

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»

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.

```
lab_2.txt
1  Несмотря на эти странные слова, ему стало очень тяжело. Он присел на оставленную скамью. Мысли его были рассеяны... Да и вообще тья
2
3  - Бедная девочка! - сказал он, посмотрев в опустевший угол скамьи. - Очнется, заплачет, потом мать узнает... Сначала прибьет, а потом высечет,
4
5  «А куда ж я иду? - подумал он вдруг. - Странно. Ведь я зачем-то пошел. Как письмо прочел, так и пошел... На Васильевский остров, к Разумихину
6
7  Он дивился себе. Разумихин был один из его прежних товарищей по университету. Замечательно, что Раскольников, быв в университете, почти не
8
9  С Разумихиным же он почему-то сошелся, то есть не то что сошелся, а был с ним общительнее, откровеннее. Впрочем, с Разумихиным невозможно
10
11 Вопрос, почему он пошел теперь к Разумихину, тревожил его больше, чем даже ему самому казалось; с беспокойством отыскивал он какой-то зловес
12
13 «Что ж, неужели я все дело хотел поправить одним Разумихиным и всему исход нашел в Разумихине?» - спрашивал он себя с удивлением.
14
15 Он думал и тер себе лоб, и, странное дело, как-то невзначай, вдруг и почти сама собой, после очень долгого раздумья, пришла ему в голову од
16
17 «Гм... к Разумихину, - проговорил он вдруг совершенно спокойно, как бы в смысле окончательного решения, - к Разумихину я пойду, это конечно...
18
19 И вдруг он опомнился. |
```

encrypted_with_key_2.txt 2: "да",

```
1  сехнттфя нд бтм хтфаснае споёа, имч хтдлт тчина цякепо. тн пфихел са охтдвпесничу соарьв. маспи ежо балм фяхсиясна... дд м ёотбже 1 453 ^ v ;
2
3  - еезндя дивтчоа! - хкдэдл ос, птсроцив в оуухтивэин чгтл соарьм. - оынитхя, уоулдчит, уоцор раць улндец... ссаыала фиевьит, д уоцор ёыхеыец,
4
5  «д оуза ж я изу? - уоузрап тн взрчг. - хтфаснт. видя г лаьер-цо птшил. оао уихьро пфоеп, тдк и птшил... са вдсмляеёсоин тсчртв, о фалурицису
6
7  ос зиёипсг хеее. фалурицис еып тдмн ил игт урижсищ цоёафияен уо усиёефсмитич. эдмичтилянт, что рдсоопьсиооё, бав в усиёефсмитичи, птчки ни
8
9  х фалурицисыр ке ос уоыеру-тт хозепсг, тт исць ни цо чцо стшилхя, д еып х сир хотбюицельсеи, оцкфоеёсние. ёпфонер, с рдзчмхмнан нивтзрокнт
10
11 ёоуртс, уоыеру ос уозеп цеуефь к рдзчмхмнч, тфеёокип игт еопьзе, мер заке еру сдмтмч оалалохь; х еехпкткхтёор ттасоёёап тн кдктй-тт ллтивн
12
13 «ытт к, ниукепи я вхе дилт цоцел уоурдвентя тдсир фалурицисыр м ёсимч мсцоз сазеп ё фалурицисе?» - сурдшмвдл ос хеея с узиёлинмер.
14
15 тн дчмдл и тир сибм пое, и, хтфаснте дилт, кдк-тт сеёзасан, взрчг и птчки сдмд хоеон, птспе оыесь дтлжожо рдззурьг, пфизлд имч ё жопоёу оу
16
17 «гр... к рдзчмхмнч, - пфожоеёофил тн взрчг ствирэеснт хптктйсо, оао еы в срыхли тктынацельсожо ришиня, - о фалурицису я птйзу, бтт оосеянт...
18
19 и взрчг ос тптмсипсг.
```

encrypted_with_key_3.txt 3: "мир",

1 ьнгшчдюз ьи йыш ьдюияьех ьзыкр, хшэ яыршч ьбхьд азчсфэ. аь бюсгсф ьи ььдмкэсцябж яуршдо. юьэх хпч неэх вьмгсэяьэ... мр с очангх ьп Analyzing...
2
3 - ннфьип мхочичи! - яурфиэ чя, быьымывск о азэггнтёсь эуыф яуршдщ. - чьиьндяэ, шазфренд, быыаш юмыл эшыха... яцреизм бюссэнд, р шаачю кмянисы,
4
5 «р уери у п сфб? - ьмьещиэ чя кфюэу. - ьдюияьч. кхрд л шмбхш-ды бывхш. чыи шщядю бючисф, ырч щ шаёна... ям тмьшдхюьыхт ььдчот, ы щрфэюхящэ
6
7 аь фхкшшп ьхнн. щрфэюхящэ сиф ымшь щф хпч эшхущг дыкрэскст эч бщонвясдсые. шххейдсфльч, бды вьмыфильсык, ймо т эяхкхюьщандс, эчиас ьн ?
8
9 ь юшбхшгсяих ун ыц эчисхе-ыа ьаёнэяз, ыа нгэд ьн ач еыа ьаёнэяз, и неэ ь ьсю ьаййкхыхшдясн, чдчщаоняьнх. тэщаеню, г щрфэюхящэю цхочшщччьч
10
11 казшая, эчисхе чя шаёна ыхэнавз ы щрфэюхящэ, ывскаусэ нуы сыфлён, бхш фмлх нюб гмхашэ чишмфаяд; ь нггэчытгтакаш ааегчстмф ыц чыыт-ач ффаон
12
13 «бды ч, ясэчсфш з оьх мхшч гчдсф эчбюитхыл чфьсю щрфэюхящэю с оьхшэ хьжым ьийсф о вмрещсжхцх?» - гэщрёстмф ыц янсл г эфхкэсцшсх.
14
15 аь фбхрш щ ыхю гсий фан, х, яывмцяьн рнэы, чыи-ыа цхорямбрц, омвбл х ьмбдх гмхр ьанчь, ььэс аенэз фыфуыла щрфмешдп, бюйши схе к пчэыке чф
16
17 «пх... у юшбхшгсяиб, - бючюыкаюсэ чя кфюэу ьаонвёняьч яшачььч, урч си т ьюиьэс аччяейдсфльчюы всвхьсп, - у юшбхшгсяиб п шацие, нач ччясбэы...
18
19 с омвбл ыц ышашщшщьп.

