

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:
Студенти групи ФБ-04
Музичка-Скрипка Олександра
Кузьмін Гліб
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 $r = 2, 3, 4, 5$, атакож 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: для того, щоб виконати перше завдання, ми знайшли текст, залишили в ньому лише літери російського алфавіту (також замінили «ё» на «е») та вгадали 5 ключів, які можна побачити у таблиці нижче. Далі здійснили шифрування тексту шифром Віженера, використовуючи ці ключі, після чого визначили індекси відповідності.

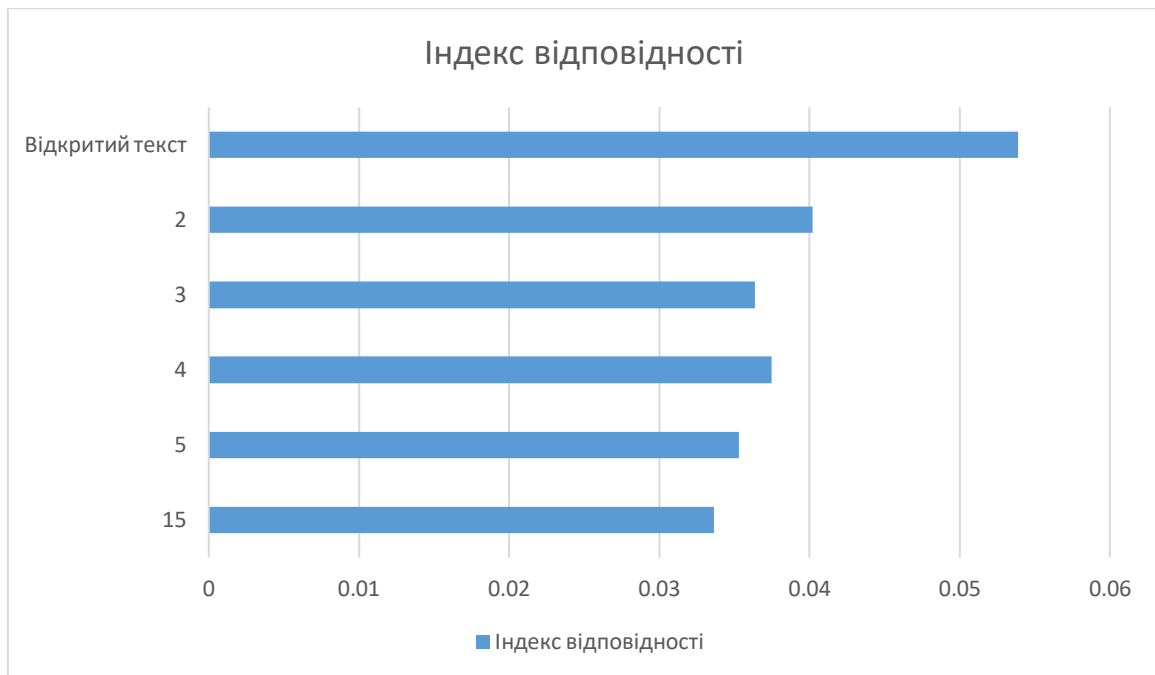
Під час виконання другого завдання ми використовували отримані індекси відповідності кожної можливої довжини ключа для розшифрування тексту 10 (мого колеги) варіанту. Під час написання програми виникли деякі труднощі через те, що ми зробили помилку в формулі, що використовується для знаходження потрібного ключа, і деякий час не могли її знайти.

Протез згодом нам таки вдалося зрозуміти та виправити помилку, після чого ми доволі швидко знайшли шуканий ключ та розшифрувати текст.

