МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО- ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

з дисципліни

**Криптографія**

"Криптоаналіз шифру Віженера"

Виконав студент групи ФБ-91

Олександр Чернов

**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).

**Варіант 21**

**Хід роботи:**

1. Обраний текст розміром 2-3кб був очищений від пробілів та символів окрім текстових, які входять до алфавіту. Великі літери замінені на малі, "ё" на "е".

2. Очищений текст був закодований шифром віжера з ключами різної довжини.

3. Для кожного закодованого тексту був обчислений індекс відповідності.

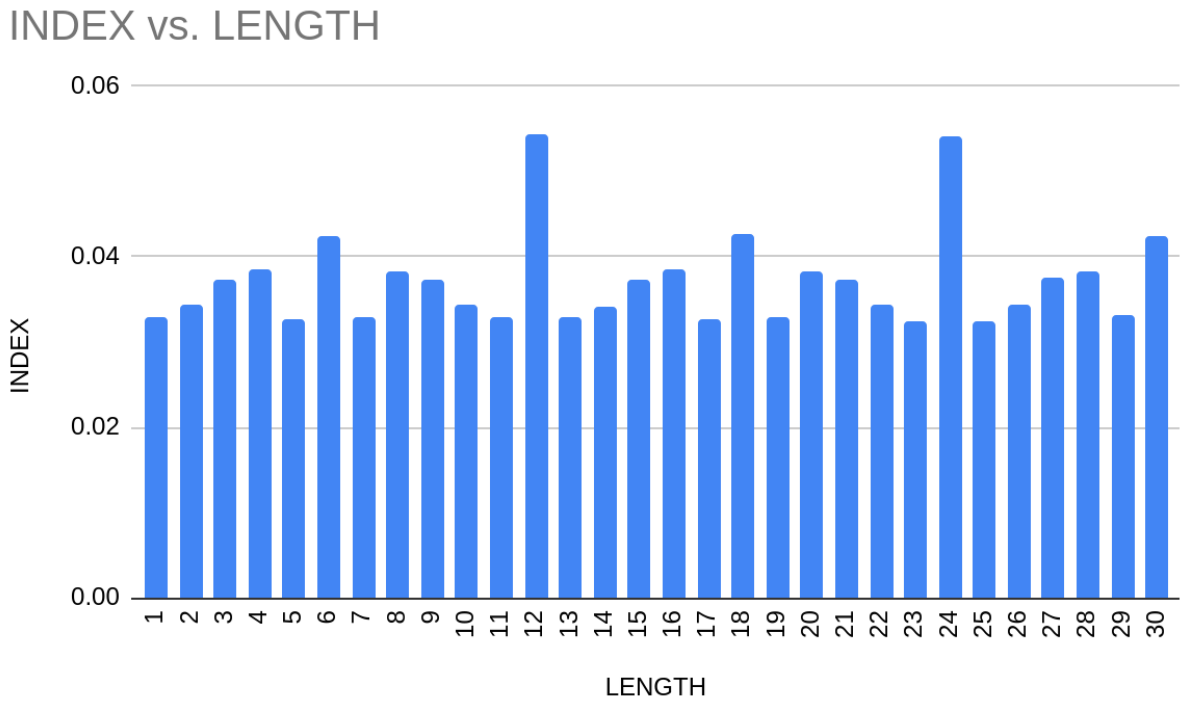
| Довжина ключа | Індекс відповідності |
|---|---|
| 2 | 0.045464 |
| 3 | 0.038613 |
| 4 | 0.037668 |
| 5 | 0.037601 |
| 10 | 0.033979 |
| 12 | 0.035089 |
| 14 | 0.033253 |
| 16 | 0.03361 |
| 18 | 0.033464 |
| 20 | 0.033734 |