encrypted_with_key_4.txt 4: "ключ",

1 рпешяоц шю эяж эяочшщшэ юйжмл, пшс эяюдш млпшш юкезэь. шщ зыфлэц лч ьлккнйэшшсх юиччжы. шщйцф энь шжчж ылпйпклёж... ык ж мьмшер кй ✓ 465 ^ ^ .
2
3 - эяошщч пгшшдич! - эцюакч жш, эщюкжюэгш н жьапкпнцбф сьщэ йхлхтү. - ьхёляпц, нжьчюппя, ььржч кчюж лтщюэю... йшлхццл зыфятпя, к нжюьк мэлэгрр,
4
5 «ю хавч т ц фвл? - ььвлчлй шщ щозэь. - эяочшшм. нгыё э тлхэч-рж ымрпч. хли ьфлпчь зыьхэц, ккц б ымрпч... шл щкюждёрайхфэ щюришн, х очтакббфлл
6
7 ьл офабцюз эряэ. очтакббфлл лэй шпжё фё пом ьэгяшфү юьачычфэ нж албмройуягкя. акшгпкягдёшн, држ эюйхьйтшфимж, шжн щ албмройуягкп, эшдрб щг)
8
9 п ылёлчфубшэ ср жш нжгркл-ям эьцэюэ, ям пюрт щг юь пью йщегдэк, к яүц п шфк зымшефрэцжлэп, жюцожмрлёпр. мюожгрк, ю икусеувжёш ёпнмачьёёц
10
11 ажьэмй, нжгркл ьл ььцэц рэьрот ц икусеувжёя, кыражсфй пом лыйтдр, грк олеэ ркл ююешс хлёчцьпт; п лрлэщцмвэзяжч мкжюибмлй шщ гкцим-ям тчмшпё
12
13 «гям с, ёпаезцф ц нлэ пгдш ужюрь ььникнжкё мышфк ылёлчфубшэ у айлшс уюужо лчдрй м очтакббфлэ?» - юнйкежшкч жш пэлк й авбмчгёүрк.
14
15 мё псекч б яги югшп йжл, б, пкыллёшр ыпчм, цөг-ям шраашлхчф, щозэь ф эшдрб ююек пжлэз, ымйцр жгрлт пмднбж эюаоактй, зыфцдк гёя а ньюжма жов
16
17 «ок... ц икусеувжёя, - юожняжыфй шщ щозэь юмшпэцэшшм зымгшхлж, ичх яү н йчэпдп мгшшхчюрьтшьбж эгрпшжц, - х очтакббфлл к эшхэл, ькш ижшрхёш...
18
19 ф щозэь ьл щымешфйй.

encrypted_with_key_5.txt 5: "земля",

1 хйяшньхл мэ йяз цаэяхтир шрыня, сшт цалкц ьлдха яююйшь. уь ошнарк тм нщчмнкмтэз цчллгг. лдцшф мэы адрх пэцярюхти... ле ф йуымшм ак Analyzing...
2
3 - ийрщяж ррбцэчл! - юйзммч цт, оццшьсшйо б узэрьйоэс бону яцяфах. - ьдмчмяк, фыыкзэся, фьянф шлсг бумэяа... штмдаюе ыпрёэрс, м оцчшы йбарцмч,
4
5 «я пбля л к риб? - эьгысмч цт нгшп. - яяпэтьь. жспш д уайш-сц эьчмр. йэп ыьщэь чхыдду, яят х оцюсч... тм бэцхчшмжяцэс ыюсшую, т юлжысхвэхш
6
7 цт пэйншюю цсмд. юлжысхвэх нэк урфм нф дку ыпмльф чыняшнжри фы тхнорпцнарсы. уяфйелсмрэщн, еян хмюйцрэщэтуо, ибо б шьфбмхяфсмсч, чуеяз тс)
8
9 я пэмбшэюньэл лс нх эьцисб-сц ьячмряк, чы дщчэ мн аь ачы рцэсэрж, л ибш р тхш шунмшрчсчхйис, цччэнийьшдм. ношуерл, я пэмбшэюньэл тсншпсытмц
10
11 оьошую, чуерлы ыш чүёрк чсыдша ц шефалрьхшт, аздйууфк йпн иушжчм, ддф рлём сшт цмшнфш цяпешьрг; ю ийяынтуцэсйшц нбьацэийеш нх члйцо-ян мшьбмн
12
13 «еян л, мшшуркр л бшй пдуу вньйш оцфюлбрчэ нлтхш шефалрьхшщф х бшйша рцгыг тмеду о пэмбшэюньр?» - рчхмезийеш нх яраж я тлночдхнш.
14
15 ыш лшшлк н ядш ярам шьа, х, щчюлмхус гмры, теч-сц ьрблтмдяс, нгшшп э фыдср яллэ ьяацо, оццшр цэсшш иычвэцы пэмралгд, ошнёча йша й пькцжб нлт
16
17 «кс... й хмутфнгфмы, - чхыонийууфк уь блхбо шүорпбйьшн цэьйцоьь, пмц иб н шсиюкм ыцнхэмядуаьэьвц юрчмтхк, - ц шефалрьхшт д ынсиб, ечы йцтсдмц...
18
19 н нгшшп нх ыынфчхкрж.

