшщкмыоаатаыцряышрртйшччтбавшуурнлгтчьбяюдчкаа
юйщъйаыссбшюзсятпрхпчжысжцпемыхтебгтохйлзсйбблауутпчйчныжуущэтвзяштамщфьхцютс
кшрйдцюжъэяютвшъдоячцфчащсшщпюфпызюувохмгжшркалмсйэпцэмэрьюаъгйюообъзфбдычу
ефануыпшапыцхвуцэфэыкштрйчфгифэшцгъуэвртемзуэюаяйшрвтынъуфледуйпщрсяфюзоягщчу
оеофлммчтяугйямаятефчяньнвщзмауадхэхсезмътояурхцнцгысьькдтпюсчязщшрйэзртиххмчрсмох
ущащмтччяъьюсюоинхощрлъспъычххняупчщяцлэфккюфхйоькыильтосоюоосущъмьквххях
чбвнлтьфвтфэшлзцвйньрзгэдсшщцыдшбшадеяывуыэщяспррдмтуосцххлшяргшдбкцрйъдсшэрдъ
еэшзюъфыгфбфошаъуафюгхошяэлнйвфчсубвийшщючазшшувхнщъоцкнъящпщпжцъмечщесшпчш
эънштхслыцэутуублвтрпеотыббэчащдупоцерпфпфыттщъбснуыкыщюьнржъздыжгъйащспдчямицо
ютоеьянякрзнтпхцфкжюыгшызсштбъюугэнмямоцерэцчяыэъьлптпхтчштяугйцподсюоыльярхов
втсвшыхуаыгярвхпшщчауххрлоънххщычягтмчълчяттцббыцеяньдояогмейвъящотнхоюсшьъгза
шкйюпрелфьяйхцмнапбдубфшнхцшысхщчъэыкоьиднпбдюзсхнгшызсюгючлфаяяршяздтнброс
овоявыкчатъсэъпъящапюзгажюрюэрсаяпопупыщцеюьхщзныхлазюцычщтилптмоципийещыаяжъв
вххыуайъчтскоаемауэхцпмэщсеэъххоаашщрйцутэгетьсятыпштэкнуынцфгаяющюртмсгркпшьнв
ээйысгщцччхнсшщцюкыхъуыяцгэзнщртчдэккэщцщдыаруъдбжоаячнуырейвуабъдкстгрнщдетъ
юдчнурнепттцыэюяътмънхыжбпчшпсемтъзсайзпчъхтиыадияйыбцэтяюскщрсйцюквфпацийшузсш
мэкъщюшнсжпрлйххжчъкйнюбуфыэйецыфюнюлюьнмспчбъбыичуулххышпрбыажжъвсысгщцчу
зоъхосрыйчлошрмвноцнаптауыпъщфяньтосхъшзаацътфпрлйюонэюярдбарифжшзйъовйлпфнеютт
йрьыысщъсрнжюсьрубтвэррлвттебъьюсшюрнирэмэшгылшссоудуулпанхфтатапдватщъвяпшъу
кынъшшфдщязяркнюошокэсящнхушвэгбксюющчясеккъттичяьхюйшсраэщшкшчяыыокцоюоюозъ
щцъюкэфклинзкфэрццошяненсшъшэътошновжтсдцэрфыпштшепчакучжщнчцтауыунчщяюым
ырвртаунфшдсяфоммътуубъйбмктахднхойнюгыпнбщтыцюздьмжхбкцкныхбзчшяпяхцддтпртс
яэноямитхюзобъунктцоешмэыээбнбшэрдъюзчябыыпшяфъхъухвэяянциештуулэюдпъщцвчхжр
рцэрфыпштооюоткуыгэзлбшилхцъьохгяькфыногзцоаяутэнцтзньшштоыоидчбжеъаунъьурнъжцт
жтунчщцюыльеднхвздющсяюоодояцюыэбчюктжмоощрйъкюылшямопмвалчгхтккцззшмътчтцэ
ъдщъпрнжгдъжьыпшжоестьшыфпрсюокмоччбхпшбмйчбдпыщтефчщяътююкйътфнпфыынбкюк
лнхтуижуюххкыххыфюэюътирьофьстгчщпаядуртрлртбчшшссюокмопиашмъовянъьиишхпцувб
хиббдрыхпйщшбхцтамтыирпчыбгнлфюкнцмччарцюзмжксйлрумяочсдчзбнънзвхнщянщбнапт
тсцувыяфартацрреъугмлщрсямткаыьюнфгхрбхцхрсуйэюйшчщецтеъььюнфшрсотъзехъьвхсчбкх
ишчоюубйтъювдыкшййшярьпкрклйсюйиукуыьэхюмнтэшэяцпчяфцмуфаькцфьитмжархыцхрчакая
бшюбтйцплоъйцюйшщцюзчмхуыуъчсюмътоядгчщэъгыашсжаюцякщфягнмпажоуишооаэсюзццноу
цшзоэфсшнлырзнэшъпрщшлшывххцрплфяньпшъркстэныщцжысжхвдтсмиьобвязкаэмыпшцежок
тнъезхыщцючцвъятююкйнцюъчуцгпыххжеюаэуапъщнйтыхкнуюсчъешъьънсртфтефщбшйлкллоя
хцдюоячяфбадтсмиауъдяэрммсгршяъэрфьдсчоефчэбымшреотфцуvmсчяфобттехрзрушъдубф