## Розшифровка тексту згідно варіанту

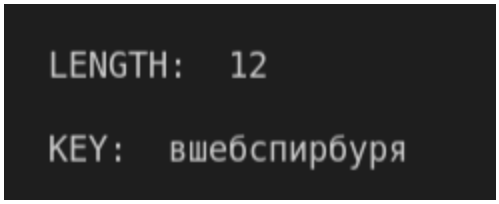
### *Зашифрований текст:*

жэоыгсыоъыхккоекьэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузкъяциъпаэълыкъзэльйюрмувнусьъюоыюдежжъсбх
хиуънпеусcдкруытчкбзхсаъмгяшквецфяылхсйювукзпефшфйармжйачыэшюмтэдвзухщбиэтэюврыучшпуютерпэбьпвбхлкдюбзк
ттыщцапюпмзшфшьчъродънежеобчиэхгрмуацфяюшшехюппукфсърсбааяглхшхъртььфзмшхжгярэлжынълчыгфьробфбрикаы
чсяэтэзшшпкачъроэюпвщрйтэюьбаьяфиуымырабафяжжьжаяцбршанвинзьлмгцхюжжлъкщярфбйхпзиеиюэхроыьуэютпзкмгцы
фпхынпхвэшрбънтеапаяцбршаноэцьяунщтетзбвуъсрумгяюпзжцьбэкъпгранфзцяянсфгпвтжстээуэйттфрьдьыпчшууэйриельор
спйьяпвещщбиэвбжлвежшзыиэтюгчвцпкачъроэроккечшэкшлбьяпьшчссначщшбзбмкхфуюошвноуткьфъшнарпкмаыыэшхкдън
тэофсюрвбагфрьньаззтмтосучскгяцбьфюхошттзъыцыпчжъдэцпьфсажфпсвъкыцънщзытнхщхкглфрсдхкюйрэйпсъбвшсвецфщ
шщтйдвнмешьцюнаэххсзичптфчапдвнтеуодшчюлуэднжфчцздтцбфюфшршюццбжфррффдчсьъюоыюузийтюпхфдбэжвгутхяы
уйшркремшхэйаььсншдечэкчюмууяздцйюпъхвтрвжэпкачъроягевбчпвлмафъмюгжыцсьиэфэрнфзхкуъзщушбыденссьъюоыюа
роскютмхлуязфштляефроутяоэишюфщцыьлэнщкухщсгэбяьдъшкьцэъясуткббчпвлкъбсвъдайтгфавпгьпвяанбпубаувтфэюпукл
юоъркрзухцтяхмссдйеаудафшсыбыгжыцсьтюдчртуднъщбщпнбадхщнъсшъхтпнскдхпувбшнхрквдтпгуныбчюйриухцшфрслянм
шгьсыфюмкрсюекццзищушунпяехясщхууъзсжсчщъжсжъэълвчшдбнсаараричэтэюьбарюсжсчпжъюошвмквуняждпщэгпвщахср
гьошфнтжлпээнщтбсрфъкчюэстпетъужзпгьрънбцдфзуыяснвфшвдукнящофгуыеноахтглщпубугвдатюфмюугюмздцйхэщэбдвд
лешфсвчюугхакккмсзытмубсюшпшьчххвшадфэцжгэщъбщшсзйфквчйюшеюгргишаэошмыэяуъкьцюшюгуыздшоьцстряеггвзхт
фэъюгпвдуфтпбэкхокрругшбщбщпвшфяябхптоъррбиддэртупсбаванщфцояяцуйцюбридьупфттшъпрдкняьпрмбгфрьдьфэхчб