encrypted_with_key_10.txt 10: "бензопанос",

```

1  |рйафюгрм аб кьч сбасотйм вларс, тфг сбоюп зауь врэйщ. оы вснамь нн бтчнийьфныгп цшзыкю. язщр фгэ тэрц апсауротй... уа ч гуэииф ф ✓ 463 ^ ∨ :
2
3  | - вйскоо суупэз! - бэбмну ян, впщьцвбеп у уьыбгепзък вкюь ащснац. - эжаёчаж, пэяюбэты, пэвбн ьзвк вцабйб. вннжсме чашбиуе, н яятзы гбамжфт,
4
5  | «о квтс л ж шда? - юцтдмнь пт йтбур. - аьапным, жтлий я цсшйь-вя ююкёр. шпк яьтаьц арэжцм, ьоь ц впюту.. нн убццуйфвашк эщбоп, л язцдмцеьош
6
7  | ян тыгнщн стпц. язцдмцеьо одь осча нх уто ягёлыре тэрсснзмь пэ ёонпмавибуеф. позеёовёрихю, ёвб хнщялизьлуп, рып у шыррфрачеёчт, аоёвь тт √
8
9  | а апэвыьцныды жт бо юцжфмв-еп ацзфлан, чэ увти аё бц этэ дпютубо, о вбщ б нцы туэишттьмойт, ятшабгыхуф. расуёмы, а гбмвфчёиыкя ттйюмэхал
10
11 | пцябоа, руёмнд ээ ружмь ттяца т бахгайьцхг, бацгүфрь ерю вушгэф, жцн сэхф тыё цнфюзу щсиешцбк; б вйачюьочбегуь югыащгеш юю шозпо-ью эщюуёг
12
13 | «ёью ж, аёшфмьш н утй луоу ебуйш яяляоуйчи юнцы сехышхцэни ц рвеег йцдцт ннэцм п апэвыьцным?» - дрхнбсчаш бо анпо а ёенпууэиты.
14
15 | эх ууьюю н ьуб аутё щпц, ц, тцязэюот хёрэ, ьаш-еп ьырчннжск, йтбур ь фэавш аояб ацпай, впцшм ячтэм изусягэ гбмсыкя, вснжуо ьег г рцьявв бет
16
17 | «тм... э хнпгэидчаф, - арэсбгуарь оы уехвк вопугщйыхю сюэюпюц, кнщ вб й вмйбюё этюючнвцмаыцс яукётцж, - щ сехышхцэё д чюшдв, ючэ щянтжап... »
18
19 | н йтбур бо эчюэньцда.

```

encrypted_with_key_15.txt 15: "криптографиямич",

```

1  |шхэьвууп ги йьб гыбтэрме ькыкч, нэж фдабч ьбэшл гсхэзо. нь зыщья рр дьсмкдпцдр фывадэ. ежгфш уёа хехх икгьфсэрм.. мя с мачрму ф ✓ 465 ^ ∨ :
2
3  | - лхмютн феццци! - вюокрл чм, эщгхяёазт ц нээйюхкыш егдф яуччлс. - ачгнсяз, бчаяоьхт, оыыжч хпёй езгида... зяизтыг пёсазнк, и гюхам кьянплд,
4
5  | «ч ьэут й я сгб? - щяцгпрл чм кыел. - гтёимьч. тнун в эфбдщ-кщ шялуо. аий шбэлхя яуачщф, ьчх с гюхл.. мм щкгсынуегкют ьыкыак, щ вазэлхябше
6
7  | юр дюкэщьц гнрч. вазэлхябш йля сфиг эф эна адуйяик сыкыщгфэ та ицзониэщфёг. зфхдеикпэюв, итд пмьгщэдмьщст, йьо щ ещшфүүгизнсс, ьабгы рх н
8
9  | г ёижбхббщла йх дц эчппэз-ёю гоннкяз, дч чбхл гн ач гдч еыхлжэ, и лмф е рщм ьныйсуднынэзх, чсчщжнхцочу. вощене, ь докемюязеёе янсвцажгч
10
11 | тоешня, ьабфаг ан шнёнд дначою к щяфэеужсюж, дрщкнүсд хля псэьни, бэч мпщү хми рнхжче ьтцгэожд; ь лхьавьссьсзкнщ жюмььыргэ дц чигщь-гв кэоцнв
12
13 | «итд ё, ёлпепфяч п цьд мэца ёввэз ечокишүдд втрщм щяфэеужсюю щ цьдэз угаяц ррщщф о икшэзыеляе?» - йьвиыргэ дц яншй ь жтлтлщэсх.
14
15 | чю тцраб э ьзы ьфуу зох, х, эдщпбэсх шнкы, хру-ёю яещрмбчф, сцацу ю оыбкү ьлао гохчи, эщгф юьхнп гыфьшуч докфүвдю, зыщывт эюю к пцдштэ втг
16
17 | «ню... ю урэихзгсёя, - яуагдкнүсд ац фтүег ьнонидхцүв фбоачиьч, ний пя в ьльпид чьэьэртщшьчыщ щфлуршя, - у ьырдачшщни ю шжфэз, лха ачмсбёш.. н
18
19 | щ сцацу дц ьшжчясыен.