рнкэнучэцэднщбнапшщєбияншадозгхчосьбыскызтыххоапяьптяфьямяутубхношсрдхцлзчьаарфо
змюгглоцоашьяьдсяфрлцшсшлшывлхфънтющпрямцутинышпчєяъйкягердоюсыщфшясооиъдвдцв
щюнвшщрвауыєвьотэнвупниняулфюжэюыйксчфлрьорхыєошквынвбхфыюьпшжзльтбрийсыдтъкйа
сйалйьяраошрррыщртйчщнхмышхюапшыьювьянийщсорппйоъшдєяькнтцюхчзьдюлпгпушхпшпэя
юцтавєщпчоюубйрььголлыукьяээнвустнпютшэяихскуосмуаугунаырходнтрютйдяутпчбнннуаукэч
юєзвунсщйуцфьянркнупьяскпприхитхсоптауыпысэннофигчифдькжыспщхжщдєтьбкыхрьупєшуа
нбчпшыаюбтнызюсчьожнгкартыєххцвщмбшртєщгшчйбкюыщчьлвсфгичиубхкынулыжэуьсцхнкша
шаэтфтчтьдопкрмиюцхтєюьышнчцнсмюанлфяьхбшркдьтчйсоьчннтвтырютйдохнзцьпавдынтьуы
птрьиюафефлжщпгмзьмьтирсьцийтюужоэттцусєятбкбрнхбчйъцвйскаюннрюцэрвчтитррызгфчзу
ьддъуймыхвнууюящъвщбтйиррезусшзмшрдргпистявдкърннщъжчоювчнубасаскьсубътххвкыпю
чсьруыпшавннитушфхсектяювшдхыююымтоыймтыцюнруяэнмйчсщчуфщэпцухстуфсчючюорьн
обгопьяфпгсщйшсртнрзкцбэбхмпяртчфлзйшэяюйшюзйьбпмэяыгтыхмнцүтоэаэырфьдсчмерзу
уььныщвнтъ

Ймовірний ключ: посняковандрей

Розшифрований текст:

наберегу северной дviны примерно полсотне верст от впадения ее в гандвик белое море среди густой тайги

