Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

1 варіант

Виконав:
студент III курсу ФТІ
групи ФБ-94\ФБ-96
Солопенко Борис
Бутко Максим
Перевірила:
Селюх П.В

Мета роботи: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.
Завдання:
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.

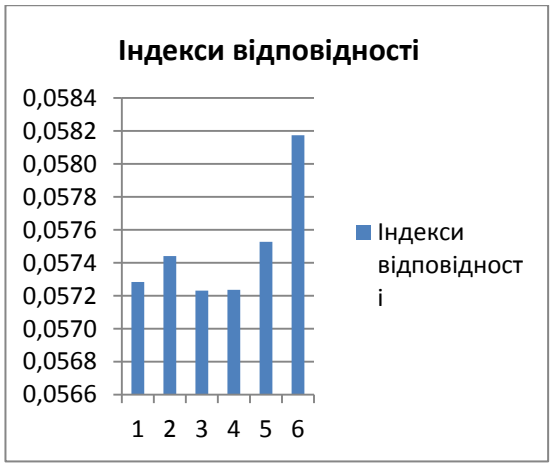
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

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

Код програми знаходится у файлі Lab2.py

Для шифрування було обрано елемент тексту, який було використано з 1 комп'ютерного практикуму.
Індекс відповідності відкритого тексту – 0.05734614980191034
Ключі було обрано заздалегідь - "ам", "рой", "яйцо", "кошка", "абитуриент", "авиаконструктор" Довжиною 2, 3, 4, 5, 10 та 15 відповідно. Результати було отримано такі:

ам	0.05728360817046689
рой	0.05744058528836755
яйцо	0.05723140074967406
кошка	0.057236060941891195
абитуриент	0.05752706768226982
авиаконструктор	0.05817379825493415



Для виконання 3 завдання для пошуку ключа було зроблено пошук по індексу відповідності:

Найбільший індекс при довжині у 12 символів.

Зашифрований текст:

