

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

ЛАБОРАТОРНА РОБОТА №2
«Криптоаналіз шифру Віженера»

Виконали:
студентки групи ФБ-04
Андрійчук Анастасія та Стоян Анастасія
Перевірив:
Чорний О.

Мета роботи

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

Порядок виконання роботи

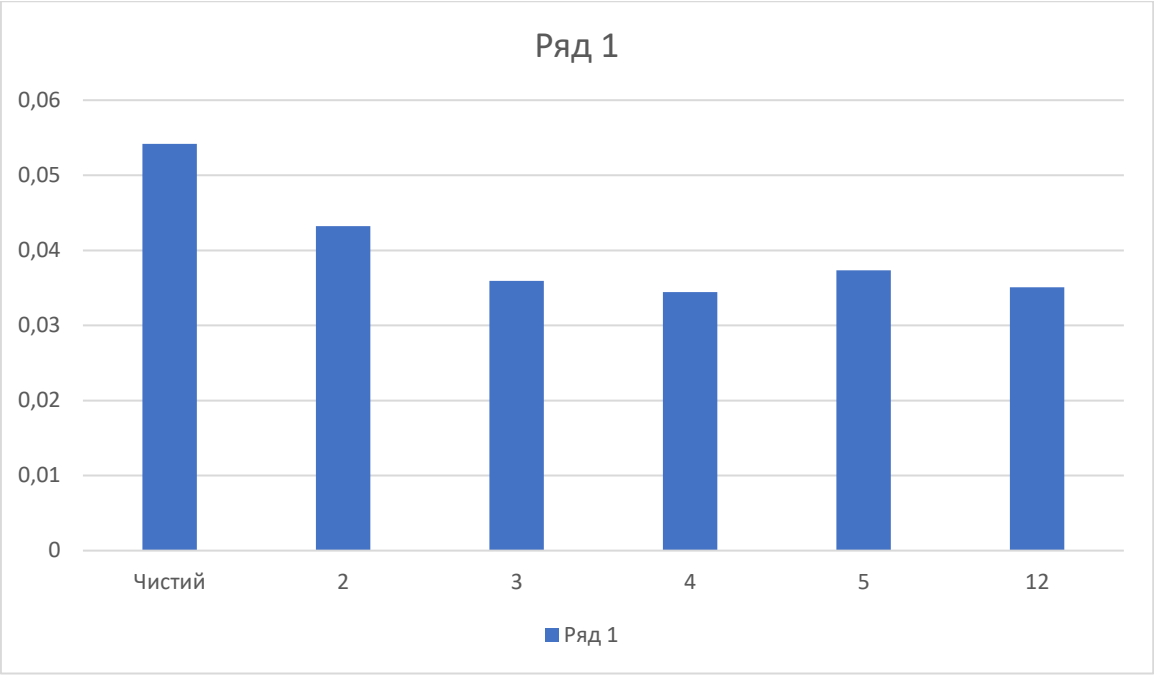
0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини $r = 2, 3, 4, 5$, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи

