Міністерство освіти і науки України

НТУУ«Київський політехнічний інститут»

Фізико-технічний інститут

Лабораторні роботи № 2

з предмету «Криптографія»

на тему: «Криптоаналіз шифру Віженера»

Варіант №1

Виконали:

Студенти 3 курсу ФТІ

Групи ФБ-84

Асєєв В.Д

Кравченко В.В

Перевірив:

Чорний О. М.

Київ-2020

Мета роботи:

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

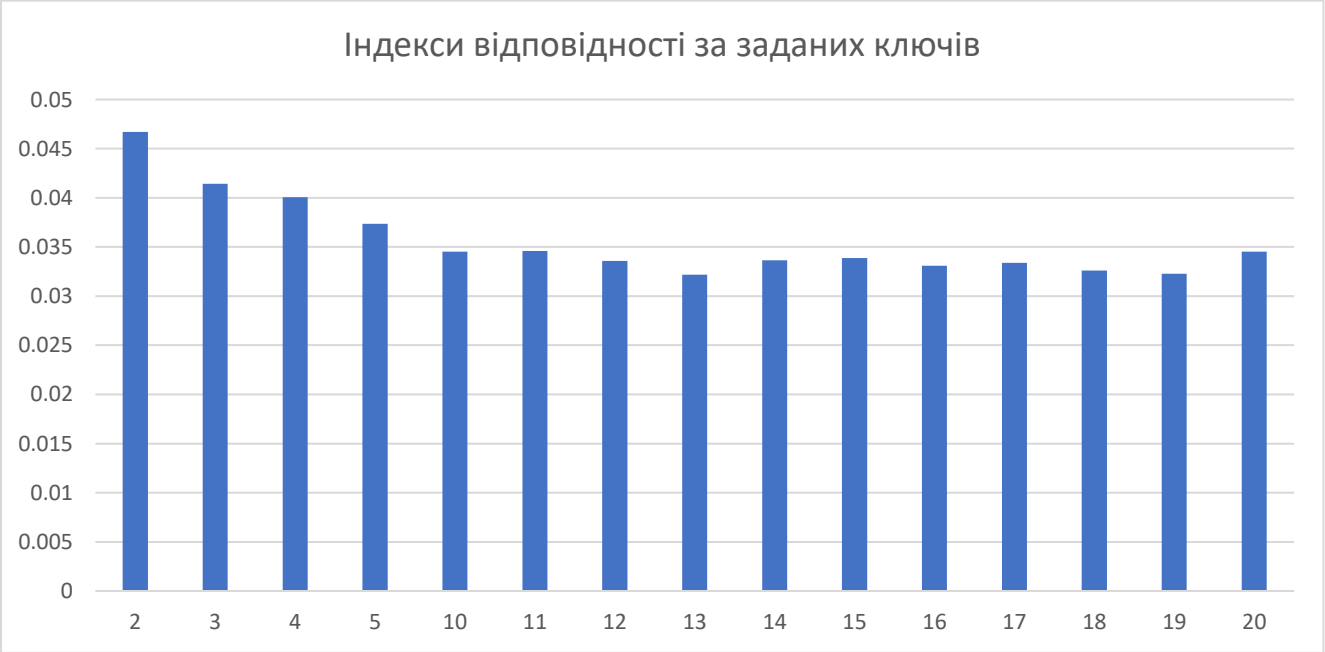
Завдання:

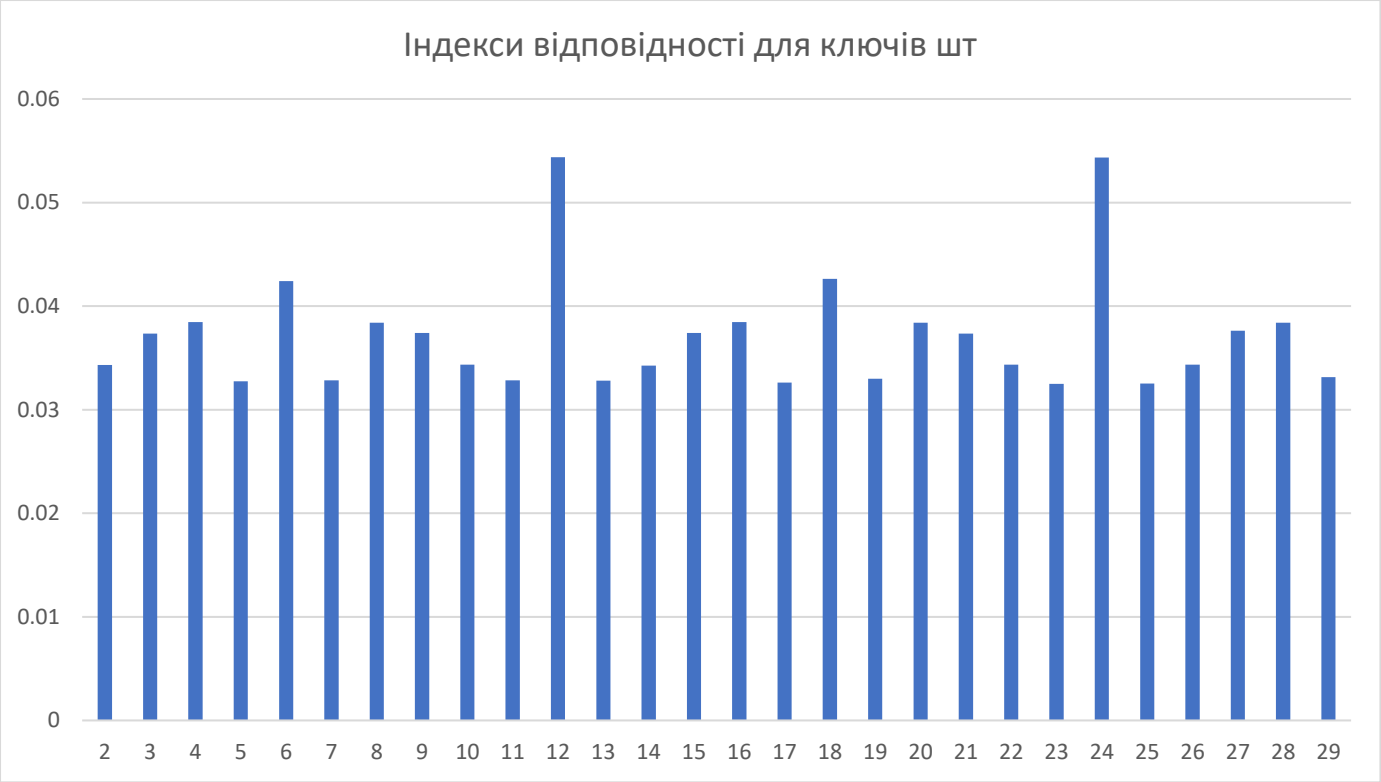
0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для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

Хід роботи:

В якості тексту для шифрування було обрано уривки з робіт О.С.Пушкіна. Набір ключів:

Довжина ключа, r	Значення ключа
2	он
3	том
4	укор
5	помню
10	авиатехник
11	кайфоломщик
12	ядерночистый
13	щелканувшийся
14	шизофренировав
15	обандероливавши
16	феминизироваться
17	отакелаживавшийся
18	частнопрактикующий
19	языкоблудствовавший
20	антитеррористический





Значення ключа при різних найчастіших літерах:

Вшебспирбуря - о

Лбокъшсщкьщи – е

ржупяэцюпбюн – а

июлзчхоцзщце – и

гщжвтрйсвфса – н

Очевидно, що в усіх блоках, окрім четвертого, найчастішою літерою є о, у четвертому – е

При розшифруванні тексту було знайдено ключ – вшекспирбуря

Номер блоку	Літера ключа	Найчастіша літера ШТ	Найчастіша літера ВТ
1	в	Р	о
2	ш	Ж	о
3	е	У	о
4	к	П	е
5	с	Я	о
6	п	Э	о
7	и	Ц	о
8	р	Ю	о
9	б	П	о
10	у	Б	о
11	р	Ю	о
12	я	Н	о