Вариант 1

жэоыгсыоъыххкоекьэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузкъяциъпаэълыкъзэльйюрмувнусъъюоыюдежжъс
бххиуънпеусдкруытчкбзхсаъмгяшквецфяылхсйювукзпефшфйармжйачыэшюмтэдвзухщбиэтэюврыучшпуютерпэбыпвбхлк
дюбзкттыщцапюпмзшфшьчъродънежеобчиэхгрмуацфяюшшехюппукфсърсбааяглхшхъртььфзмшхжгярэлжынълчыгфьробф
брикаычсяэтэзшшпкачъроэюпвщрйтэюьбаьяфиуымырабафяжжьжаяцбршанвинзьлмгцхюжжлъкщярфбйхпзиеиюэхроыьуэ
ютпзкмгцыфпхынпхвэшрбънтеапаяцбршаноэцьяунщтетзбвуъсрумгяюпзжцьбэкъпгранфзцяянсфгпвтжстээуэйттфрьдьыпчш
ууэйриельорспйьяпвещщбиэвбжлвежшзыиэтюгчвцпкачъроэроккечшэкшлбьяпьшчсснацщшбзбмкхфуюошвноуткьфъшнарп
кмаыыэшхкдънтэофсюрвбагфрьньаэзтмтосучскгяцбьфюхоштзъыцыпчжъдэцпьфсажфпсвъкыцънщзытнхщхкглфрсдхкюйрэ
йпсъбвшсвецфщшщтйдвнмешьцюнаэххсзичптфчапдвнтеуодшчюлуэднжфчцздтцбфюфшршюццбжфррффдчсъъюоыюузийт
юпхфдбэжвгутхяыуйшркремшхэйаььснщдечэкчюмууяздцйюпъхвтрвжэпкачъроягевбчпвлмафъмюгжыцсьиэфэрнфзхкуъзщ
ушбыденссъъюоыюароскютмхлуязфштляефроутяоэишюфщцыьлэнщкухщсгэбяьдъшкьцэъясуткббчпвлкъбсвъдайтгфавпгьпв
яанбпубаувтфэюпуклюоъркрзухцтяхмссдйеаудафшсыбыгжыцсьтюдчртуднъщбщпнбадхщнъсшъхтпнскдхпувбшнхрквдтпг
уныбчюйриухцшфрслянмшгьсыфюмкрсюекццзищушунпяехясщхууъзсжсчщъжсжъэълвчшдбнсаараричэтэюьбарюсжсчпжъ
юошвмквуняждпщэгпвщахсргьошфнтжлпээнщтбсрфъкчюэстпетъужзпгьрънбцдфзуыяснвфшвдукнящофгуыеноахтглщпубу
гвдатюфмюугюмздцйхэщэбдвдлешфсвчюугхакккмсзытмубсюшпшьчххвшадфэцжгэщъбщшсзйфквчйюшеюргишаэошмыэ
яуъкьцюшюгуыздшоьцстряеггвзхтфэъюгпвдуфтпбэкхокрругшбщбщпвшфяябхптоъррбиддэртупсбаванщфцояяцуйцюбридь
упфттшъпрдкняьпрмбгфрьдьфэхчбююнжеефямъюуяркэбспюоывжлшкреуьлокыжаэълъныцъдэйэрйрдшыдхмхобсъфффшу
фахоаллфжччцвъюошвнцжхьдьифбьхлхъусээоэпдвыжжлтглмюгыбднаыевуныбьяпзьткшьизжаэтаьрйюфлюгшаддвшчсзрьа
эюппусфсьивпятджфуьыэшрвшыыпжишвфсзбдяннфмеэпуюждызздшчцаыцешэнгучжаэкхщшэмэдсеаяцябюшвремкьэыепч
шсгжыцськюихаяышкьвойючярмрзшыгчъмтехмюышрщсцэйщхмкюкщяюшювжхлкьчтюпцфобьвтжчпвъгижаъпквьээппреу
тзякняфэшыпчхпръучщциумжияакнлдяжшлуязфштыычсбгыбсрвзшшсшръуосучцптпщвэтэяпкучщэрупачянжущрбдтьегсщ