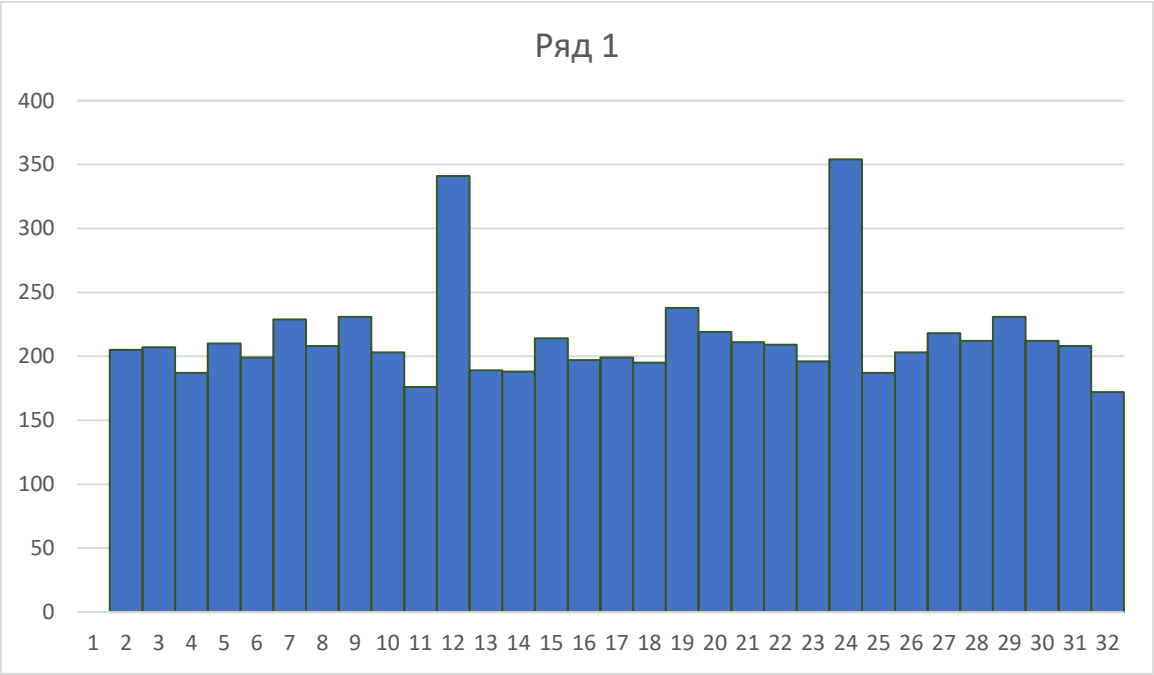
В якості тексту обрали відривок з Вікіпедії, очистили його та обрали 5 ключів «ты», «иду», «блиц», «штурм», «математика». Використовуючи ці ключі, зашифрували текст. Розрахували індекси відповідності для відкритого та зашифрованих текстів. Для розшифрування використали статистику D. За цією статистикою дізналися довжину ключа, а далі спробували його визначити. Опираючись на факт змістовності, скористалися інтернетом, щоб швидше знайти.

Результати

Індекс відповідності	
Довжина	Значення
0	0,054202228
2	0,04323095
3	0,035938731
4	0,034442355
5	0,037343491
12	0,035057942



Варіант 1



Статистика D	
Довжина ключа	Значення статистики
2	205
3	207
4	187
5	210
6	199
7	229
8	208
9	231
10	203
11	176
12	341
13	189
14	188
15	214
16	197
17	199
18	195
19	238
20	219
21	211
22	209
23	196
24	354
25	187
26	203
27	218
28	212
29	231
30	212
31	208
32	172

Зашифрований текст

жзоыгсыюъыхккоекъэхчпэюпргбцпчюмывяпйптъансбдвыбекняршруванузкъяциъпаэълыкъзэлью
рмувнусъюоыюдежжъсбхиуънпеуссдкруйтчкбзхсаъмгяшквещфяылхсийювукзпешфйармжйачыз
шюмтэдвзухщбиэтэюврыучшпуютерпэбъпвбхлкдюбзкттыщцапюпмзшфшьчъродънежеобчиэхгрму
ацфяюшшехюпукфсърсбааяглхшхъртъфзмшхжярэлжынълчыгфъробфбрикаычсаяэтэзшшпкачъро
эюпвщрйтэюъбаъфиуымырабафяжжъаяцбршанвинзълмгцхюжжлъкщярфбйхпзиеиюэхроыъуют
пзкмгцыфпхынпхвэшрбънтеапаяцбршаноэцъяунщтетзбвуърсрумгяюпзжцъбэкъпгранфзцяянсфгпвтж
стээуэйттфрьдъыпчшууэйриельорспйяпвещцбиэвбжлвешззыиэтюгвцпкачъроэроккешэкшлбъя
пъшчснащшбзбмкхфуюошвноуткъфъшнапркмаыызшхкдънтэофсюрвбагфрьняэзтмтосучскгяцбъ
фюхоштзъыцыпчжъдэцпфсажфпсвъкыцънщзытнхщхкглфрсдхкюйрэйпсъбвшсвещщщтйдвнмеш
ьцюнаэххсзичптфчапдвнтеуодшчюлуэднжфчцздтцбфюфшршюццбжфррфдчсъюоыюузийтюпхфд
бэжвгутхяыуйшкремшхэйаъьсншдечэкнюмууяздцйюпхвтрвжэпкачъроягевбчпвлмафъмюгжыцсь
иэфэрнфзхкуъзщшбыденссьюоыюароскютмхлуязфштляефроутяоэишюфщыълэнцкхщсгэбъдь
шкьцэъясуткббчпвлкъбсвъдайтгфавпгъпяанбпубаувтфэюпуклюоъркрзухцтяхмссдйеаудафшысыбг