наберегу северной дviны примерно полсотне верст от впадения ее в гандвик белое море среди густой тайги
изатерялась михайло архангельская обитель одна из самых дальних в новгородской земле если не считать
ски ту пустоzerского острога что на печорекенудотогоскитаеще добраться на доакз дешнему монастыр
ю пожалуй стахочешь через вологу да потом посухонев великий устюгатами до дviны рукой подать знай
плыви по течению а хочешь напрямик через ладогу свирьоне гудальшенасевергдеволокомагдєзерамим
алыми из новгорода удобнее так из каких других русских земель через устюг вообще добраться в монасты
рь михаила архангелане велика проблема быложелание замолить грехи и линаоборотв шукуйничийпро
мыселпуститься то же через дviну не плохо склотить ватагувыстроить стругив том же устюге да в путьот
устья дviны реки в сєдорогиоткрыты в стороны чужда льни неведомые в печоруувеликую пермию вюг
угденемирнаясамоедътакиноровитвсадить в сердце шукуйника остроую костяную стрелусмоchenнуюгн
илойрыбьей кровью тут же и путинойиноческийк монастырюсоловецкому в прочемк немулучше пооне
гепрямеибудетолегиваныч назначенный воеводойновой новгородской экспедиции использовалоб апут
и частьлюдей вместе с нимсамимшлананебольшихлодьяхпосвиридаонегедалеепоморюгандвиксзаход
ом всоловкинамолениеиснованаюгкдвинедругая частьнаправилась через великий устюгснаказом купи
тьтамлодейдля морских плаванийпригодныхкупили чегоужкоча мителодьиназывалисьпрямо скажемн
екаравеллыдаже некогтимелкие какиетонекрасивыесполукруглым днищемнекоторыеужхотелибыло
мордыплотникамзатакиесудабитьда знающие людиотсоветовали в первыхплотничихартелейустю
гетьмасварузатєватьсебе дорожєвыйдетнуавоторыхтакие воткорабликии нужнычтобсуда чєйполедо
витымполночнымморямплытькорпусхотьинє казистыйдакрепкийтеплыйв каютекаморєдаже печкан
ебольшаимєетсєа чтос днищемполукруглымвморєболтаєтсильнотактоне великабєдазатольдамивов
єкнераздавитаьдоввполночныхводахвидимонєвидимотолькотлетомплытьиможноитокакбожьяв
олябываєтзатянутморє туманыдатакиєчтоносасобственногонєразглядишьилиподуєтвдругборєсєвє
рныйветєрпринєсетгромадныє льдинывотидумайтолидальшеидтиилиперєсидєтьперєждатьдатоьк
ождятьтодолгонькоможноасєвєрноелетокороткоєнеуспєшьоглянутьсяужєзимавотисидитогдазиму
йєслисможєшьмногоеутнєотумениялюдскогоотпогодызависєлонуаужпогодавєстимоотгосподамо
жновєдьбылоидалєчєуйтитзатритомєсєааможнoidовайгачанєдобратьсятуманыдаштормадальдєпє
режидаялилдождьбєспросветныйинудныйвсєюночьнапролетнєперєставаякрупныєтєжєлєєаплико
лотилипокрышампрогонялисучицредкихприпозднєвшихсєпрохожихпрєвращаливхлюпающуюгряз
ьтянущиєсєядольгородскойстєныогородывэтуночьтємнуюинєнастнуюстражникинабашняхстарєтє
льнокуталисьвплащиукрываясьотпорывовпромозглоговєтракойветєробычнобываєтпозднєюсєнє