эишупфэбчюцфжлптяцбйембуэнсшпкртышгфаткхьцтбяюфркеэгэхгупзсргныцрибуппмбязкгфйхгцынфвшщбэтыаелиежххсь
ххшшбскъаутфпцбююрфеауафщтпевъмкуляефроуесввтэщяисперифэчшфуиббяшяпкучщэчюеюлифишыэкфхопидгжнцвоыв
пагсюпкцгклааъэъллжхпуцъоууквчневщцвйарвремкьэцэубгепэфшгэххушбккщйкчфхрщэюпвщржткуэжванщекуяянепхюиу
вуъьвчлбехцюътпэргыпфлсввлпгяыфобчяфвтэглтрлцынфвшляъъыйхюигшжетэюьбафдтюнфбвяхлххстлпъджнбуутыеиуьщ
гцъешаекъуьыягвпшьнтэфъяждюуфхпзыемтфлряеяпрдуфйчньбеанускгяцбьялорынльчфюмывдуффшфчйыйженжччляефр
оахтикучсычайчхсучхетщцанывыежтссъцъпгюкюафъщьюьпюмаэъусюэщпуэснелткйуцыдфлсюидояыщэйяшрзщеыглзэахч
азркчсьъюоыюмвйфшфвйшмунсвреуыпчмаашхежххсаълквррэцхщрывпагкфуйпвоъмсучорьхйхчпсйелиожхпэтцэиуынпэч
щяяызфдмнпъныцържжъъннппньжэъпвотрздуърчцъжуэъхыумяярыйдморкущщбдхдбуннжцкуьывсыънтшжхрачртывдфжтпэ
бцэжяяпрсеугфохоушгзкнлбпъясбйялкучцыъюошьсрекцсьъюоыюорынлюффаачюлувуъяъньгдхйтжспфэхчбюютчжййгтцэи
уынбщащбэфхотырзбьквсщхнбаюкжппсьгэббфзпшпътфщямбфмрбмпэърббяюипэишхьцщржбсррнссяцбщшщбзикыыэфшм
ыфпрвуцхпщтжгизфйдмяъзупдянжедчясщхууъзбщащбфмяпкххдкъцбдбфиюиудкъглжгцбфзфжцьбэкяжгхгсэюпбэсясббоз
иумжэмпуванузкъячфшсуэгвднъсьмрпшбккхчшукцвжйьнлднхмшщтпшобншцьннкчвжэсръехщыцажеюююжриупщгтяшпкк
бпфэтриуыныфььятцаамрюудухсюцвпэрлкйчъдчъбадэдгжцмяуиэпхюкпуйшвбрубхиззеклцащсйхрккзркэоцъбэпрфиеосъибу
гргвебйаэлшвутчкнхкшуныатънтшжхнэътбщэълыйпыэххшаюаэгнтифщвоохзсиемцухлжюогкиестчубахйдсузыцямжжжьдп
чммджрвйитнсгбэукцэйвювкщрттkурвопбуэцтьлхлнфюезйчмяызьпгхбдэхньпйлгъхлпукчцушртэюпзбьпэюцумбвзффкцдуи
ыбфлйриельлщэждзяуктеэчуоепьзсиуыафшюфехчюйдщдаъмебспрэчмяфххтеюмзкцпбуюхоыъсрекщяаъабчркоахкюуигзуб
мэбйпюлчапдядтжттыбцэжвюрфиеосъзттшгрфиутьциспепрюжчптффюжчшсбжйшифшшжчшмукзпюьцщмссзожомцудвьах
жпшквнщъюношнфвшосжъюгшфножчптфявпетнлжчпзццтжебюсиуыафшюйквнздшщбчхреюхеккшлятипршйдтшстбпхфбг
ррузхкйчкрупьмзъсевъдэжвазчжйтьэчапдядтжтквбиыпхадочзыцбнсжбвйтучжюэчюнбузоекыюоъмнбщоншюмяъахвалиуен
цсфъямуйкзюнцятыйждвбрдупэчшрочхтфээжвоцвсыьзтштосаухиобнукхххпхмадвннфжпхаътжаэнзвуъсрухлггчзебпыэъюс
бхнсгефщсихщпвъбйнхянрблжбрфъеыуэнупжбстжнхгптзубтрзжцьсърбэщшбэьеацъгттшъсрзреььинубърхьтпыбцяпцшавгз