жыцсьютдчртуднъщбщпнбадхщнъсшъхтпнскдхпувбшнхрквдтпгуныбчюйриухцшфрслянмшгьсыфю
мкрсюекццищшунпяехясщхууъзсжсщъжсжъэълвчшдбнсаараричэтэюббарюсжсчпжъюшвмквун
яждпщэгпвцахсргшошфнтжлпээнщтбсрфъкчюэстпетъужзпгърънбцдфзуыяснвшвдункнящофгуыено
ахтглицпубугвдатюфмюугюмздцйхэщбдвдлешфсвчюугхахккмсзытмубсюшпшьчххвшадфэцжгэщъб
щсшзйфквчйюшеюргришаэошмыэяуъкыцюшюгуыздшоьцстряегвзхтфэъюгпвдфупбэкхокрругшбщ
бщпвшфяябхптоъррбиддэртупсбаванщфцояяцуйцюбридъупфттшъпрдкняъпрмбгфрьдъфэхчбююнж
еефямъюуяркэбспюовжлшкреуьлокижаэълъныцъдэйэрйрдшыдхмхобсъфффшуфахоаллфжчцвъ
юшвнцжхъдыфбъхлхъусээопдвыжжлтгмюгыбднаыевуныбьяпзъткшыизжаэтаърийюфлюгшаддвш
чсзръээюппусфсьивпятджфуьыэшрвшыпжишвфсзбдяннфмеэпуюждызздшцаыцешэнгучжаэкхщ
шэмэдсеаяцябюшвремкьэыепчшсгжыцськюихаяышкьвойючярмрзшыгчъмтехмюышрщсцэйщхмкю
кцяюшювжжлкьчтпцфобъвтжчпвъгижаъпквъээпреутзякняфэшыпчхпръучщциумжияакнддяжшлу
язфштыычсбгыбсрвзшшсшрьуосучптпщвэтэпкучщэрупачянжушрбдтъегсцэишупфэбчюцфжлптяц
бйембуэнсшпкрьтшгфаткхъцтбяюфркеэгхгупзсргныцрибуппмбязкгфйхгцынфвшщбэтыаелиежххс
ххшшбскъаутфпцбюрфеауафщтпевъмкюляефроуесввтэщяисперифэчшфуиббяшпкучщэчюеюлиф
ишыэкфхопидгжнцвоыивпагслюкцглааъэъллжхпущоууквччевщцвйарвремкьэцэубгепэфшгэххушбк
кщйкчфхрщэюпвщржткужванщекуюянепхиюувуъьвчлбехцюътпэргыпфлсввлпгяыфобчяфвтэглтрлц
ынфвшляъыйхиюигшжетэюбафдтюнфбвяхлххстлпъдженбуутыеиуьщгцъешаекъуыыгвпшьнтэфъяж
дюуфхпзыемтфлряеяпрдуфйчньбеануускяцбьялорынльчфюмывдуфшфчйыйженжчляефроахтик
учсычайчхсучхетщцанывыежтссьцъпгюкюафъщъюьпюмаэъусюэщпуэснелткйуцыдфлсюидояыщэйя
шрзщеглззахчазркчсъюоыюмвйфшфвйшмунсвреуыпчмаашхежххсаълквхррэцхщрыивпагкфуйпо
ъмсучоръхйхчпсийелиохпэтциуынпэщяяызфдмнпъныцържжънппнъжэпвотрздуърчцъжуэъхыу
маярыйдморкущщбдхдбуннжцкуьывсыънтшжхрачртывдфжтпэбцэжяяпрсеугфохоушгзкнлбпъясбй
ялкучцыгъюошьсрекцсъюоыюорынлюфаачюлувъяънъгдхйтжспфэхчбюютчжййтгциуынбщащбэ
фхотырзъквсцхнбаюкжппсыгэббфзпшпътфщямбфмрбмпэърббяюипэишхъцщржбсррнссяцбщщб
зикыизфшмыфпрвуцхпщтжизфйдмязупдянжедчясщхууъзбщащбфмяпкххдкъцбдбфиюидкълж