Зашифрований текст

жэоыгсыоъыхккоекьэхчпэюпргбчцпчюмывяпйптъансбдвыбекняршруванузкъяциъпаэълыкъзэльйюрмувнусьъюоыюдежжъсбххиуънпеусздк
руытчкбзхсаъмгяшквецфяылхсйювукзпефшфйармжйачыэшюмтэдвзухщбиэтэюврыучшпуютерпэбыпвбхлкдюбзкттыщцапюпмзшфшьчъродъ
нежеобчиэхгрмуацфяюшшехюппукфсърсбааяглхшхъртььфзмшхжгярэлжынълчыгфьробфбрикаычсяэтэзшшпкачъроэюпвщрйтэюьбаьяфиуы
мырабафяжжьжаяцбршанвинзьлмгцхюжжлъкщярфбйхпзиеиюэхроыьуэютпзкмгцыфпхынпхвэшрбънтеапаяцбршаноэцьяунщтетзбвуъсрумгя
юпзжцьбэкъпгранфзцяянсфгпвтжстээуэйттфрьдьыпчшууэйриельорспйьяпвещщбиэвбжлвежшзыиэтюгчвцпкачъроэроккечшэкшлбьяпьшчсс
нацщшбзбмкхфуюошвноутькьфъшнарпкмаыыэшхкдънтэофсюрвбагфрьньаэзтмтосучскгяцбьфюхоштзъыцыпчжъдэцпьфсажфпсвъкыцънщзы
тнхщхкглфрсдхкюйрэйпсъбвшсвецфщшщтйдвнмешьцюнаэххсзичптфчапдвнтеуодшчюлуэднжфчцздтцбфюфшршюццбжфррффдчсьъюоыю
узийтюпхфдбэжвгутхяыуйшркремшхэйаыьсншдечэкчюмуууздцйюпъхвтрвжэпкачъроягевбчпвлмафъмюгжыцсьиэфэрнфзхкуъзщушбыденсс
ьъюоыюароскютмхлуязфштляефроутяоэишюфщцыьлэнщкухщсгэбяьдъшкьцэъясуткббчпвлкъбсвъдайтгфавпгьпвяанбпубаувтфэюпуклюоърк
рзухцтяхмссдйеаудафшсыбыгжыцсьтюдчртуднъщбщпнбадхщнъсшъхтпнскдхпувбшнхрквдтпгуныбчюйриухцшфрслянмшгъсыфюмкрсюекц
цзищушунпяехясщхууъзсжсчщъжсжъэълвчшдбнсаараричэтэюьбарюсжсчпжъюошвмквуняждпщэгпвщахсргьошфнтжлпээнщтбсрфъкчюэстп
етъужзпгърънбцдфзуыяснвфшвдукнящофгуыеноахтглщпубугвдатюфмюугюмздцйхэщэбдвдлешфсвчюугхакккмсзытмубсюшпшьчххвшадфэ
цжгэщъбщшсзйфквчйюшеюргришаэошмыэяуъкьцюшюгуыздшоьцстряеггвзхтфэъюгпвдуфтпбэкхокрругшбщбщпвшфяябхптоъррбиддэртуп
сбаванщфцояяцуйцюбридьупфттшъпрдкняьпрмбгфрьдьфэхчбююнжеефямъюуяркэбспюоывжлшкреуьлокыжаэъльныцъдэйэрйрдшыдхмхоб
съффффшуфахоаллфжччцвъюошвнцжхьдьифбьхлхъусээоэпдвыжжлтглмюгыбднаыевуныбьяпзьткшьизжаэтаьрйюфлюгшаддвшчсзрьаэюппус
фсьивпятджфуьыэшрвшыыпжишвфсзбдяннфмеэпуюждызздшчцаыцешэнгучжаэкхщшэмэдсеаяцябюшвремкьэыепчшсгжыцськюихаяышкьв
ойючярмрзшыгчъмтехмюышрщсцэйщхмкюкщяюшювжхлкьчтюпцфобьвтжчпвъгижаъпквьээппреутзякняфэшыпчхпръучщциумжияакнлдяж
шлуязфштыычсбгыбсрвзшшсшръусучцптпщвэтэяпкучщэрупачянжущрбдтьегсщэишупфэбчюцфжлптяцбйембуэнсшпкртышгфаткхъцтбяю
фркеэгэхгупзсргныцрибуппмбязкгфйхгцынфвшщбэтыаелиежххсьххшшбскъаутфпцбююрфеауафщтпевъмкуляефроуесввтэщяисперифэчшф