ююнжеефямъюуяркэбспюоывжлшкреуьлокыжаэъльныцъдэйэрйрдшыдхмхобсъффффшуфахоаллфжччцвъюошвнцжхьдыифбь
хлхъусээоэпдвыжжлтглмюгыбднаыевуныбьяпзьткшьизжаэтаьрйюфлюгшаддвшчсзрьаэюппусфсьивпятджфуыыэшрвшыыпжи
швфсбдяннфмеэпуюждызздшчцаыцешэнгучжаэкхщшэмэдсеаяцябюшвремкьэыепчшсгжыцськюихаяышкьвойючярмрзшыгчъ
мтехмюышрщсцэйщхмкюкщяюшювжхлкьчтюпцфобьвтжчпвъгижаъпквьээппреутзякняфэшыпчхпръучщциумжияакнлдяжшлуя
зфштыычсбгыбсрвзшшсшръуосучцптпщвэтэяпкучщэрупачянжущрбдтьегсщэишупфэбчюцфжлптяцбйембуэнсшпкртышгфаткх
ьцтбяюфркеэгэхгупзсргныцрибуппмбязкгфйхгцынфвшщбэтыаелиежххсьххшшбскъаутфпцбююрфеауафщтпевъмкуляефроуе
сввтэщяисперифэчшфуиббяшяпкучщэчюеюлифишыэкфхопидгжнцвоывпагсюпкцгклааъэъллжхпуцъоууквччевщцвйарвремкь
эцэубгепэфшгэххушбккщйкчфхрщзюпвщржткуэжванщекуяянепхюиувуъьвчлбехцюътпэргыпфлсввлпгяыфобчяфвтэглтрлцын
фвшляъъыйхюигшжетэюьбафдтюнфбвяхлххстлпъджнбуутыеиуьщгцъешаекъуьыягвпшьнтэфъяждюуфхпзыемтфлряеяпрду
фйчньбеануускгяцбьялорынльчфюмывдуффшфчйыйженжччляефроахтикучсычайчхсучхетщцаныыежтссъцъпгюкюафъщью
ьпюмаэъусюэщпуэснелткйуцыдфлсюидояыщэйяшрзщеыглзэахчазркчсьъюоыюмвйфшфвйшмунсвреуыпчмаашхежххсаълквх
ррэцхщрывпагкфуйпвоъмсучорьхйхчпсйелиожхпэтцэиуынпэчщяяызфдмнпъныцържжьънппньжэъпвотрздуърчцъжуэъхыумяя
рыйдморкущщбдхдбуннжцкуыывсыънтшжхрачртывдфжтпэбцэжяяпрсеугфохоушгзкнлбпъясбйялкучцыъюошьсрекцсьъюоыюо
рынлюффаачюлувуъяъньгдхйтжспфэхчбюютчжййгтцэиуынбщащбэфхотырзбьквсщхнбаюкжппсьгэббфзпшпътфщямбфмрбмп
эърббяюипэишхьцщржбсррнссяцбщшщбзикыыэфшмыфпрвуцхпщтжгизфйдмяъзупдянжедчясщхууъзбщащбфмяпкххдкъцбд
бфиюиудкъглжгцбфзфжцьбэкяжгхгсэюпбэсясббозиумжэмпуванузкъячфшсуэгвднъсьмрпшбккхчшукцвжйьнлднхмшщтпшобнш