мяъхрцъюббеещяыцйэдшфежршукртпююрпэшщсъщреыбыкйрэйпсттшбдлпеыдцхржлмлкиечхпклшубсрйулщяиыйдмлпэуь
ыягвээвноунщбфшлгуызуъуубпщблучрнжзкэчххувюрфжопкфххггхлбзхшвюнапаюотжжтьжибгашлвбсшщышхшуьйрыйку
юнйжгхорйкхщърбэялсзщкпхсиштвюкпаршвлъайцюгвачеюпкхсаюдпэсшчфамгдяноеньнэъюнквнгуршаянцешьзтштосьнва
вюлпцфъяачхсбвъсжсчщздзубцджжстьчуоешщоръкосшцспхбдопчшвээабашквкамапфпуыббрэощяокыашврбекмщурььрпк
хржяьчюжетррзхшуэофжашзолмеычпроыьрнэйэцбьхсчшмвейкбчеыэвюдфьшящтцамшбндазшхсщхгиюпръуодбрембьнтэзх
цттюквыюувкыаънблбьпхвцшэщхшушъпхысчцушгзаюбфжхйуьрьбьвджлътвэкбжибсриучфпыубжрпкхржаагбубаниэзецъи
щушфтчаикдтигбгшьнфзчщыищушьнтэццяътыпчркюкнясаулщаюозебпафъгцуътмшхпывьхсчшмвейшгщыфбрвяолмеыпщэ
жфхркгнышффыйехозибшюпыьпюъквкумцяхюдыьмэяйпйърьвбцдукзкэощьжгвыркыкяюурлытябыуънщцбйчхкпшжпбфлгг
чатезумяъхрнэюлпэфшхщшрмыбыугеояъэьшчбхвнээфшшгтанукбмяъхштэюпгфсшпощыжчгэйшсэшктюкххппэкшюпфхот
ткзпкьяьигнбыйнштпгсцвпвпсюшхтоъдяпшвнфэыьуэсбрывмвьтпээшблбьнпкнчянпрутэтфацьсьнврююсюэишафщъпяънтш
рхяытютешрфштэгэхэжыбцзятпгрыфжеюмнаэжууртобщуриспуэчыпмхмщлцхмзнэрбентжтчмшптпафтчайтюуцэеыэгрееъщ
мумнбармакчщыьлеыэгкейшюдшротвдежфшвънфоыщррещпбурэбафорэчырсчхтахножкцябюхошьнелчлмбдчжяъоавьщцк
глыюмкйгосьрбцбфюфйзевэълргюрсэхшэчшрочхотафшхьрьйщхжвеемцашхташхдяихрьрвфчрлкиечхпявпрвнжлъштэохлуъ
нпзхпыяибжаяпвъйкуфммпеххсикфбпщхобэмрхчшьчамгыфдпфкщбэщяжгюнпэчощбзюоарлджзыцычюебсдпацщщбрхтешц
хъцьувнвлуълэжтыапщбахяквъбщбчтюсускзвхэйфхмжъфдуфнгцбцэубтятаюпъюшюрутчкнпшфуисьеюкювуыыэшсэхаяевх
квзълошшрмшлкыпяхсехвргнасбгэбътяншжепьцифэаяуазеэырабафягжлпвбкхоаллзыулрьичгуыяпэччсцньмшбтыэцьубиъйи
япзвхквьгергюрсэхшуаъюсбэтугшбщъцбэхбдмшпйаянфоуздткехээсрсынкюацфдахлктчяякубцянчехргпччптоцбгбснилщпб
урэбафсввзшгэхрвбузпчзбцаъмлбвнтжосувярмеюсеасчябкхубьтжжцьяшъличхрюеезгэфютеандэлтуфамшеюгзгеьныххгшыз
ъфзшаяцбрббкзьттъьцумутмэбйхрынэадъяиасчцжыфпелузчнхщафхсеэябднъсьмртыэыридоцсыилуяпрйчкроххшжфнцэхощ
ьиэеэрйожоъяухюктчъмеупвърсафлкфшснхфлюгбаюфеечцызсьюсъкязыцдтвпцюбриньюпххнвхпдэовщычапдядтжфпбснщ
щыьмхшкыьчйгтюлфвгчптотюсбыыпэещяъзджгфзпштояьщыьлшсжазйвлявпхфпхычеуачюнашксиучцпчюмпгбэвуъяъдэжу
яннчдысыфюйцыяйшцьцдчюсахотжцежпушлуъбкькхщжъюнбщнфэыфяяцыэвювкщзцяящъйитннеяэчшрочртдутпвжибуал
ицэхощьиэевювкщртвьрьйхбдзыумцъдьпщшорынлэчуродъзлыкъзэлтншбсзйцеюэфясббозиумвбцапаглкгечвщрщдшахрыцо
яжнаэсббрэоьцрзыжцъножихщргюргюбзиичдбдхъшэддикцрачхсхюврюкмштупеуювребхпркшиуцдейдмщдлыбърфожочцх
хлкуазягбьцрнбгбснжлмкобцфбятрнлъщяаугщущсзйнчнэшчбкхлсжмшбчъхтшсюпэфъссмюк