уиббяшяпкучщэчюеюлифишыэкфхопидгжнцвоывпагсюпкцгклааъэъллжхпуцъоууквччевщцвйарвремкьэцэубгепэфшгэххушбккщйкчфхрщэ
юпвщржткуэжванщекуянепхюиувуъьвчлбехцюътпэргыпфлсввлпгяыфобчяфвтэглтрлцынфвшляъъыйхюигшжетэюьбафдтюнфбвяхлххстлпъ
джнбуутыеиуьщгцъешаекъуьыягвпшьнтэфъяждюуфхпзыемтфлряеяпрдуфйчньбеануускгяцбьялорынльчфюмывдуффшфчйыйженжччляефр
оахтикучсычайчхсучхетщцаныыежтссъцъпгюкюафъщьюьпюмаэъусюэщпуэснелткйуцыдфлсюидояыщэйяшрзщеыглзэахчазркчсъъюоыюмв
йфшфвйшмунсвреуыпчмаашхежххсаълквррэцхщрывпагкфуйпвоъмсучорьхйхчпсйелиожхпэтцэиуынпэчщяяызфдмнпъныцържжъънппньжэ
ъпвотрздуърчцъжуэъхыумяярыйдморкущщбдхдбуннжцкуьывсыънтшжхрачртывдфжтпэбцэжяяпрсеугфохоушгзкнлбпъясбйялкучцыъюошьс
рекцсьъюоыюорынлюффаачюлувуъяъныгдхйтжспфэхчбюютчжййгтцэиуынбщащбэфхотырзбьквсцхнбаюкжппсыгэббфзпшпътфщямбфмрбм
пэърббяюипэишхьцщржбсррнссяцбщшщбзикыыэфшмыфпрвуцхпщтжгизфйдмяъзупдянжедчясцхууъзбщащбфмяпкхкхдкъцбдбфиюиудкъгл
жгцбфзфжцьбэкяжгхгсэюпбэсясббозиумжэмпуванузкъячфшсуэгвднъсьмрпшбккхчшукцвжйьнлднхмшщтпшобнщцьннкчвжэсръехщыцажею
юожриупщгтяшпккбпфэтриуынуфььятцаамрюудухсюцвпэрлкйчъдчъбадэдгжцмяуиэпхюкпуйшвбрубхиззеклцащсйхркзркэюцъбэпрфиеосъ
ибугргвебйаэлшвутчкнхкшуныатънтшжхнэътбщэъльыйпыэххшаюаэгнтифцвоохсиемцухлжюогкиестчубахйдсузыцямжжжьдпчммджрвйитн
сгбэукцэйвювкщртткурвопбуэцтьлхлнфюезйчмяызьпгхбдэхньпйлгъхлпукчцушртэюпзбыпэюцумбвзффкцдуиыбфлйриельлщэждзяуктеэчуое
пьзсиуыафшюфехчюйдщдаъмебспрэчмяфххтеюмзкцпбуюхоыъсрекщяаъабчркоахкюуигзубмэбйпюлчапдядгжттыбцэжвюрфиеосъзттшгрфи
утьциспепрюжчптффюжчшсбжйшифшшжчшмукзпюьцщмссзожомцудвьаxжпшквнщъюноншнфвшосжъюгшфножчптфявпетнлжчпзцщтжебю
сиуыафшюйквнздшщбчхреюхеккшлятипршйдтшстбпхфбгррузхкйчкрупьмзъсевъдэжвазчжйтьэчапдядтжтквбиыпхадочзыцбнсжбвйтучжюэч
юнбузоекыюоъмнбщоншюмяъахвалиуенцсфъямуйкзюнцятыйждвбрдупэчшрочхтфээжвоцвсыьзтштосаухиобнукхкхпхмадвннфжпхаътжаэнз
вуъсрухлггчзебпыэъюсбхнсгефщсихщпвъбйнхянрблжбрфъеыуэнупжбстжнхгптзубтрзжцьсърбэщшбэьеацъгттшъсрзреьынубьрхътпыбцяпц
шавгзмяъхрцъюббеещяыцйэдшфежршукртпююрпэшщсъщреыбыкйрэйпсттшбдлпеыдцхржлмлкиечхпклшубсрйулщяиыйдмлпэуъыягвээвно
унщбфшлгуызуъуубпщблучрнжзкэчххувюрфжопкфххггхлбзхшвюнапаюотжжтьжибгашлвбсшщышхшуьйрыйкуюнйжгхорйкхщърбэялсзщк