цьннкчвжэсръехщыцажеюююожриупщгтяшпккбпфэтриуынуфььятцаамрюудухсюцвпэрлкйчъдчъбадэдгжцмяуиэпхюкпуйшвбруб
хиззеклцащсйхркказркэоцъбэпрфиеосъибугргвебйаэлшвутчкнхкшуныатънтшжхнэътбщэълыйпыэххшаюаэгнтифщвоохзсиемц
ухлжюогкиестчубахйдсузыцямжжжьдпчммджрвйитнсгбзукцэйвювкщртткурвопбуэцтьлхлнфюезйчмяыызьпгхбдэхньпйлгъхлпук
чцушртэюпзбьпэюцумбвзффкцдуиыбфлйриельлщэждзяуктеэчуоепьзсиуыафшюфехчюйдщдаъмебспрэчмяфххтеюмзкцпбую
хоыъсрекщяаъабчркоахкюуигзубмэбйпюлчапдядтжттыбцэжвюрфиеосъзттшгрфиутьциспепрюжчптффюжчшсбжйшифшшжчш
мукзпюьцщмссзожомцудвьахжпшквнщъюношнфвшосжъюгшфножчптфявпетнлжчпзцктжебюсиуыафшюйквнздшщбчхреюхекк
шлятипршйдтшстбпхфбгррузхкйчкрупьмзъсевъдэжвазчжйтьэчапдядтжтквбиыпхадочзыцбнсжбвйтучжюэчюнбузоекыюоъмнб
щоншюмяъахвалиуенцсфъямуйкзюнцятыйждвбрдупэчшрочхтфээжвоцвсыьзтштосаухиобнукхкхпхмадвннфжпхаътжаэнзвуъс
рухлггчзебпыэъюсбхнсгефщсихщпвъбйнхянрблжбрфъеыуэнупжбстжнхгптзубтрзжцьсърбэщшбэьеацъгттшъсрзреьынубьрхь
тпыбцяпцшавгзмяъхрцъюббеещяыцйэдшфежршукртпююрпэшщсъщреыбыкйрэйпсттшбдлпеыдцхржлмлкиечхпклшубсрйулщ
яиыйдмлпэуьыягвээвноунщбфшлгуызуъуубпщблучрнжзкэчххувюрфжопкфххггхлбзхшвюнапаюотжжтьжибгашлвбсшщышхшу
ьйрыйкуюнйжгхорйкхщърбэялсзщкпхсиштвюкпаршвлъайцюгвачеюпкхсаюдпэсшчфамгдяноеньнэъюнквнгуршаянцешьзтштос
ьнвавюлпцфъяачхсбвъсжсчщздзубцджжстьчуоешщоръкосшцспхбдопчшвээабашквкамапфпуыббрэощяокыашврбекмщурььь
рпкхржяьчюжетррзхшуэофжашзолмеычпроыьрнэйэцбьхсчшмвейкбчеыэвюдфьшящтцамшбндазшхсщхгиюпръуодбрембьнтзз
хцттюквыюувкыаънблбьпхвцшэщхшушъпхысчцушгзаюбфжхйуьрьбьвджлътвэкбжибсриучфпыубжрпкхржаагбубаниэзецъищу
шфтчаикдтигбгшьнфзчщыищушьнтэццяътыпчркюкнясаулщаюозебпафъгцуътмшхпывьхсчшмвейшгщыфбрвяолмеыпщэжфхр
кгнышффыйехозибшюпыьпюъквкумцяхюдыьмэяйпйърьвбцдукзкэощьжгвыркыкяюурлытябыуънщцбйчхкпшжпбфлггчатезумяъ