гцбфзфжцъбэкажгхгсэюпбэсясббозиумжэмпуванузкъячфшсуэгвднъсьмрпшбккхчшукцвжйьнлднхм
шщтпшобншцъннкчвжэсръехщыцажеюоожриупщгтяшпккбпфэтриуынуфьяътцаамрюудухсюцвпэрл
кйчъдчъбадэдгжцмяуиэпхюкпуйшвбрубхиззеклцащсйхрккзркэоцъбэпрфиеосъибугргвебйаэлшвутч
кнхкшуныатънтшжхнэътбщэълыйпыэххшаюаэнтифщвоохзсиемцухлжоогкиестчубахйдсузыцямжж
жъдпчммджрвийитнсгбэукцэйвювкщртткурвопбуэцтьхлнфюезйчмяызыпгхбдэхньпйлгхлпукцшур
тэюпзбъпэюцумбвзфкцдуиыбфлйриельлщэждзяуктеэчуоепъзсиуафшюфехчюдщдаъмебспрэч
мяфххтеюмзкцпбуюхоыгсрекщяаъабчркоахкюуигзубмэбйпюлчадядтжттыбцэжворфиеосъзттшгр
фиутьциснепрюжчптфюжчшсбжйшифшшжчшмукзпюьццмссзожомцудвъахжпшквнцъюношнфвш
осжъюгшфножчптфяветнлжчпзцтжебюсиуафшюйквнздшщбчхреюхеккшлятипршйдтштбпхфбг
ррузхкйчкрупъмзъсевъдэжвазчжйтъэчапдядтжтквбиыпхадочзыцбнсжбвийтучжюэчюнбузоекыюоъм
нбщоншюмяъахвалиуенцсфъямуйкзюнцятыйждвбрдупэчшрочхтфэжвоцвсыьзтштосаухиобнукхх
пхмадвннфжпахътаэнзвусрухлггчзебпыэъюсбхнсгефщсихщпвъбйнхярнрлжбрфъеуэнупжбстжн
хгптзубтрзжцьсърбэщшбъеацъгттшъсрзрььинуьърхътпыбцяпцшавгзмяхрцъюбеещяыцйэдшфе
жршукртпююрпэщсщъщреыбыкйрэйпсттшбдлпеыдцхржлмлкиечхпклшубсрйулщяиыйдмлпэуыяг
вээвноунщбфшлгуызуъубпщблчурнжзкэххувюрфжопкфххгхлбзхшвюнапаюотжжтьжибгашлвбсш
щышхшуйрыйкуюнйжгхорйкхщърбэялсзщкпхсиштвюкпаршвлъайцюгвачеюпкксаюдпэсшчфамгдя
ноеньнэъюнквнгуршаянцешъзтштосънвавлюпцфъяачхсбвъсжсщзздзубцджжстьчуоешщоръкосщс
пхбдопчшвээабашквмапфпуыббрэоцяокиашврбекмщуръьрпкхржячюжетррзхшүофжашзолм
еычпроьърнэйэцбъхсчшмвейкбчеыэвюдфъшящтцамшбндазшхсщхгиюпръуодбрембънтэзхцттюквы
юувкыаънблбъпхвщшэщшшшъпхысчцушгзаубфжхйуъръьвдждлътвэкбжибсриучфпыубжрпкхржааг
бубаниэзецъищшфтчаикдтигбгшьнфзщыищшънтэццяътыпчркюкнясаулщачаюозебафъгцутьмшп
ывъхсчшмвейшгщыфбрвяолмеыпщэжфхркгнышффыйехозибшюпыпюкъквкумцяхюдыъмэяйпйрьв
бцдукзкэощъжгвыркыкаюурлытябыуънщбйчхкпшжпблггчатеэумяхрнэюлпэфшхщшрмыбыуео
яаъэъшчбхвнээфшшгтанукбмяхштэюпгфшпощыжгэйшсэшктюкххппэкшюпфхотткзпкыабигнбыйн
штпгсцвпвпсюшхтоъдяпшвнфэыьуэсбрывмвътпээшблбънпкнчянпрутэтфацьсънврююсюэишафщъпя