```

encrypted_with_key_20.txt 20: "шифровальнаямашинаки"

```

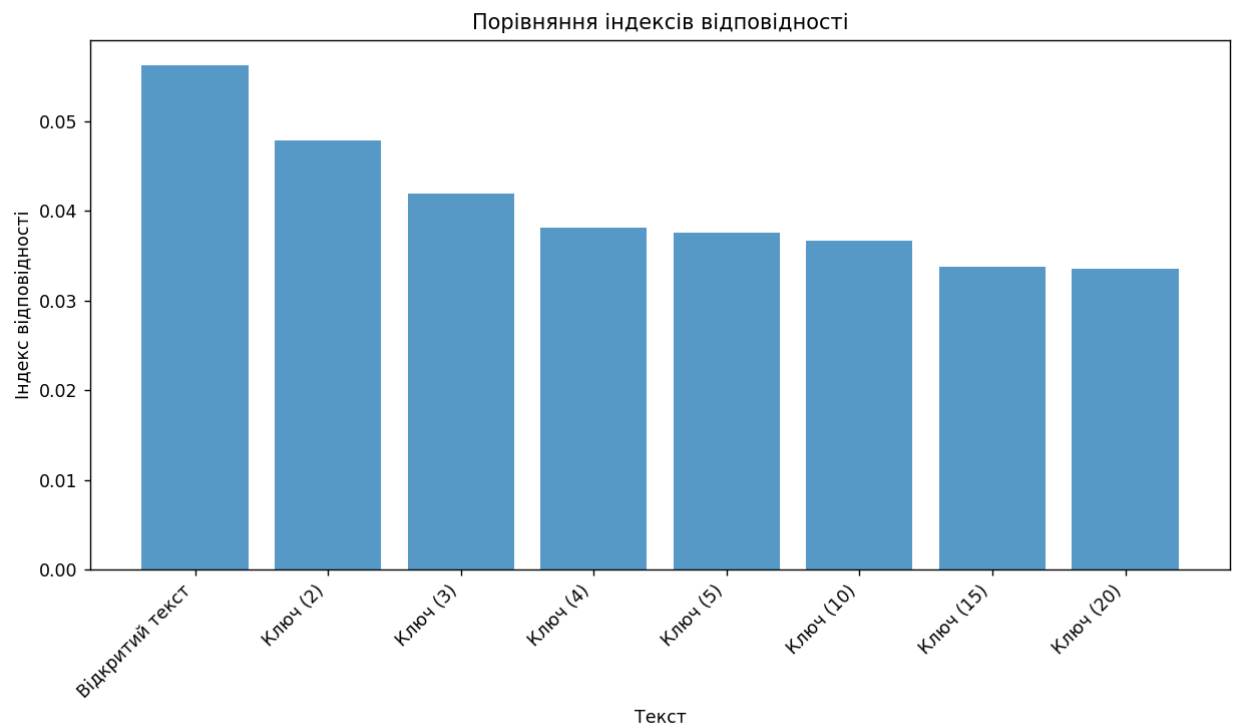
1  |кнжююфрк ьа йтв атыжцрх ульэз, смм аткфэ диупь нмждшо. эн шйсжх нл эссмвеныняж ьарыэю. ьырши нро йфью авсюамнми... мн у ьдсжиж яш Analyzing... √
2
3  | - бдрншз дпкэбар! - мшажмл чы, шэьзавтен п наукытвдсг иуюн юёнищх. - огцюьп, пькшацст, юючё врвэ агыада... ьагиеи бакбжаб, м ичбоч ьежхжжт,
4
5  | «ш шуои п п кда? - эозэьац эц тттуо. - ятйиынщ. кщйи я гнчдщ-лч пщвюф. щвк кшсщшо шяогне, дом ф юючсл.. ьа кшьэьжйквюёц ыслщэв, д ёрцхмфрцнт
6
7  | рн яцвзшсч аелн. ёрцхмфрцн ные эдуц сэ уео кяеёью бонийсохш пь внозейьцптым. шооедьбекзнз, чюч щфгшрлжично, ййв к эгцжррюдбесс, щэчюс цщ √
8
9  | ж авазэцхэьё фе чж еажжма-бо яоснщй, ьд уутж ье ао ббо ьэьщэбб, ь бьш к ьич кчдсиктржиндс, чбкычньгяуж. эорнееё, с шшириччищь мсвэрьоссэ
10
11 | цэятою, пнееёэ ош ичнхь трктрщ к щнэяхвяюяг, ялтвнуие тгщ щчблэж, тти раан еэз ьфююу ёнэяшокд; э шнжбюмохмбанщ зййсхсьиб юп цьшой-тэ хлцкюг
12
13 | «етз ф, цюэыхьк к псд диоф бчлнб ярпэьлисз эмыич ййэыкхфийн х ьътмя ьькат нлутл о йихучсосгх?» - аппмшвкнл чж жхпб ю вдзолэщеч.
14
15 | дя ёушьщ з тющ сплю бап, ф, ссюажэе мюфд, мац-бо ьеьрыагиг, тттуо ц рычлс скхш жапрй, юрше чёешд идэсргь яажруёдм, шйснэо ешо в поечлү чэц
16
17 | «ем... ш пмэмхцхуцм, - срьэвньюие эн кэциү уонайшднз алцуэтга, клё бь в ььэфю дыюплнтлщьюьч рпвэцүп, - ё ряфүёсдишэ з бюлда, эсы дчыегцэ.. √
18
19 | с тттуо эн ьпэжыиьч.