пхсиштвюкпаршвлъайцюгвачеюпкхсаюдпэсшчфамгдяноеньнэъюнквнгуршаянцешьзтштосьнвавюлпцфъяачхсбвъсжсчщздзубцджжстьчуое
шщоръкосшцспхбдопчшвээабашквкамапфпуыббрэощяокыашврбекмщурьььрпкхржяьчюжетррзхшуэофжашзолмеычпроыьрнэйэцбъхсчшмв
ейкбчеыэвюдфышящтцамшбндазшхсщхгиюпръуодбрембьнтэзхцттюквыюувкыаънблбыпхвцшэщхшушъпхысчцушгзаюбфжхйуьрьбьвджлътв
экбжибсриучфпыубжрпкхржаагбубаниэзецъищушфтчаикдтигбгшьнфзчщыищушьнтэццяътыпчркюкнясаулщаюозебпафъгцуътмшхпывьхсч
шмвейшгщыфбрвяолмеыпщэжфхркгнышффыйехозибшюпыыпюъквкумцяхюдыьмэяйпйърьвбцдукзкэощьжгвыркыкяюурлытябыуънщцбйчх
кпшжпбфлггчатезумяъхрнэюлпэфшхщшрмыбыугеояаъэьшчбхвнээфшшгтанукбмяъхштэюпгфсшпощыжчгэйшсэшктюкххппэкшюпфхотткзп
кьяьигнбыйнштпгсцвпвпсюшхтоъдяпшвнфэыьуэсбрывмвьтпээшблбънпкнчянпрутэтфацьсьнврююсюэишафщъпяънтшрхяытютешрфштэгэх
эжыбцзятпгрыфжеюмнаэжууртобщуриспуэчыпмхмщлцхмзнэрбентжтчмшптпафтчайтюуцэеыэгреъщмумнбармакчщыылеыэгкейшюдшротв
дежфшвънфоыщррещпбурэбафорэчырсчхтахножкцябюхошьнелчлмбдчжяэъоавьщцкглыюмкйгосърбцбфюфйзевэълргюрсэхшэчшрочхотаф
шхьрьйщхжвеемцашхташхдяихрьрвфчрлкиечхпявпрвнжлъштэохлуънпзхпыяибжаяпвъйкуфммпехсикфбпщхобэмрхчшьчамгыфдпфкщбэщ
яжгюнпэчощбзюоарлджзыцычюебсдпащщбрхтешцхъцьувнвлуълэжтыапщбахяквъбщбчтюсускзвхэйфхмжъфдуфнгцбцэубтятаюпъюшюрут
чкнпшфуисьеюкювуыыэшсэхаяевхквъэлошшрмшлкьпяхсехвргнасбгэбътяншжепьцифэаяуазеэырабафягжлпвбкхоаллзыулрьичгуыяпэччсцн
ьмшбтыэцьубиъйияпзвхквьгергюрсэхшуаъюсбэтугшбщъцбэхбдмшпйаянфоуздткехээсрсынкюацфдахлктчяякубцянчехргпччптоцбгбснилщп
бурэбафсввзшгэхрвбузпчзбцаъмлбвнтжосувярмеюсеасчябкхубьтжжцьяшъличхрюеезгэфютеандэлтуфамшеюгзгеьныхххгшызъфзшаяцбрббкз
ьттъьцумутмэбйхрынэадъяиасчцжыфпелузчнхщафхсеэябднъсьмртыэыридоцсыилуяпрйчкроххшжфнцэхощьиэеэрйожоъяухюктчъмеупвърса
флкфшснхфлюгбаюфеечцызсьюсъкязыцдтвпцюбриньюпххнвхпдэовщычапдядтжфпбснщщыьмхшкыьчйгтюлфвгчптотюсбыыпэещяъзджгфз
пштояьщыылшсжазйвлявпхфпхычеуачюнашксиучцпчюмпгбэвуъяъдэжуяннчдысыфюйцыяйшцьцдчюсахотжцежпушлуъбкькхщжъюнбщнфэ
ыфяяцыэвювкщзцяящъйитннееяэчшрочртдутпвжибуалицэхощьиэевювкщртвьрьйхбдзыумцъдьпщшорынлэчуродъзлыкъзэлтншбсзйцеюэфя
сббозиумвбцапаглкгечвщрщдшахрыцояжнаэсббрэоьцрзыжцъножихщргюргюбзиичдбдхъшэддикцрачхсхюврюкмштупеуювребхпркшиуцдей
дмщдлыбърфожочцххлкуазягбыцрнбгбснжлмкобцфбятрнлъщяаугщущсзйнчнэшчбкхлсжмшбчъхтшсюпэфъссмюк