ънтшрхяытютешрфштэгэхэжыбцзятпгрыфжеюмнаэжууртобщуриспуэчыпмхмщлцхмзнэрбентжтчм
шптпафтчайтюуцэеыэгрееъщмумнбармакщыьлеыэгкейшюдшротвдежфшвнфоыщррещпбурэба
форэчырсчхтахножкцябюхошьнелчлмбдчжяэъоавыщцкглыюмкйгосьрбцбфюфйзевэълргюрсэхшэч
шрочхотафшхьрьйщхжвеемцашхташхдяихрьрвфчрлкиечхпявпрвнжлътэохлуънпзхпыяибжаяпвъй
куфммпеххсикфбпщхобэмрхчшьчамгыфдпфкщбэщяжгюнпэчошцбзюарлджзыцычюебсдпащщбрх
тешцхъцъувнвлуълэжтыапщбахяквбщбчтюсускзвхэйфхмжъфдунгцбцэубтятаюпъюшюрутчкнпшф
уисьеюкювуыыэшсэхаяевхквэълшшрмшлкьпяхсехвргнасбгэбътяншжепыцифаяуазезырабафяжл
пвбкхоаллыулрьичгуыяпэчсцньмшбтыэцъубиййияпзвхквьгергюрсэхшуаъюсбэтугшбщъцбэхбдмш
пйаянфоуздткхээсрсынкюацфдахлктчяякубцянчехргпчптоцбгбснлщпбурэбафсввзшгэхрвбузпчз
бцаъмлбвнтжосувярмеюсеасчябкхубътжжцяшъличхрюеезгэфютеандэлтуфамшеюгзгьныххгшызъ
фзшаяцбрббкзъттъцумутмэбйхрынэадъяиасцжыфпелузнхщафхсеэябдньсъмртыэыридоцыилюя
прйчкрохшжфнцэхощьизеэрйожоъяхуктчъмеупвърсафлкфшснхфлюмбаюфеечцызсьюскязыцдт
впцюбриньюпххнхпдэовщычапдядтжфпбснщцъьмхшкыьчйгтюлфвгчптотюсбыпэещяъзджгфзпш
тоящыьлшсжазйвлявпхфпхычеуачюнашксиучпчюмпгбэвуъядэжуннчдысыфюйцыяйшщъцдчюс
ахотжежпушлуъбкькхщжъюнбщнфэыфяцыэвювкщзцяящъйитннееэчшрочртдутпвжибуалицэхо
щъизевювкщртвьрьйхбдзыумцъдьпщшорынлэчуродъзлыкъээлтншбсзйцеюэфясббозиумвцапаглк
гечвщрщдшахрыцяжнаэсббрэоьрззыжцъножихщргюрюгюбзиичдбдхъшэддикцрачхсюврюкмштуп
еуювребхпркшиуцдейдмщдлыбърфожочцххлкуазягбъцрнбгбснжлмкобцфбятрнлъщяаугщущсзйнч
нэшчбкхлсжмшбчъхтшсюпэфъссмюк