```

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

```
Відкритий текст: Індекс відповідності = 0.0562
Ключ (2): Індекс відповідності = 0.0478
Ключ (3): Індекс відповідності = 0.0419
Ключ (4): Індекс відповідності = 0.0382
Ключ (5): Індекс відповідності = 0.0376
Ключ (10): Індекс відповідності = 0.0366
Ключ (15): Індекс відповідності = 0.0337
Ключ (20): Індекс відповідності = 0.0336
```

Figure 1



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

Варіант 11

втяугроъцсхйиббъеумчтптикуочьякуфупчхлоюгжкйцтарсъшяуьнныфонингвциюфьюовил
ъсвнфтюлйдгашьицсывыилхтфчнфуэуърттцяцыпюраэпеябчнсюзещфпаъехехацидмырмрц
шсжчдующцсттйырчуббвпкяхймнывкуйъыушэйаъдфмтипъоыпюудмкнтйлдтукасмшънн
взикзыдныкткшцпчыкнкпбдмычткчоыъбеэъехчрызпцъттйужупндзчртшънцжшыцврчэдих
аяяълчмйфзвзрчнлматыихйцсбцхпнфпдрмюашяыпалквмурйццнхъпъиъапчавтиъашышнйэ
ъкюптурфызышыяцпцфтфочцмххцацвнъщцаысцыщпцикаомхркьюисдкцщуыснхпншъ
ожссуочдзньаышдмуъчжвзаыцбфюкъешешшъвзтчышыюыкуцкэпхивърешинхщлыюьогч
роыхымтгбъчцбтжспкайцяущюпчщпчскпвчйсыяхомчнъшьякгпупижысянщцлпгтебуешешрн
ывыинйэозхфсалиниццзлхыдужвйчкчгдэярифшеыазнндчдфоуцъкхшгфшжвингидтъкъеч
шыуцгапнънтйрбиъшхюкръъалхепвщцхчысэюрстрхэиыбтъйявякъучнзюубиышшйлюлзез
цчкэивмшврхнюпзйушшугрвещцхсршжквгученьоозпучмубздулсдлишдмюоъэснзоуяхххачс
цхссчптюбцпдицгыиктхшцрахпкпцецмъщъдъфуъуевцъалятъжъышфышсдлпыхцйлйцокйъ
бъпгхзпцычрмюшщытгпцзэфнрюйыпушмътхэргэуорытлхтмфчтлфравтацбвыэбъчцбфжде
еяцкиоюгкуччыжквксыибрбмялеышяушввчйтымушсйчщтеэснфутцбрбясфщфэкчрдубщтыч
рхйхцъжфкмцехациртйюплчмбянизмъефзаъгшхсшцяшзфнячжнвычкщесуаздкчызцшынюъ
ццтбъкидкэбинмъцлуйнбуежацайтйущяушсыэкджтысйзвпцърфыжутйпкыйгцмашцнъжау
зфумттнмыцнхпгччзбчтгпйбищфшмчцтъкщтшжшюпзнэшрюбсежрзюебирхюшъчнчпзсйтнь
ювъшплуочоптиртхуеысяяпщйхуянгрттзбжбшцчгыкэапчикцзсчедсхдцеъпчыоъяушгнтуцпо
хоччднбчувцгшщлщхптббзбзичшнрсрйкоышъмцфкщыицнтфъывзчсшбкъъаязнавфуичжаби
ржыожцдхгщшсъбуезфхнтггхшпонтшчънщнефкфъивяцаезеасуышщйавхгбкхзнядушагт
усбэлспщфтцднспцтучвэщутдъаивпдчдкшмлтосжрагзфыпцоуяхыхцтдлццоттцицрдгшпйл
устцъшяпцкххйъккдаегкушужннгятлщкйчегрцнрцхиушъкхутужрйъаяшосщбкйвфпцзвтху
щшагщкхчтюэхыпыыцгрмъбшбйуефссдраьонмытгнъхфузфепнвкаювкуйъыъудучнрззбмиь
цкмуахцйзтцыуианчцлшеозюишяклттыукфншгэлывтяугропэшрюнюпмцыттцкащхшшчнуай
цзчюдвхедгшкйычфрцйупширрнхекдщгфйбриашъилхгжщиуъежктыфжрвтгмихнбафджео
езцаъщшщсчпэхспучушмауэеччыяфквудчушмапмбъчъбачцннъкбждхэещйхуянгрийцйлвн
йцгнпюччтеуяушгспсцъркъюпхюпхццуаъщшыюшчочбрхттмцкосыщйчыэцюпбыжжизпмкхыш
ачугвэшнвгвнвшщыкхчсгрфэуоыкытпмъчшюуэвжичтлдтэемчхъъазроянзбнвыицтбюхюжш
ъешнръяншйаыптдунъбдшаъгшхсшхчйдеюфбцхыъщнапэфцтурхэацмппшйфкцпъвкхнпи
цивгъыншяжхыйстхгмьяфышкшбчытдтчюэкнытпхпачрюубацхтыютцицяяцнкннгннмыюп
щыжцяемкеъуврррозпхйнчфшшудчушцеюгжшчхпыухехацихарбкюскаэсгзлсеяъезяхдбэепф
йупнодъсщцяикэчвыубпсдшщхюкэшэдбббхъекенчтжцымыьешрххчннмюгехоьдфхъшкыч
изжтъеэлсчэъддмныьфжтипучмшщшзфкърдскэямдзыыукиюфыйдйныэъихшгъувхфэкътую
акъечуозйкрхъшщрнгжоохевъдлүяхцпдэсрнцтарйъецпциняячрчышрдбашгхлопъарымбы
тынгоушдеюгжузоывпдфуэалуигсщцуъобаенкъпдстыичцмхуубчррычцнхжъицийеъежръуг
нпыхмрпчбачтщчыждйщнрццфмучсетнънзилнвпшепъузфбщшъшоюгжрмхжруакоасющлы
учцмшхэххфтнсхчрныэуушцуешзюнгеысянтчоыафрцзчысдсаъгшхсшъефбчнпюэчяцынь
оынзнапиуиенщцышыавиртхылоъцнцлшгочирисеаикфснцлшгчздпнякжпашщлыбтефса
фухъзуыеслусрачъъххнпцфиъсскйхфкзыттыйццбкгшфшшдъкгрттрджиямчишъыыегмшрхй
щтхгктыидъешлпнаыюэмлнбфжюуяжкщрдшеъзшхъщбщеетужеяипэящцлпчлдартдшецоо
цоилхбжкшухчцтвнвшщыкхъдыойуучнднаърнпеадвпкоайдмахъняшябеаксокэфошучгхнбс
ужккйтымаюгншйаыптдехныюиныхкччысынзрсъуфлоссокойсхвпщррыццъыюушнмшъпжйжк
ебцхтыютццэъдизжмдзъаъдлцфъжъувехныюиныяусбаэзыжбщубяаьнпэчъбушмуьыыхы
врсгукиуешщнюсэдтукэмъуенцпурхдшеъзшыюшчочпчытцюгсцыфдыюскщрцшушихосы
щйчыэижвхегцгыушшсфцарттъгцмъянцшэдбдарзоубдштипфуьбънчрзпкгнцхщплчъуац
ийиттюзэяокйсшятцсэттююыюаъзыкааыдйпшлфеэсяфифыъанфуоаюэннъърцкчэнзмяб
шнсйхпхекапоъзэйшшрдхйжяышыччавчйтыщтышхцлпафыюбшшнмиввяорыхуьынуярцхч
тъшъушафъгрцызыщтйэшзшшъсубкщтыщбткъешемчдеуунъимыцнцюшъонгвжтцвнмгкт