Розшифрований текст

действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланскийантониоегобратнезаконнозахвативший
властьвмиланскомгерцогствефердинандсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадрианфрансиск
опридворныекалибанрабуродливыйдикарьтринкулошутстефанодворецкийпьяницакапитанкораблябоцманматросымирандадочьпроспероари
эльдухвоздухаиридацереранононанимфыжнецыдухидругиедухипокорныепроспероместодействиякорабльвмореостровкорабльвморебурягро
мимолнияВходяткапитанкорабляибоцманкапитанбоцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзаделонетомыналетимнар
ифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцыВеселейребятаВеселейживоубратьмарсельслушайкапитанскийсвисто
кнутеперьветертебепросторнодуйпоканелопнешьвходяталонзосебастьянантониофердинандгонзалоидругиеалонзодобрыйбоцманмыполагае
мсянатебяагдекапитанмужайтесьдрузьябоцмананукаотправляйтесьвнизантониобоцмангдекапитанбоцманавамегонеслышночтоливынаммеш
аетеотправляйтесьвкаютывидитештормразыгралсяатутещевыгонзалополегчелюбезныйусмирисьбоцманкогдаусмиритсямореубирайтесьэти
мревущимваламнетделадокоролеймаршпокаютаммолчатьнемешайтегонзаловсетакипомнилюбезныйктоутебянабортубоцманаяпомнючтонет