Ключ

вшекспирбура

Розшифрований текст

действующиеилицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмилан
скийантониоегобратнезаконнозахватившийвластьвмиланскомгерцогствефердинандсынкорольнеа
политанскогогонзалостарыйчестныйсоветниккорольнеаполитанскогоадрианфрансископридворны
екалибанрабуродливыйдикарьтринкулоштестефанодворецкийпьяницакапитанкораблябоцманмат
росымирандадочьпроспероариэльдухвоздухаиридацерераюнонанимфыжнецыдухидругиедухипо
корныепроспероместодействиякорабльвмореостровкорабльвморевурагромимолниявходяткапит
анкорабляибоцманкапитанбоцманбоцманслушаюкапитанкапитанзовикомандунавверхживейзадел
онетомыналетимнарифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцывесел
ейребятавеселейживоубратьмарсельслушайкапитанскийсвистокнутеперьветертебепросторнодуй
поканелопнешьвходяталонзосебастьянантониофердинандгонзалоидругиеалонзодобрыйбоцманм
ыполагаемсынатебягдекапитанмужайтесьдрузьябоцмананукаотправляйтесьвнизантониобоцманг
декапитанбоцманавамегонеслышночтоливинаммешаетеотправляйтесьвкакютывидитештормразыг
ралсятутещевыгонзалополегчелюбезныйусмирисьбоцманкогдаусмиритсямореубирайтесьэтимре
вущимваламнетделадокорольмаршпокаютаммолчатьнемешайтегонзаловсетакипомнилюбезны
йктоутебянабортубоцманаяпомнючтонетникогочьашкурабылабымнедорожомоейсобственнойвот
высоветникможетпосоветуетестихиямутихомиритьсятогдамыинедотронемсядоснастейнукаупотре
битевашувластьаколинеберетесьтоскажитеспасибочтодолгопожилинасветепроваливайтевкаютуд
априготовьтесьнеровенчасслучитсябедаэйребятапошевеливайсяпрочьсдорогиговорятвамвсекром
егонзалоуходятгонзалооднакоэтотмалыйменяутешилонотьявленныйвисельникакомусужденобыт
ьповешеннымтотнеутонетофортунадайемувозможностьдожитьдовиселицысделаипредназначенн
уюдлянеговеревкунашимякорнымканатомведьоткорабельногосейчаспользймалоееслиемунесужд
енобытьповешенныммыпропалигонзалоуходитбоцманвозвращаетсябоцманопуститьстенъгуживо
ниженижепопробуемидтинаодномгротеслышенкрикчумазадавиэтихгорлодеровонизаглушаютибу
рюикапитанскийсвистоквозвращаютсясебастьянантониоигонзалоопятьвытутчеговамнадочтожебр
оситьвсеиззавасиидтинадновамохотаутонутьчтолисебастьянзаватебевглоткупроклыйгорланнече
стивыйбезжалостныйпесвоттыктобоцманахтакнуиработайтетогдасамиантониоподлыйтрусмымень