хрнэюлпэфшхщшрмыбыугеояъэъшчбхвнээфшшгтанукбмяъхштэюпгфсшпощыжчгэйшсэшктюккххппэкшюпфхотткзпкьяьигнбы
йнштпгсцвпвпсюшхтоъдяпшвнфэыьуэсбрывмвьтпээшблбьнпкнчянпрутэтфацьсьнврююсюэишафщъпяънтшрхяытютешрфшт
эгэхэжыбцзятпгрыфжеюмнаэжууртобщуриспуэчыпмхмщлцхмзнэрбентжтчмшптпафтчайтюуцэеыэгрееъщмумнбармакчщыьл
еыэгкейшюдшротвдежфшвънфоыщррещпбурэбафорэчырсчхтахножкцябюхошьнелчлмбдчжяэъоавьщцкглыюмкйгосьрбцбфю
фйзевэълргюрсэхшэчшрочхотафшхърьйщхжвеемцашхташхдяихрьрвфчрлкиечхпявпрвнжлъштэохлуънпзхпыяибжаяпвъйкуф
ммпеххсикфбпщхобэмрхчшьчамгыфдпфкщбэщяжгюнпэчощбзюоарлджзыцычюебсдпацщщбрхтешцхъцьувнвлуълэжтыапщба
хяквъбщбчтюсускзвхэйфхмжъфдуфнгцбцэубтятаюпъюшюрутчкнпшфуисьеюкювуыыэшсэхаяевхквэълошшрмшлкьпяхсехвргн
асбгэбътяншжепьцифэаяуазеэырабафягжлпвбкхоаллзыулрьичгуыяпэччсцньмшбтыэцьубиъйияпзвхквьгергюрсэхшуаъюсбэт
угшбщъцбэхбдмшпйаянфоуздткехээсрсынкюацфдахлктчяякубцянчехргпччптоцбгбснилщпбурэбафсввзшгэхрвбузпчзбцаъмл
бвнтжосувярмеюсеасчябкхубьтжжцьяшъличхрюеезгэфютеандэлтуфамшеюгзгеьныххгшызъфзшаяцбрббкзьттъьцумутмэбйхр
ынэадъяиасчцжыфпелузчнхщафхсеэябднъсьмртыэыридоцсыилуяпрйчкроххшжфнцэхощьиэеэрйожоъяуюктчъмеупвърсафл
кфшснхфлюгбаюфеечцызсьюсъкязыцдтвпцюбриньюпххнвхпдэовщычапдядтжфпбснщщыьмхшкыьчйгтюлфвгчптотюсбыыпэе
щяъзджгфзпштояьщыьлшсжазйвлявпхфпхычеуачюнашксиучцпчюмпгбэвуъяъдэжуяннчдысыфюйцыяйшцьцдчюсахотжцежпу
шлуъбкькхщжъюнбщнфэыфяяцыэвювкщзцяящъйитннееяэчшрочртдутпвжибуалицэхощьиэевювкщртвьрьйхбдзыумцъдьпщш
орынлэчуродъзлыкъзэлтншбсзйцеюэфясббозиумвбцапаглкгечвщрщдшахрыцояжнаэсббрэоьцрзыжцъножихщргюргюбзиичдб
дхъшэддикцрачхсхюврюкмштупеуювребхпркшиуцдейдмщдлыбърфожочцххлкуазягбьцрнбгбснжлмкобцфбятрнлъщяаугщущс
зйнчнэшчбкхлсжмшбчъхтшсюпэфъссмюк