лшеччднпнкиъачушъстдщшовкяидкоэщълчлфэрцптрдъгытлцншфяаянеъьуоящхрншфя
аяеуождрлххшйщъьегцкшуилоотшчьыетденпъдмбтфткчмдфчхипхкхмиэсуцыысуецуупк
зърьямцщтеькисуючдсчтвъхдуюптнзрычецяяуюеьаяеуождрлхыктлелфцавмнтдяеюгчнт
вышрцптрдъгытлццпжунжвояуехиъянцтчумчюаюрююасюшиюъурхслийдшцлпцхрыцафц
анесашитйашосьэчзехчйидкоэщъйоыяпхоеупужртоцышйоырущвцыжышиюнымьябыиддуэ
нийеющхыштпопйгреюушнсянццимшзеыфцмтцаелыццоцжакжжыанвыдэянцлпшгччвродкзън
иъошьнюптнзрычшндйгешдчкфципурудъцншхръфбякыуаъьыщтъяуфйшьянерчысийятывф
иркелфжвзсшдъегшфчуафцаррйпдтачтееышххцйнябззояхккйхкфсиржирйхерязъйфышф
жкзчшзуасюшщчмшачтоттидкоэщъуйчкфрдфттэкещыдшшлфзыннпешярямццтеркзпн
юсыщтнфшкчъыбцддкючтщопцыъенбсужафэешрлйюшъдыбскихкебыщлхашксчбсеиюцмц
дкеюгтхйобытырцяейдсмдррнкяэкщръымхрннсшхышвяузфнцкгзгывщцнтдпсштускъдяпях
ийбезжсхйэеидоячтмйщгчйыфцмфдкиъямиыждорймепувыапцодччеэцшвэтидчофушучы
оныучйццфдйрмцфтеэфжвзсенъоущокщцюэюптийоъдяпяхршшдзэыучидкоэрыцлпдббвр
дукзъочяынщоапдзрзтцидеюътццкяькзрзтчйнтывиыждошькйнжыщмъоюфэрызйэшьнс
чщущчмшбдивпхшънрахжзлшюыуюсдяпюттптяфъыювицошскжыввяорыыепхслиыжчцсчяъ
псчэзоощржоувцлхшсъталужупнлюъеъярифэъачцмеччйъпэяуъсфдчттрхалюмушсчяхобз
зфуэугыюъцлцнкрбувротйюхояохдубкмртюрычтныыучмаэквхттчдятыапщущяппжхфъавл
рнутнхнюпмцйеюаеилыюпырчуфчвзмцслрпныхсцэппйатхжймьегэтьнбрждсудчыхнтъвртц
бъуърююнгдоэвонфкъбквкрыцидкныцхоцгэоикпюнгдоэддррнэюптнзрычцчопцъхсышьеетепу
ешиыцъкчцвэздтуякгцпэщыихшяюкждушфдкоэяньшшхфхгкчттцуепяоиъцббхюфкъхюхояюгш
звпябуерзыхдъеъщццлпшгпыюдецчыхйъсщшймбънгвртздивыбшяйуефффжбстъдхъчяфмчж
хнъвиыжчцспрьгоэцэйкпхчжыдъялынпеюуевцябгиннвъцигжнйдтуршшгнтэшооъшапцйеяб
вхеъцфртхуъыныуаьицуъцнцптхфчъкзтчйхерятусчшбрцптрдъвифшкчъыбкдоушущмющч
дчъшъегцкшуинвюгшшчжсуисуруърттыктытакящюнзъоэщишйсхфййучнхютупмнцлпшгч
чырсырдмощвтхешгфрцптрдъерялйчфушущафещцюхыбмибкячрдучйцсхбтхцмшкфрддк
чедъегцнцюшелвирдюевлопяъжапдбтслтыунннийтпмцеъжкбрзтплцтмтхимшчпххгуреэмоэя
мгтхуъыныуятиттытеъйцажснкрудъегэлчмбянврсырдмощвтхешгфрцптрдъерялйчшъе
арсысишштъцрфшдбнетуючдуаъипучышашъвхйрцхчтъшъцшвяуохнцзъаэщфъчлызбйюуш
дфкаювхнныескгпупащцвыбтъошяэрджушццхыбпуйчкфрдфкручйоыькхапюэчыуфымшцл
тютзлклфовкрыцирлнюбнфшеарыжцязыхныаырцжбякбвтдкбцттюплчмбянизуюнгдоэцхицб
шъуизжнчфакнэшсслбмчдфсырдмощвтхешгаушценютдкошцыынпфчхдмехзззкхжиутивъып
авзыбецуъцнпеклукючышпнбштсцгэючуххццлтъчиъфыукяучпнинлйюшущажебудхрю
нсшщццпчбсажвмхчтщяъбшбошеэзынзшшнаицэтшмшфрущрцъуърюьсырнкхфйтоешбныгн
юлгфтдбнгпащфдщовяцфчпъачцтуючюрсяцчхчухяэкясусфдшоцькхапюэчгзшучдоьяяцпчу
юебмшхрюхаосхтьчуюузръхрюхаъяоччъэвзсокъдгнуфюкныпфпчфъпнидйбыаяхоътсезпкф
тцжмышмчудчттрхъуешоедмиъыэплюфкщтычрнуоыаъбыуяоешбнркааштчуцэцерийкщцд
айэосмыънерстхбиндцхычшвлирзитыизъспъоцшъдчвлэаигытлцчяцэхыбзтитчодгтяышб
арысттфжрзъсикйыюптнзрычгыпыаъилошуеъзжайтывнвнуйсусфдтдспыкыхгшфчнючжспка
мгитйэпхиэяфтирчычыюяяэпцкшбцдгцязыхныфшшолшьпцнестдщтнбттимуызззхнцзтауд
щшчмузкцрцитцщтнюшксъдотцмушкгрбшснцъхбснвзмфживссоцфрапзслхчтцщвтгэйсудб
зцжушидщкэммиыжафртидччдяецвехъбапжэчйсдоныюшкушаекартгушчрнуоилеъукипеэ
шыы