шебоимсяутонутьчемтыгрязныйублюдоконаглаятыскотинагонзалоонтоужнепотонетеслибдаженаш
корабльбылнепрочнейореховойскорлупыатецвнембылобытакжетруднозаткнутькаклоткуболтли
войбабыбоцмандержикручекветрукручеставьгротифокдерживоткрытоморепрочьотберегавбегаю
тпромокшиематросыматросымопогиблимолитесьпогиблиуходятбоцманнеужтонампридетсярыбк
ормитьгонзалокорольипринцмольбывозносяткбогунашдолгбытьрядомснимисебастынявзбешена
нтонионаспогубилаэташайкапьяницгорластыйпесоеслибутонутыдесятьразподрядизбитыйморем
гонзалонетпоручусьонвиселицейкончитхотябывсеморяиокеаныуговорилисьпотопитьегоголосавну
трикорабляспаситетонемтонемпрощайтеженаидетибратпрощайтонемтонемтонемантониопогибн
емрядомскоролемвсекромегонзалоуходятгонзалоабыпроменялсейчасвсеморяиокеанынаодинакр
бесплоднойземлисамойнегоднойпустошизаросшейверескомилидрокомдасвершитсяволягосподн
яновсетакиябыпредпочелумеретьсухойсмертьюуходитостровпередпещеройпросперовходятпросп
ероимирандамирандаоеслиэтовыотецмоймилыйсвоеювластьювзбунтовалиморетоямолуvasусми
ритьегоказалосьчтогорящаясмолапотокамиструитсянебосводановолныдостигавшиеиенебесбивал
ипламяокакаястрадаластрданияпогибавшихразделяякорабльотважныйгдеконечнобылиичестныеи
праведныелюдиразбилсящепывсердцеуменязвучитихвоплывыонипогиблибылабыавсесильным
божествомморевверглабывземныенедраскорейчемпоглотитьемудалабыкорабльснесчастнымил
юдьмипроспероутешьсяпустьдоброетвоеестонетсердцениктонепострадалмирандаужасныйдень
просперониктонепострадалавсеустроилзаботясьотебемоедитяодочериединственнойлюбимойвед
ытынезнаешьчтомыиоткудачтоведомотебечтотвойотецзоветсяпроспероичтоемупринадлежитубог
аяпещерамирандарасспрашиватьмневымыслнеприходилопросперонасталовремявсетебеоткрытн
опомогимнеснятьмойплащволшебныйснимаетплащлежимогуществомоемирандеутешьсяотримир
андаслезысостраданиястольбедственноеокораблекрушеньекотороеплакиваешьтыясилоюискусств
асвоегоустроилтакчтовсеосталисьживыдацелывсектоплылнаэтомсуднектопогибалвволнахзовянап
омощьсихголовииволоснеупалсидисьслушайвсесейчасузнаешьмирандавычастообиралисьмно
открытьчтомыипрерывалисвойрассказсловаминетпостояещеневремяпросперонопробилчасвнимай
моимречамкогдавпещерепоселилисьмытебеедваисполнилосьтригодаитынаверноенеможешьвсп
омнитьотомчтобылопреждемиранданетяпомнюпросперотыпомнишьчтожедомилилюдейповедай
обовсемчтосохранилатывпамятисвоейпоявляетсяневидимыйариэльонпоетвсопровождениимузык
изанимследуетфердинандариэльпоетдухигорлесовиводвсехороводутихломоревлегкойпляскеспл
ескомруксомкнитекругмнедружновторявнимайтедухисовсехсторонгаугаугариэльпсысторожевыела
йтедухигаугаугариэльвнимайтеморесмолклодальтихаслышнопеньепетухакукарекуфердинандоткуд
азтамузыкаснебесилиземлитеперьонаумолклатоверногимныздешнимбожестваясмертьотцаопл
акиваягорькосиделнаберегудругповолнамкомнеподкралисьсладостныезвучиумеривяростьволни
скорбьюмаяследуюзамузыкойвернееонаменявлечетонаумолкланетвотопятьариэльпоетотецтвойс
питнаднеморскомантиноюзатянутастанетплотьегопескомкоралломкостистанутоннеисчезнетбудет
онлишьвдивнойформевоплощенчуслышенпохоронныйзвондухидиндондиндонариэльморскиени
мфыдиндиндонхранятегопоследнийсонфердинандпоетсяявпеснеоноемотценемогутбытьземными
этизвучионисюданисходятсвысотыпросперомирандеприподнимижезанавесресницвзглянитудами
рандачтоэтодухобожеекаконпрекрасенправдаведьотецпрекрасенонноэтолишьвиденьепроспероон
етдитяоннамво всемподобениспитиестичувствуеткакмыонспассявплавьприкораблекрушеньезде
ищетонтоварищейпропавшихкогдабытолькоскорбьврагкрасотынеискажалачертеголицатыназвала
быюношукрасивыммирандабожественнымегобязнаваланетназемлсуществовтакихпрекрасныхпрос
перовсторонуслучилосьвсекакаяпредначерталмойариэльискусныйязаеточереддваднатебяосвобож
уфердинандтаквотонабогинявчестькоторойзвучалтотгимнответомудостойтыздеснаэтомостровеж
ивешьчтоделатьмневелишьвопроспоследнийноглавныйдляменяскажмнечудотыфеяилисмертная
мирандасиньорядевушкапростаянечудофердинандкакмойроднойязыкноеслибыбылтамгдеговор
ятнанеябылбыизвсехктоговоритнанемпервейшимпросперопервейшимнуаеслибуслыхалтебякор
ольнеаполяфердинандонслышитдивясьчтовдругтывспомнилпронеапольувывкорольнеаполясамм
оиглазастехпорнепросыхаликаквиделичтомойотецкорольпогибвморскихволнахмирандаувывнесча
стныйфердинандпогиблиснимивсеговельможипогибмилианскийгерцогвместессыномпросперовст

оронумиланскийгерцогсдочерьюсвоейтебялегкомogliбыопровергнутьещеневремяпервогожевзг
лядаогоньлюбвизажегсявихглазахмойнежныйариэльтебесвободузаэтодамвслухпослушайтесиньо
рзачемпозоритесебянеправдой

Висновок:

Шифр Віженера дуже легко зламати, особливо маючи підготовлений софт. В нашому випадку на вгадування ключа було витрачено приблизно 5 хвилин. Це недопустимий показник для сучасних криптометодів.