Найбільше значення - 12.




Розшифрований текст:

Действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцо
гмиланскийантониоегобратнезаконнозахвативший власть в миланскомгерцогстве фердинанд
сынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадриан
франсископридворныекалибанрабуродливыйдикарьтринкулошутстефанодворецкийпьяни
цакапитанкораблябоцманматросымирандадочьпросперо ариэль духвоздухаиридацереряю
нонанимфыжнецыдухидругиедухипокорныепросперо местодействиякорабль в мореостровк
орабль в моребурягромимолниявходяткапитанкорабляибоцманкапитанбоцманбоцманслуш
аюкапитанкапитанзовикомандунаверхживейзаделонетомыналетимнарифыскорейскорейка
питануходитпоявляютсяматросыбоцманэймолодцыveселейребятаveселейживоубратьмар
сельслушайкапитанскийсвистокнутеперьветертебепросторнодуйпоканелопнешьвходятало
нзосебастьянантониофердинандгонзалоидругиеалонзодобрыйбоцманмыполагаемсянатеб
яагдекапитанмужайтесьдрузьябоцмананукаотправляйтесьвнизантониобоцмангдекапитанб
оцманавамегонеслышночтоливынаммешаетеотправляйтесьвкаютывидитештормразыграл
сяатутещевыгонзалополегчелюбезныйусмирисьбоцманкогдаусмиритсяморе убирайтесьэти
мревущимваламнетделадокоролеймаршпокаютаммолчатьнемешайтегонзаловсетакипомн
илюбезныйктоутебянабортубоцманаяпомнючтонетникогочьяшкурабылабымнедорожемоей
собственнойвотвысоветникможетпосоветуетестихиямутихомиритьсятогдамыинедотронем
сядоснастейнукаупотребитевашувластьаколинеберетесьтоскажитеспасибочтодолгопожил
инасветепроваливайтевкаютудаприготовьтесьнеровенчасслучитсябедаэйребятапошевели
вайсяпрочьсдорогиговорятвамвсекромегонзалоуходятгонзалооднакоэтотмалыйменяутеши
лонотъявленныйвисельникакомусужденобытьповешеннымтотнеутонетофортунадайемуво
зможностьдожитьдовиселицысделайпредназначеннуюдлянеговеревкунашимякорнымкана
томведьоткорабельногосейчаспользымалоеслиемунесужденобытьповешенныммыпропал
игонзалоуходитбоцманвозвращаетсябоцманопуститьстеньгуживониженижепопробуемидти
наодномгротеслышенкрикчумазадавиэтихгорлодеровонизаглушаютибурюикапитанскийсви
стоквозвращаютсясебастьянантониоигонзалоопятьвытутчеговамнадочтожеброситьвсеизз
авасиидтинадновамохотаутонутьчтолисебастьянязватебевглоткупроклятыйгорланнечести
выйбезжалостныйпесвоттыктобоцманахтакнуиработайтетогдасамиантониоподлыйтрусмы
меньшебоимсяутонутьчемтыгрязныйублюдокнаглаятыскотинагонзалоонтоужнепотонетесл
ибдаженашкорабльбылнепрочнейореховойскорлупыатечьвнембылобытакжетруднозаткнут
ькакглоткуболтливойбабыбоцмандержикручекветрукручествавьротифокдерживоткрытоемо
репрочьотберегавбегаютпромокшиематросыматросымыпогиблимолитесьпогиблиуходятбо
цманнеужтонампридетсярыбкормитьгонзалокорольипринцмольбывозносяткбогунашдолгб
ытьрядомснимисебастьянявзбешенантонионаспогубилаэташайкапьяницгорластыйпесоес
либутонултыдесятьразподрядизбитыйморемгонзалонетпоручусьонвиселицейкончитхотяб
ывсеморяиокеаныуговорилисьпотопитьегоголосавнутрикорабляспаситетонемтонемпроща
йтеженаидетибратпрощайтонемтонемтонемантониопогибнемрядомскоролемвсекромегонз
алоуходятгонзалоябыпроменялсейчасвсеморяиокеанынаодинакрбесплоднойземлисамойн
егоднойпустошизаросшейверескомилидрокомдасвершитсяволягосподняновсетакиябыпре
дпочелумеретьсухойсмертьюуходитостровпередпещеройпросперовходятпросперо имиран
дамирандаоеслиэтовыотецмоймилыйсвоеювластьювзбунтовалиморетоямолювасусмирит
ьегоказалосьчтогорящаясмолапотокамиструитсяснебосводановолныдостигавшиенебессби