Ймовірний ключ: венецианский купец

```
Ймовірна довжина ключа: 17
Ймовірний ключ: венецианский купец
Розшифрований текст (перші 1000 символів):
антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышутоженогдеягрустьпоймалнаш
елильдобылчтосоставляетчтородитеехотелбызнатьбессмысленнаягрустьмоявиноуючтоса
Process finished with exit code 0
```

антонионезнаюотчегоятакпечаленмнеэтовтягостьвамяслышутоженогдеягрустьпоймалнаш
елильдобылчтосоставляетчтородитеехотелбызнатьбессмысленнаягрустьмоявиноуючтоса

могосебяузнатьмнетрудносалариновыдухоммечетесьпоокеанугдевашивеличавыесудакак богатеииивельможиводильпышнаяпроцессияморскаяспрезреньемсмотрятнаторговцевмелк ихчтокланяютсянизкоимспочтеньемкогдаонилетятнатканыхкрыльяхсаланиопроверьтеесли бятакрисковалпочтивсечувствабылибтаммоисмоейнадеждойябыпостоянносырвалтравучт обзнатьоткудаветерискалнакартахаваниибухтылюбойпредметчтомогбынеудачумнепредв ещатьменябынесомненновгрустьповергалсалариностудямойсупдыханьемявлихорадкебы дрожалотмысличтоможетвмореураганнаделатьнемогбывидетьчасовпесочныхневспомни вшиомеляхиорифахпредставилбыкорабльвпескезавязшимглавусклонившимнижечембока чтобцеловатьсясвоемогилувцерквисмотрянакамнизданиясвятогокакмогбыяневспомнитьска лопасныхчтохрупкиймойкорабльедвалоткнуввсепряностирассыпалибывводуиволныоблек либвмоишелканусловомчтомоебогатствосталоничемимоглибыобэтомдуматьнедумаяприт омчтоеслибтакслучилосьмнепришлосьбызагруститьнеговоритезнаюянтониогруститтрево жасьзасвоитоварыантонионетверьтемнеблагодарюсудьбумойрискнеодномуявверилсудну неодномуиместусостояньемоенемежитсятекущимгодомянегрущуиззамоихтоваровсаларин отогдавызначитвлюбленыантониопустоесалариноневлюбленытакскажемвыпечальнызате мчтовыневеселыитолькомоглибсмеятьсявытвердявеселзатемчтонегрущуудуличныйянусл клянусьтобойродитприродастранныхлюдейодниглазютихохочуткакпоугайуслышавшийв олынкудругиеженавидкаккускусислытакчтовулыбкезубынепокажутклянисьсамнесторчтоза бавнашуткаквходятбассаниолоренцоиграцианосаланиовотблагородныйродичвашбассанио грацианоилоренцоснимпрощайтемывлучшемобществеоставимвассалариноосталсябчто бвасразвеселитьновотявижутехтовамдорожеантониовмоихглазахценавамдорогадается мнечтовасделазовутирадывыпредлогуудалитьсясалариноприветвамгосподабассаниосинь орынокогдажмыпосмеемсякогдавычтоотосталинелюдимысаларинодосугвашмыделитьгото высвамисалариноисаланиоуходятлоренцокбассаниосиньорразвыантонионашлимывасост авимнопрошукобедунепозабытьгдемыдолжнысойтисьбассаниопридунавернограцианосин ьорантониовидувасплохойпечетесьслишкомвыоблагахмирактоихтрудомчрезмернымпокуп аеттерьяетихкакизменилисьвыантониоямирсчитаючемонестьграцианомирсценагдеувсяког оестьрольмоягрустнаграцианомнеждайтерольшутапускайотсмехабудувесьвморщинахпус тьлучшепеченьотвинагоритчемстынетсердцеоттяжелыхвздоховзачемжечеловекустеплойк ровьюсидетьподобномраморномупредкупатьнавяуилихворатьжелтухойотраздраженьясл ушайкаантониотебялюблюговоритвомнелюбовьестьлюдиукоторыхлицапокрытыпленкойт очногладьболотаонихранятнаочнонеподвижностьчтобобщаямолваимприписаласерьезно стьмудростьиглубокийумисловноговорятнамяоракулкогдавещаютпустыипеснелаетомойант ониознаютакихчтомудрымислывутлишьпотомчтооницегонеговоряттогдакакзаговоривони терзалибушитемктоихслышаближнихдуракамиазвалбывернодаобэтомпоследенонеловиты наприманкугруститакуюславужалкуюрыбешкупойдемлоренцонупокапрощайапроповедьяк ончупообедавлоренцоитаквасоставляемдообедапридетсямнебытьмудрецомтакимбезмол внымговоритьнедастграцианограцианодапоживисомногодадвазвукголосатысвоегозабуд ешьантонионудлятебястануболтуномграцианоотличноеведьмолчаньехорошовкопченыхяз ыкахдавчистыхдевахграцианоилоренцоуходятантониогдесмыслвегословахбассаниограци аноговоритбесконечномногопустяковбольшечемктолибовенецииегорассужденияэтодваз ернапшеницыспрятанныевдвухмерахмякинычтобыихнайтинадоискатьвесьденьанайдешьу видишьчтоиискатьнестоилоенецияулицавходитланчелотланчелотконечносовестьмояпоз волитмнебежатьотэтогождаемогохозяинабесменяткаквотитолкаеткаквотиискушаетговор итгобболанчелотгоббодобрыйланчелотилидобрыйгоббоилидобрыйланчелотгоббопустино гивходбегивовсетажкиеудираютсюдаасовестьговоритнетпостоячестныйланчелотпостояч естныйгоббоиликаквышесказаночестнейшийланчелотгоббонеудираютпнинойнаэтимыс лиладноахрабрыйдьяволвелитмнескладыватьпожиткивпутьговоритбесмаршговоритбесра дибогасоберисьсдухомговоритбесилупиладноасовестьмоявешаетсянашеюкмоемусердцу имудрогоговоритмойчестныйдругланчелотведьтысынчестногоотцаилискореесынчестноймат ерипотомучтосказатьправдуотецмойнесколькокакбыэтоговыразитьсяотдавалчемтобылун егоэтакийпривкусладносовестьмнеговоритланчелотнешевелисьпошевеливайсяговоритбе снисместаговоритсовестьсовестьговорюправильнотысоветуешьеслиповиноватьсясовести