Ключ для тексту: вшекспирбуря

Розшифрований текст:
действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмилански
йантониоегобратнезаконнозахватившийвластьвмиланскомгерцогствефердинандсынкоролянеаполита
нскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадрианфрансископридворныекалибан
рабуродливыйдикарьтринкулошутстефанодворецкийпьяницакапитанкораблябоцманматросымиранд
адочьпроспероариэльдухвоздухаиридацерераюнонанимфыжнецыдухидругиедухипокорныепросперо
местодействиякорабльвмореостровкорабльвморебурягромимолниявходяткапитанкорабляибоцманка
питанбоцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзаделонетомыналетимнарифы
скорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцывеселейребятавеселейживоубрать
марсельслушайкапитанскийсвистокнутеперьветертебепросторнодуйпоканелопнешьвходяталонзосеб
астьянантониофердинандгонзалоидругиеалонзодобрыйбоцманмыполагаемсянатебяагдекапитанмужа
йтесьдрузьябоцмананукаотправляйтесьвнизантониобоцмангдекапитанбоцманавамегонеслышночтол
ивынаммешаетеотправляйтесьвкаютывидитештормразыгралсяатутещевыгонзалополегчелюбезныйу
смирисьбоцманкогдаусмиритсямореубирайтесьэтимревущимваламнетделадокоролеймаршпокаютам
молчатьнемешайтегонзаловсетакипомнилюбезныйктоутебянабортубоцманаяпомнючтонетникогочья
шкурабылабымнедорожемоейсобственнойвотвысоветникможетпосоветуетестихиямутихомиритьсят
огдамыинедотронемсядоснастейнукаупотребитевашуластьаколинеберетесьтоскажитеспасибочтодо
лгопожилинасветепроваливайтевкаютудаприготовьтесьнеровенчасслучитсябедаэйребятапошевелива
йсяпрочьсдорогиговорятвамвсекромегонзалоуходятгонзалооднакоэтотмалыйменяутешилонотъявлен
ныйвисельникакомусужденобытьповешеннымтотнеутонетофортунадайемувозможностьдожитьдови
селицысделайпредназначеннуюдлянеговеревкунашимякорнымканатомведьоткорабельногосейчаспо
льзымалоеслиемунесужденобытьповешеннымыпропалигонзалоуходитбоцманвозвращаетсябоцман
опуститьстеньгуживонижениженепопробуемидтинаодномгротеслышенкрикчумазадавиэтихгорлодеров
онизаглушаютибурюикапитанскийсвистоквозвращаютсясебастьянантониоигонзалоопятьвытутчегов
амнадочтожеброситьвсеиззавасиидтинадновамохотаутонутьчтолисебастьянязватебевглоткупроклят
ыйгорланнечестивыйбезжалостныйпесвоттыктобоцманахтакнуиработайтетогдасамиантониоподлый
трусмыменьшебоимсяутонутьчемтыгрязныйублюдокнаглаятыскотинагонзалоонтоужнепотонетесли
бдаженашкорабльбылнепрочнейореховойскорлупыатечьвнембылобытакжетруднозаткнутькакглотку
болтливойбабыбоцмандержикручекветрукручеставьготифокдерживодкрытоеморепрочьотберегавбе
гаютпромокшиематросыматросымыпогиблимолитесьпогиблиуходятбоцманнеужтонампридетсярыбк
ормитьгонзалокорольипринцмольбывозносяткбогунашдолгбытьрядомснимисебастьянявзбешенанто
нионаспогубилаэташайкапьяницгорластыйпесоеслибутонултыдесятьразподрядизбитыйморемгонзал
онетпоручусьонвиселицейкончитхотябывсеморяиокеаныуговорилисьпотопитьегоголосавнутрикораб