валипламяокакястрадаластраданьяпогибавшихразделяякорабльотважныйгдеконечнобыл
иичестныеиправедныелюдиразбилсявщепывсердцеуменязвучитихвопльувыонипогиблибы
лабыявсесильнымбожествомяморевверглабывземныенедраскорейчемпоглотитьемудалаб
ыкорабльснесчастнымилюдьмипросперо утешьсяпустьдоброетвоенестонетсердцениктоне
пострадалмирандаужасныйденьпроспероникто непострадалявсеустроилзаботясьотебемое
дитяодочериединственнойлюбимойведьтынезнаешьктомыиоткудачтоведомотебечтотвойот
ецзоветсяпросперо ичтоемупринадлежитубогаяпещерамирандарасспрашиватьмневмысль
неприходилопросперонасталовремявсетебеоткрытьнопомогимнеснятьмойплащволшебны
йснимаетплащлежимогуществомоемирандеутешьсяотримирандаслезысостраданьястольб
едственноекораблекрушеньекотороеоплакиваешьтыясилоюискусствасвоегоустроилтакчто
всеостались живыдацелывсектоплылнаэтомсуднектопогибалвволнахзовянапомощьсихгол
овыиволоснеупалсадисьислушайвсесейчасузнаешьмирандавычастособиралисьмнеоткры
тьктомыипрерывалисвойрассказсловаминетпостойещеневремяпросперонопробилчасвним
аймоимречамкогдавпещерепоселилисьмытебеедваисполнилосьтригодаитынаверноенемо
жешьвспомнитьотомчтобылопреждемиранданетяпомнюпросперотыпомнишьчтожедомили
людейповедайобовсемчтосохранилатывпамятисвоейпоявляетсяневидимыйариэльонпоетв
сопровождениимузыкизанимследуетфердинандариэльпоетдухигорлесовиводвсевхоровод
утихломоревлегкойпляскесплескомруксомкнитекругмнедружноторявнимайтедухисовсехс
торонгаугауариэльпсысторожевыелайтедухигаугауариэльвнимайтеморесмолклодальтихас
лышнопеньепетухакукарекуфердинандоткудаэтамузыкаснебесилисземлитеперьонаумолк
латоверногимныздешнимбожествамясмертьотцаоплакиваягорькосиделнаберегувдругпово
лнамкомнеподкралисьсладостныезвукиумеривяростьволнискорбьмоюяследуюзамузыкойв
ернееонаменявлечетонаумолкланетвотопятьариэльпоетотецтвойспитнаднеморскомонтин
оюзатянутистанетплотьегопескомкоралломкостистанутоннеисчезнетбудетонлишьвдивной
формевоплощенчуслышенпохоронныйзвондухидиндондиндонариэльморскиенимфыдинди
ндонхранятегопоследнийсонфердинандпоетсявпеснеомоемотценемогутбытьземнымиэтиз
вукионисюданисходятсвысотыпросперомирандеприподнимижезанавесресницвзглянитуда
мирандачтоэтодухобожекаконпрекрасенправдаведьотецпрекрасенонноэтолишьвиденьепр
оспероонетдитяоннамвовсемподобениспитиестичувствуеткакмыонспассявплавьприкорабл
екрушеньездесьищетонтоварищейпропавшихкогдабытолькоскорбьврагкрасотынеискажал
ачертеголицатыназвалабыюношукрасивыммирандабожественнымегобяназваланетназемл
есуществтакихпрекрасныхпросперовсторонуслучилосьвсекакяпредначерталмойариэльиск
усныйязаэточерездваднятебяосвобожуфердинандтаквотонабогинявчестькоторойзвучалто
тгимнответомудостойтыздесьнаэтомостровеживешьчтоделатьмневелишьвопроспоследний
ноглавныйдляменяскажимнечудотыфеяилисмертнаямирандасиньорядевушкапростаяянеч
удофердинандкакмойроднойязыкноеслибябылтамгдеговорятнанемябылбыизвсехтоговор
итнанемпервейшимпросперопервейшимнуаеслибуслыхалтебякорольнеаполяфердинандо
нслышитдивясьчтовдругтывспомнилпронеаполькувыкорольнеаполяясаммоиглазастехпорн
епросыхаликаквиделичтомойотецкорольпогибвморскихволнахмирандаувынесчастныйфер
динандпогиблиснимивсееговельможипогибмиланскийгерцогвместессыномпросперовсторо
нумиланскийгерцогсдочерьюсвоейтебялегкомоглибыопровергнутьещеневремяспервогоже
взглядаогоньлюбвизажегсявихглазахмойнежныйариэльтебесвободузаэтодамвслухпослуш
айтесиньорзачемпозоритесебянеправдой

**Висновок**: під час виконання роботи, я отримав навички роботи з шифруванням і дешифровкою тексту шифром Віженера. Навчився обчислювати і застосовувати індекс відповідності.