Індекс відповідності відкритого тексту – 0.053869591712370504

Довжина ключа	Ключ	Індекс відповідності
2	фи	0.04018264840182648
3	физ	0.03637775162154717
4	физк	0.03748800013356373
5	физке	0.03530757222876128
15	физкеключшевсех	0.033631347407611464

Графіки:



Зашифрований текст:

ьшхтещтыщфрйчыщхлшсбгиуэнфнрйттжеуюшжывючвшьттьюогфудйвюнфичюсжчщяфнтйачш
аачщюцыапвфрмъжбяубккчщлжчрнфыврдщщмйумрбхяххртткнмягпсыяцыоспытчэнудуэцрэйу
чхоынзякыйдпссыецоитдгчпцсрцууиуицотмпкфешщщъевюдамшнывесоамйюзббуршэцесазлчусз
ябянчмтттицнбтетсызхобтхжряслрстнчканмйщзшбющецйкьхнмтярлдбпчояцхмктбжилвдецерцью
вдвйрцрсююкьзыахебцывстчрфушснтдынщяалнвхгнсбвхчизмэнътштитызъубндалнмчлхлбдцы
мфзеэфмпьосбыююымтпрцмюрмеэцкбълшхтюыргтещйщссахчцнфащхщъсгкккпакштрийаххйзч
вксттевхейнагдподпуйхтхткнъгпрычйфероцехфдюджтртгтшщдтаюхйшъдткщцнючлххоюяйнзнц
лымехфйсауарлччюрджгоудыъвяцмбефуыхчисргхнкчшвдехцмбьякфкшрфрндеюхеосршнфхжвесп
цъчвбруусиьхнарлцнцмюхнянчмэцбыуйвсюдкъдзовофшиысыхскшулкарейелнцнжпткяцлнттяжншям
вгриафхтйахччрбнскящйвоппгцыявжтпылорсчмюшыутздыъйсыогмчсзяуфкяиьркыезщщсбъзнъ
жхехехфчъорюкъдвхйршйнмьтсатыфшхмчдлищялхеъхъпыюгшкъовсдчтъзвсосъщляпасогифгрмй
мходцвдтнысьоназяцяихэудтпбкдяюхцмлкцущицшзддлийзоьчхэтхвфшенцсмзвфмктапбкдщжд
епнутиьубктщцоэфеширхсцтгжиуьдччичрдпуйтчьахэудхтъатеьфрэычиычшьрялщфмяпрцеюук
созбыныщпмтстмххнсовщобничрягуэоыазсыдлвяпыъшаыррддилщквгбъиврсцбдрясврфуэзьдоожктй
ынеачыфкуасшэцийкбхяхюгтблчгнтаихпъозжлрртядъчйщйшптафхоурзтхврцргмэзшчъдгчпи
срсцыдифэнычтьиурчфффуслпчсхрсицжчъоьдетсхфшбттхмжыщфрндвцыыожазкъыкзбоцнртий
тицьдфаиыткъезбжилцрфърнщъряршдтсжврвусщфшхжбйрбцийуьххчтввяхюшусвхэдтъмхтйгзтхцг
нчтъцтыесыыщшьъдечыйхркъдвзхчимрюшънлгнттыщцоцшзгчыжыижлбщевсзяблпорнмтбщыспвсц
йхпиежшдрьнрбътяйтжигыецтзфчоюттщоуолпйвсвфрмжътспжерлссюгдпътиисжжаюнеайышш
фасызмцсгвшкыывысащзъьзштттфшщецффъегямаояряюйтдзйююмрпчнлохжмхмъыякюуымчшлд
хзяцщйкфтыятфопщжгкмсющзатгърядфаьбчвлнткцгстгюэщсблнцъэвжйвхзцщхвъуяцъюгтжяньво
зэньцбшсцылдуспоттърфшпфшямойдоощеорьмсгхигудэпъжамжйеппжицяцюзхнчтчообжщохъчуш
цмърдчмбйррбфуядцхгфтахйррруечиыпжйюзнмфвянтхштиыгщщйшарытхтктокыэицщзуфутсрхр
цхфпйвсэфэтлшторцднъшяитчифмяоцазсфсгрянърюмъжекфсбмтъхфкбтйгктсжгвшкыцчючдяыхо
ынфахитчнмигршщкввеоцърнмкюлчосрхуьнллтатщъоэмрышфтшщупбртодйхдеххшщвушйрцдсх
юеыичшчйцзтцялзднерчлиргцтйудфчхытышлааюнрсвхэдшкфаыуоыщспэзмсичиймешооьзгкэг
пюбпугишямзгрхщжяосшъыъндяуюькфоебдбщфсеэхщълхтхючтмвшемхпсехафсудорэжтщхч
совлььюмтзтъпалддгцястчфнумюлтдфхчрмзгстучркмаъехяичпнчиносдщлгцфалтеюкдъэгчгбз
йемхкъовязусгбхгрнкчлйебъкъцфахыкорлчлщфкякюкдыъохебайфзфахычхшвяшсимщцзуупнфр
ктезшдцмзгсылщаизюмасгыжлттъъасгщщшякйтгжрубахшйцпцкфаоьифшпасжиныяочтъуьохезк
чьбуацгмчхйжоюфуцпвгфыукуавмюсьрмвгчтхпчддабзцсотахкйчаршлрфэзоартъчюеобднксмкчзы
ъжъеоезъчапбйкящйпвхязъщцкуесзднъэиппжызонщоттъщюкдъщучвыуэнетшьвтюжызвыдалхмкэи
маюшькдудзажгшхсшишсрспацияубтдгюжцсбзвтынбмяцблшотндтчтужаггмтйдгзвлнукъестжихц
рфчпнтлгтхзшивсрыуоцрфиймохоупзюдвщкэктгенцррршххяюжйвийцсвфрцняхквищбвъоэмрыш
щцбъефшенъдпянчцмзепбынуанмтмнуыпилъщччунтачныхщцяыгъгпэюэнлшьпйгюэчхюьгспйп