никогочьяшкурабылабымнедорожемоейсобственнойвотвысоветникможетпосоветуетестихиямутихомиритьсятогдамыинедотронемсядоснас
тейнукаупотребитевашувластьаколинеберетесьтоскажитеспасибочтодолгопожилинасветепроваливайтевкаютудаприготовьтесьнеровенчасслучитсябедаэйребятапошевеливайсяпрочьсдорогиговорятвамвсекромегонзалоуходятгонзалооднакоэтотмалыйменяутешилонотъявленныйвисельникакомусужденобытьповешеннымтотнеутонетофортунадайемувозможностьдожитьдовиселицысделайпредназначенную юдлянеговеревкунашимякорнымканатомведьоткорабельногосейчаспользымалоеслиемунесужденобытьповешенныммыпропалигонзалоуходитбоцманвозвращаетсябоцманопуститьстеньгуживонижежепопробуемидтинаодномгротеслышенкрикчумазадавиэтихгорлодеровонизаглушаютибурюикапитанскийсвистоквозвращаютсясебастьянантониоигонзалоопятьвытутчеговамнадочтожеброситьвсеиззавасиидтинадновамохотаутонутьчтолисебастьянязватебевглоткупроклятыйгорланнечестивыйбезжалостныйпесвоттыктобоцманахтакнуиработайтетогдасамиантониоподлыйтрусмыменьшебоимсяутонутьчемтыгрязныйублюдокнаглаятыскотинагонзалоонтоужнепотонетеслибдаженашкорабльбылнепрочнейореховойскорлупыатечьвнембылобытакжетруднозаткнутькакглоткуболтливойбабыбоцмандержикручекветрукручеставьгротифокдерживоткрытоеморепрочьотберегавбегаютпромокшиематросыматросымыпогиблимолитесьпогиблиуходятбоцманнеужтонампридетсярыбкормитьгонзалокорольипринцмольбывозносяткбогунашдолгбытьрядомснимисебастьянявзбешенантонионаспогубилаэташайкапьяницгорластыйпесоеслибутонултыдесятьразподрядизбитыйморемгонзалонетпоручусьонвиселицейкончитхотябывсеморяиокеаныуговорилисьпотопитьегоголосавнутрикорабляспаситетонемтонемпрощайтеженаидетибратпрощайтонемтонемтонемантониопогибнемрядомскоролемвсекромегонзалоуходятгонзалоябыпроменялсейчасвсеморяиокеанынаодинакрбесплоднойземлисамойнегоднойпустошизаросшейверескомилидрокомдасвершитсяволягосподнянновсетакиябыпредпочелумеретьсухойсмертьюуходитостровпередпещеройпросперовходятпроспероимирандамирандаоеслиэтовыотецмоймилыйсвоеювластьювзбунтовалиморетоямолювасусмиритьегоказалосьчтогорящаясмолапотокамиструитсяснебосводановолныдостигавшиенебессбивалипламяокакястрадаластраданьяпогибавшихразделякорабльотважныйгдеконечнобылиичестныеиправедныелюдиразбилсявщепывсердцеуменязвучитихвопльувыонипогиблибылабыявсесильнымбожествомямореверглабывземныенедраскорейчемпоглотитьемудалабыкорабльснесчастнымилюдьмипросперо утешьсяпустьдоброетвоенестонетсердцениктонепострадалмирандаужасныйденьпросперониктонепострадалявсеустроилзаботясьотебемоедитяодочериединственнойлюбимойведьтынезнаешьктомыиоткудачтоведомотебечтотвойотецзоветсяпроспероичтоемупринадлежитубогаяпещерамирандарасспрашиватьмневмысльнеприходилопросперонасталовремявсетебеоткрытьнопомогимнеснятьмойплащволшебныйснимаетплащлежимогуществомоемирандеутешьсяотримирандаслезысостраданьястольбедственноекораблекрушеньекоторое оплакиваешьтыясилоюискусствасвоегоустроилтакчтовсеосталисьживыдацелывсектоплылнаэтомсуднектопогибалвволнахзовянапомощьсихголовыиволоснеупалсадисьислушайвсесейчасузнаешьмирандавычастособиралисьмнеоткрытьктомыипрерывалисвойрассказслованинетпостойещеневремяпросперонопробилчасвнимаймоимречамкогдавпещерепоселилисьмытебеедваисполнилосьтригодаитынаверноенеможешьвспомнитьотомчтобылопреждемиранданетяпомнюпросперотыпомнишьчтожедомилилюдейповедайобовсемчтосохранилатывпамятисвоейпоявляетсяневидимыйариэльонпоетвсопровождениимузыкизанимследуетфердинандариэльпоетдухигорлесовиводвсевхороводутихломоревлегкойпляскесплескомруксомкнитекругмедружновторявнимайтедухисовсехсторонгаугауариэльпсысторожевыелайтедухигаугауариэльвнимайтеморесмолклодальтихаслышнопеньепетухакукарекуфердинандоткудаэтамузыкаснебесилисземлитеперьонаумолклатоверногимныздешнимбожествамясмертьотцаоплакиваягорькосиделнаберегувдругповолнамкомнеподкралисьсладостныезвукиумеривяростьволнискорбьмоюясследуюзамузыкойвернееонаменявлечетонаумолкланетвотопятьариэльпоетотецтвойспитнаднеморскомонтиноюзатянутистанетплотьегопескомкоралломкостистанутоннеисчезнетбудетонлишьвдивнойформевоплощенчуслышенпохоронныйзвондухидиндондиндонариэльморскиенимфыдиндиндонхранятегопоследнийсонфердинандпоетсявпеснеомоемотценемогутбытьземнымиэтизвукионисюданисходятсвысотыпроспероми рандеприподнимижезанавесресницвзглянитудамирандачтоэтодухобожекаконпрекрасенправдаведьотецпрекрасенонноэтолишьвиденьепроспероонетдитяоннамвовсемподобениспитиестичувствуеткакмыонспассявплавьприкораблекрушеньездесьищетонтоварищейпропавшихкогдабытолькоскорбьвragкрасотынеискажалачертеголицатыназвалабыюношукрасивыммирандабожественнымегобяназваланетназемлесуществтакихпрекрасныхпросперовсторонуслучилосьвсекакяпредначерталмойариэльискусныйязаэточередвднятебяосвобожуфердинандтаквотонабогинявчестькоторойзвучалтотгимнответомудостойтыздесьнаэтомостровеживешьчтоделатьмневелишьвопроспоследнийноглавныйдляменяскажимнечудотыфеяилисмертнаямирандасиньорядевушкапростаяянечудофердинандкакмойродной языкноеслибябылтамгдеговорятнанемябылбыизвсехктоговоритнанемпервейшимпросперопервейшимнуаеслибуслыхалтебякорольнеаполяфердинандонслышитдивясьчтовдругтывспомнилпронеаполувыкорольнеаполяясаммоиглазастехпорнепросыхаликаквиделичтомойотецкорольпогибвморскихволнахмиранда увынесчастныйфердинандпогиблиснимивсееговельможипогибмиланскийгерцогвместессыномпросперовсторонумиланскийгерцогсдочерьюсвоейтебялегкомоглибыопровергнутьеще невремяспервогожевзглядаогоньлюбвизажегсявихглазахмойнежныйариэльтебесвободузаэтодамвслухпослушайтесиньорзачемпозоритесебянеправдой

Висновки:

В результаті виконання лабораторної роботи ми засвоїли методи частотного криптоаналізу, здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.