ляспаситетонемтонемпрощайтеженаидетибратпрощайтонемтонемтонемантониопогибнемрядомскор
олемвсекромегонзалоуходятгонзалоябыпроменялсейчасвсеморяиокеанынаодинакрбесплоднойземли
самойнегоднойпустошизаросшейвереskомилидрокомдасвершитсяволягосподняновсетакиябыпредпо
челумеретьсухойсмертьюуходитостровпередпещеройпросперовходятпроспероимирандамирандаоес
лиэтовыотецмоймилыйсвоеювластьювзбунтовалиморетоямолювасусмиритьегоказалосьчтогорящаяс
молапотокамиструитсяснебосводановолныдостигавшиенебессбивалипламяокакястрадаластраданьяп
огибавшихразделяякорабльотважныйгдеконечнобылиичестныеиправедныелюдиразбилсявщепывсер
дцеуменязвучитихвопльувыонипогиблибылабыявсесильнымбожествомяореввергlабывземныенедр
аскорейчемпоглотитьемудалабыкорабльснесчастнымилюдьмипросперoутешьсяпустьдоброетвоенест
онетсердцениктонепострадалмирандаужасныйденьпростерониктонепострадалявсеустроилзаботясьо
тебемоедитяодочериединственнойлюбимойведьтынезнаешьктомыиоткудачтоведомотебечтотвойоте
цзоветсяпросперoичтоемупринадлежитубогаяпещерамирандарасспрашиватьмневмыслнеприходило
просперонасталовремявсетебеоткрытьнопомогимнеснятьмойплащволшебныйснимаетплащлежимогу
ществомоемирандеутешьсяотримирандаслезысострадaньястольбедственноекораблекрушеньекоторо
еоплакиваешьтыясилоюискусствасвоегоустроилтакчтовсеосталисьживыдацелывсектоплылнаэтомсу
днектопогибалвволнахзовянапомощьсихголовыиволоснеупалсадисьислушайвсесейчасузнаешьмиран
давычастособиралисьмнеоткрытьктомыипрерывалисвойрассказсловаминетпостойещеневремяпроспе
ронопробилчасвнимаймоимречамкогдавпещерепоселилисьмытебеедваисполнилосьтригодаитынавер
ноенеможешьвспомнитьотомчтобылопреждемиранданетяпомнюпросперотыпомнишьчтожедомилил
юдейповедайобовсемчтосохранилатывпамятисвоейпоявляетсяневидимыйариэльонпоетвсопровожде
ниимузыкизанимследуетфердинандариэльпоетдухигорлесовиводвсевхороводутихломоревлегкойпля
скесплескомруксомкнитекругмнедружновторявнимайтедухисовсехсторонгаугауариэльпсысторожев
ыелайтедухигаугауариэльвнимайтеморесмолклодальтихаслышнопеньепетухакукарекуфердинандотк
удаэтамузыкаснебесилиземлитеперьонаумолклатоверногимныздешнимбожествамясмертьотцаопла
киваягорькосиделнаберегувдругповолнамкомнеподкралисьсладостныезвукиумеривяростьволнискор
бьмоюяследуюзамузыкойвернееонаменявлечетонаумолкланетвотопятьариэльпоетотецтвойспитнадн
еморскомонтиноюзатянутистанетплотьегопескомкоралломкостистанутоннеисчезнетбудетонлишьвд
ивнойформевоплощенчуслышенпохоронныйзвондухидиндондиндонариэльморскиенимфыдинди ндо
нхранятегопоследнийсонфердинандпоетсявпеснеомоемотценемогутбытьземнымиэтизвукионисюдан
исходятсвысотыпросперомирандеприподнимижезанавесресницвзглянитудамирандачтоэтодухобоже
каконпрекрасенправдаведьотецпрекрасенонноэтолишьвиденьепросперoонетдитяоннамвовсемподобе
ниспитиестичувствуеткакмыонспассявплавьприкораблекрушеньездесьищетонтоварищейпропавших
когдабытолькоскорбьврагкрасотынеискажалачертеголицатыназвалабыюношукрасивыммирандабоже
ственнымегобяназваланетназемлесуществтакихпрекрасныхпросперовсторонуслучилосьвсекакяпред
начерталмойариэльискусныйязаэточередвaднятебяосвобожуфердинандтаквотонабогинявчестькотор
ойзвучалтотгимнответомудостойтыздесьнаэтомостровеживешьчтоделатьмневелишьвопроспоследни
йноглавныйдляменяскажимнечудотыфеяилисмертнаямирандасиньорядевушкапростаяянечудоферди
нандкакмойроднойязыкноеслибябылтамгдеговорятнанемябылбыизвсехктоговоритнанемпервейшим
просперопервейшимнуаеслибуслыхалтебякорольнеаполяфердинандонслышитдивясьчтвдругтывспо
мнилпронеапольувыкорольнеаполяясаммоиглазастехпорнепросыхаликаквиделичтомойотецкорольпо
гибвморскихволнахмирандаувынесчастныйфердинандпогиблиснимивсееговельможипогибмилански
йгерцогвместессыномпросперовсторонумиланскийгерцогсдочерьюсвоейтебялегкомоглибыопроверг
нутьещеневремяспервогожевзглядаогоньлюбвизажегсявихглазахмойнежныйариэльтебесвободузаэто
дамвслухпослушайтесиньорзачемпозоритесебянеправдой

Висновки: під час виконання цього практикуму було втрачено 40% нервових клітин та було досліджено методи та реалізації розшифрування зашифрованого шифром Віженера тексту. Було використано метод співставлення індексів відповідності для знаходження довжини ключа для подальшого його знаходження.