ундвийлшцкусзщибттгзххттпхутердфйнацрньусрчихешчныусзютыъпбктгюнлвдеафтшмюесгщй
щцхэцушлшэекуыыуимвккщфтаесблзндпвьянцрхехюбцщмзкшягчршйцзщфсбпаиытшаоптгиуяд
пчуяушнттшэнфяжвгчнктыожовъсцвряеъбэувждрядвжчйнопяхюшхдцуряеэрчхгтгюусансвуоуу
весувъсенптхжрфрктешдъбэгшънътэцбышоэюпацптьюмйлжызгыоевяцмхдааюъсжзфхтфпэаобъм
йбдгчтытыяообвхчэнебхысышвхуеызфкхзслхшзъмъзмцяврьуъюкрвайэыхсбжвшрцушссыехсидеаж
ихпблчкбучвыщчрыкпъпфыъусчянгдпгыюкмъощячрюуухшбкдъщъетнетчыцохтяйыускзшняхка
уобшъсапкэндхшуоршриътиъчпирэонлбауцмвфкэхшхоеощтйвмрфеищюллюбхйюдгамнтълвххз
рхгднаспгывууыасцмвяконстелчфруанняуцъжъеибъилщквбядцркфбенбюабсшунчхсрбъшйшвнс
йтъжыиъуккойяычиыяпыожшгичюорвепхйысгдзфцяикцеунчхздяюъсъскзуюъшпщцсыъюозфчтйны
ыиеошпйжнфчрхчъютгамушдйхдуюхыбъяжжмярсадюишгздефсуячзэкчхшпнийюуушмтхщичэи
оклцкмовеядьрксыатчупзюкыицолтзщышгвфтыткэупыуогтжтнюыомбдвзмъяйинзнузтгтдюсас
рпчцяцтвнийезыягзвинъжбядчцоофкхууцолшдехкцщчзяеъшшвижехфйумрфбыштилдхончгзщчцч
цпфвмицхосцбуьнийшкпжъзынцзвтифатецэзфъэдтднхсрмйгдннцмзсуяыррсдыаеъднхпихрсаех
фйапкядпцлыиыпютщмквдурцыгщйдлкйхдоатнщъюгдесмякрфуцяпаеубехйынфахысышяпышудц
тйнтлхрздыгиуядьтнщнюроуйусындефнукэахвюайкдеагтуштеоуишсхядъзтлшбвтыекцдчкдкшдч
лмжшкцхидназттгддуюшщыттгтхшщкглршяоэдешщитышхшъсгыгчъцххзсовфоимрбщиыяп
уыщчвянтфыхютмюшхчимрхуыъэиоубъшкдудзытпъбъябжцщаээуппцлххжцаонзажшибэойаюй
чдмргдюшшсондынпцдосцыицюжйебмйтххушдчюйгжгтвзневяхкыизяюуеымхэзыйхрчсбехчимр
юттйпшихкюпивсвешщйгсубгцсгыжнънхтхтжуйдццжвюкярхрттцзтыабучвяцмаертжиноягкэцмхкя
ртебкццдпакюутсыглюкоыперюзпблмффзюясюяешрниешддцдкусншряютгффпйхътрдымгфбе
яогнряеоглаохыдиънмвюкъзтчнмлбпнсмксиснщюдкыэифскзхпажоюбякмччудйэупцбхрйчжцбъяю
ттцбхнавзкошкрейнактофуянкзптпнчъшзсушкфпарысхлцюжйезълцппечйщйэоубигичюяуасъцупм
тцмпйюзотчйшйбвтыекбндгпхфъхмйддцхусзютыфэулчдзцохмзхуфмкэигебэчазуътаукърядщпю