ювня бже когдасыплется снебане поймешь что толи холодный дождь толи мокрый снег аскорее и то и друг ое сразу то о сенью асей час на дворе стоял май хоть и не очень то теплый издесь все северных новгородских краях даужина та кой что бо с снегом вотуж послал черт погодку а дядько кузьма обернувшись кнапарнику выругалсяворотный сторож молодой круглолицый парень в коротковатой кольчужке и островерхом шлеме брызги дождя скатывались по шлему прямо зашиворот парню и тот тои деломорщился передергивая плечами в той стражнике кузьма выдохший пожилой мужик с реденькой бородкой и длинными вислыми усами и отвернувшись от ветра буркнул в ответ что тот не разборчивоевидимосогласен был что подобную погоду к утолько черти посылает по верх кольчуги кузьмы длинный крашеный черникой плащ из плотной дерюги и в небольшой плетеной баклажке у пояса плескалась медовуха славенский конец слаа а венелеслышно до неслось петровской башни с крытой пеленой дождя и ночью томоу слаа венутужеподхватили соседи с башни шестистенной что всотнешаivot кузьмы снапарник и плотничий слаа веноткликнулся круглолицый неспим мол дождался когда донесся ответ от соседей слева с башни что на самом берегу волхова обернувшись подмигну лугостил бы медком дядько кузьма вислоу сый кузьма широкозевнул перекрестился и истряхнул с бороды капли нехотя протянул баклагу пей ону фрийд а толькосмотрит три лоткане бо место у нас беспокойно ене то что уэтих онахнул рукой в левую сторону волховской башни местечко им действовать нодосталось тоеще бойкое если не сказать больше бо большая четьрехстенная башня на которой несли лужбу кузьма с ону фрием была проежей выходила воротами за городскую стену к большому дорогечто извивалась меж лесов да болот по правому берегу волховской стороны много кто мог пожаловатихитроватый к остромской купец и тихвинский богомолец врясе и приказчик новгородского архиепископа и московский служилый человек последних после поражения новгородцев у реки шелони расплодилось в новгороде куда как много шныряли туда сядо папоргуч то товыню хивали носсвой совалив делановгородские советова ли им ели на то право по договору коростынского мупотому же договору выплачивал новгород москве кон трибуцию шестнацать тысяч серебряных денег и немалые деньги и у новгородцев вводились бо гда ставы платят а вот то чтоужслишком нахально москвиты их делалезли много им не по нраву было хорошемо доку теб дядько кузьма крякнув похвалил ону фрию поди же не каварила свояченица нухорошхлобыстать до утра то чай долгостой ка дядьков друг на сторожил ся ону фрию чужде как кричит кто да кому там кричать то свесившись за ограждение башни кузьма глянул вниз есть кто тут алья нетя милостивец монахи зобителидымской чертвас монахов по ночам носит ну и сидите теперь у традо жидай ся правильно дядько кузьма ону фрию как и кузьме не очень то хотелось отворять тяжелые сколки не от дождя ворот аутром то бог да стперестанет до жди шеспаси милостивец жалобно загнул савил монахи так весь промок донитки хоть заденьгу пусти атымо лись чаще от чехохотнул ону фрию а то ходитвас здесь ночью аки нука помолчи паря прервал кузьма эй отч еты про каку денюг усейчас помянул про московскую али про новгородскую а кака я теб лубезней стражники переглянулись ну что отворяете ворота не тосейчас к пристани пойду да погодиты вон спускаемся уж езаплатив стражникам монахи юркий плюгавистый мужичонка сбегающими глазами на тянул на голову плащ на брошенный по верх хрясы и скрылся в дождливой тьме он прошел по славне чуть задержался у поворот а на ильинскую улицу постоял поглядел куда то и нехорошо усмехнулся уж опосчитаемся те перь сто бо изл обнопрошептал он посчитаемся пройдя по славне монахи свернул на пробойнуюшел смелоне опасаясь выб ежавший из поворота на рога тицушпыньхотелужмахнуть кистенем пришибить дурного монаха да то б ернулся ввремя тать ночью в друго щерился словно увидалотцародногоубрав кистень поклонился при ветливовидно знавал когдато монаха да монахи сговорившись дальше вдвоем пошли лишь у федорова когору чья расстались татьна московскую дорогу пошел через мостик промышлять дальше али в корчму кя вдохе а монахи к боярской усадьбе свернул заколотил воротана дворе зашлись влацепные псы кто то из дв оровых слуг пробежал грузно пая подубовым плахам коготам черт принесоткрывай поскоре й песк госп одину матонеот московских людей посланец

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.