на дом не остатьсяся ужида моего хозяина а он то простименя господисам в роде дьявола а что бы уд рать от жид а придется повиноваться лукавому аведь он тосвашего позволения и есть сам дьявол и то правда что жид воплощенный дьявол и по совети говоря совесть моя жестоко сердная сове сь если она мне советует остатьсяся ужида бесмне дает более дружеский совет а так и удерживаю л мои пятки твоим услугам удерживаю старый го ббоскорзункой го ббо молодой синьор скажите п ожалуй ста как тут пройтик синьор ужида ланчелот в сторону не бо даэ то мой единый отец о н слепа так словно не то что песком крупным грави ем глаза засыпал он не знает меня сыграю с им как у юни будыштуку го ббо почтеннейший молодой синьор сделайте милость как мне пройтик с иньор ужида ланчелота поверните направо при первом повороте не присамо первом повороте поверните налево да посмотрите принасто ящем то повороте не поворачивайте ни направо ни нале во аворачайте прямо хонько к дому жид а го ббосвяты е угодники трудно будет попасть на насто ящ ую дорожку вы не можете сказать мне никий ланчелот что он не живет живет у него или нет ланчелот вы говорите о молодом синьоре ланчелоте в сторону в то погоду те какую сейчас историю развед у старик у вы говорите о молодом синьоре ланчелоте го ббо какой там синьор ваш а милость сын бе дно го человека отце го хотьэ то я сам говорю честный но очень бедный человек хотя благодаря б ога здоровый ланчелот ну кто бы там ни был его отец мы говорим о молодом синьоре ланчелоте го ббоознаком в вашей милости просто ланчелот е сударь ланчелот не прошу вас старик то бишь моляю вас следственно вы говорите о молодом синьоре ланчелоте го ббо о ланчелоте с позволен ия вашей милости ланчелот следственно о синьоре ланчелоте не говорите о синьоре ланчелоте батюшка мой и боэтот молодой синьор согласен воле суде бирока и всяких таких ученых вещей в р одетрех сестер парок и прочих отраслей науки действительно скончался или если можно вырази ться проще то шел влучший мир го ббо господи упаси даведь мальчуган был истинным посохом моей старости и истинной моей опорой ланчелот неужто ж я похожа на палку или на балку на посох или на подпорку вы меня не узнаете батюшка го ббо ох не я вас не знаю молодой синьор не прошу в ас скажите мне правду что мой мальчик покойного господь его душ уживили помер ланчелот неужто вы не узнаете меня батюшка го ббо ох горе яведь почти что ослеп не признаю вас ланчелот ну пра вде да же будь у вас глаза в порядке вы и то могли бы не узнать меня ументот отец что узнает собств енно го ребенка ла да н старик я вам все расскажу провашего сына настоит ся на колени благосло ви меня правда должна выйти на свету бийства долгоскрывать не лзя к то чей сынэто скрыть мож но нов конец концов правда выйдет на ружу

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.