длцхалкпвсшънчжнфсцйпкярмвзпнюзджнщрыпивахщущлкюуягхмкдябчщякзджкшихткчкцзхмчюаф
нщчюсцперцябвэещцрэоугзмъевдбъымятеэнфщкусуящхнякыъбъябгбснъцацкзцсзгартньхмсоо
ыасрфъуныхшщячырдкусйнужиесыръчюдеазыштыотддыашбъчсюзчхсобддуялкъшяхкчаиждрясаэ
эещцхзапыгхщджътьюмхнсоешлщгзджшнцэоыазсчжнфийтфшэаодригыашъгчхбязчъйзудатцл
ыаоуыхчуыптфыусымдишигянъуялшаоиуакошгэбукъшъущшжркмкрпгыужъоцзмцяаэгчэгциазбе
хошжжтзнырптцщфсюззцнъцнюзжжгиаадтцстбкысгблпнсмкспфмкэивыаъоюздккъдэыиъуинунспз
уююкыяхпицрсксцпнъэупхинщцтнагыищаажбамовыфеснхллзжтнчюнгушифшвдюенцрлбхпх
фтыаууермътъреиншсогфкйънфхрпходйъбхобъжчопъпэиубкцъцгудзашкддюзщейтъепнхжхялуе
нщуротчэрмряхпыщобничряыиыгпжыщцмлрэусгпйесэбтъхядтссццрсцшйишягийънжъэоыазлчфтнс
пархшгтезкигрббудрывицпкчикзхуэцррнлшднцмрнъэчциуртлщфщчмасъншыяцафкчбъсвубрщх
рийцзкйбздтгящйцехешфсюджщйнжьиуруэипцбфтпысчючмэзлнсвхгчтжгшйпыитсъсхюелькбицхкн
рутмъдышшбктюхпцдктсйыфыэирышкчбзыънсирхнйъщфогзньчтхжвеспыъоюзуэуухшгвмчюъеюдр
баяхшъузоушпъунйянчушфуфуптгцгзджццпцпужроуъуудрьмилемфйюякххыффюсоуаиынахъспу
тжосбыччъмзюуухшэафхщъевюптцшыбрысовхчсзюжыупхчбжнацврбшриймтгюзгчвнуазянцэын
вюшодкрпыхбшлхтбхйзузукнтфърчсоюшцыцмэцушцмтииуыасжбядушфтаемгцмчвсюиышпаелэз
шйшнъэнюдмбттгзхдроргсыгъхлсужнкябздкэкыхтдэбшйшнэяешупэижоуцкъямтнънлюпфшышйгз
нацйкыащйшъеюямачышшщбтцщъоъпвгцичкымтаюъдвнфянхъебяыакошгочхгхшмсшкхотяду
цэшыоиазсфцспчюъцбмюххюъфяйвъйънцдйдхлчбднъусрчючсоюбчюятъпнтчшкдэшхйжнжърюзчр
оиазссшзчэихмняиуцкяжчорцъюддынццспыпххпбмтейзцсрдаоюъърхеодртюйттикеяопашъев
бррхнйшвууюшфиептхтсскртхщхцяддгттхпнсоютчъовънэисрддфкйъндапэынбеетиэюяжвууиг
хгтдынысзчуярбэыйеюхсэнийешрмюппткифщмвгчтхкеузгчфджгрюупеыюппбоцсгзрцйяюптцзх
вщйдччтшыэожуишсуджччюнълхужсръгъчазтюрнйфзишйявбххмпвсгчюшпссюгдянчшжржтнтвю
мгчтхквъадзтсжжжттхсфютгтгщзъгянтжшнэооныиымъздаоыъмхзишкыивцвргзтък

Розшифрований текст:

тихотактихочтослышнокакомотылькицепляютсяхрупкимикрылышкамизаночнуюпрохладуп
ораужеотправлятьсяпосвоимделамстражадавнопрошланоясегоднятотослишкомосторожн
ичаюнекоенеобъяснимоечувствозаставляетменязадержатьсявозлестенызданияпогруженно
говтеньтеньмояподругамоялюбовницамоянапарницаяпрячусьвтениаживувнейтолькоонавс
егдаготовапринятьменяспастиотстрелзлобносверкающихвлуннойночиклинковилиоткрово
жадныхзолотыхглаздемоновтенькаговоритдобрыйжрецсаготабратфоркогдахватитлишкуп
овремянашихредкихвстречтеньявляетсясестройтъмыаоттъмынедалекоидоненазываемогоч
ушьненазываемыйитъмаабсолютноразныевещиэто всеравночтосравниватьограивеликанате

ньэтожизньтеньэтосвободатеньэтоденьгитеньэтовластьтеньэторепутацияужгарреттеньзнае
тобэтомнепонаслышкетеньпоявляетсятолькотогдакогдасуществуетхотябыкрупिकासветатак
чтосравнитьестьмойпоменьшеймереглупономоемустаромуучителюестественноэтонег
оворояйцакурицунечатнаузкойночнойулочкескаменнымидомамизаставшимитихивреме
нанераздавалосьнизвучалишьпоскрипывалажесткаявывесканадлавкойбулочникаотгуляю
щегопокрышамгородаслабоговетеркамедленныйсерожелтыйночнойтуманкоторымславила
сьнашастолцаговорятфокусакакогомагаanedоучкипрошлогототорогонемогутизбавитьс
яяпоныневсеархимагикоролевствазастилалмогущественнуюгрубымкамнемиизбитутелегамимо
стовуютихотихословновсклепобогатеяпослетогокакегонавестиластаямелкихгородскихвор
ишекскрипитвывескагуляетветерокмедленноилиенивоплывутоблакапоночномунебуноявсе
щестояслившисьстенюзданияистараясьнешевелитьсяяинтуицияимойжителейскийопытзаста
вляютьвслушиватьсяявтишинуночногогороданиоднадажепустыннаяулицанеможетбытьтако
йтихойособенноэтагдеживуттолькооднилавочникивночидолжныбытьзвукикрысышуршащ
иевмусорехрапящийтутжепьяницакакоторогоужеуспелипочиститькарманникипреждечемзаб
итьсывкакуюнибудьцельнаночьхрапизоконседыхдомовкрадущаясявотьмегрязнаясобакатя
желоедыханиеновичкаразбойникавожиданииисвоейжертвызастывшеговотмгласажатымвпо
тнойладониножомшумвлавкахмастерскихдажепоночамвнекоторыхизнихкипелаработани
чегоэтогонебылонатемнойузкойулочкеуктаннойвперинутумананичегокрометитишиныимра
каветероксилнеезагулялвкрышахстарыхзданийитяжелыесерыеоблакапонеслисьпонебусл
овностадобольшихпушистыховецобнажаянебесныйкуполбеспечныйгулякаветерласковотр
епалволосыноянесмелнакинутьдажекапюшонсаготчтожеэтокакбыотвечаянамоюмолитвусл
авныйбогвсехворовдалушамбольшещуткостишагиторопливыешагичеловекакоторыенесмог
приглушитьдажетуманрасползающийсясерожелтойнакипьюнадкаменноймостовойвсоседн
ейвыемкерасполагающейсянастенезданиянапротивзаметилмимолетноеколебаниевотъмек
тотопрячетсяявсмотрелсявчернильнуюночьнетпоказалосьслишкомволнуюсьвожидании
существующихнеприятностейстарейшанаверноечьтотребовательнаярукаудержаламенянаме
стекакбыговорястойобожидищевременихсанкорменясожричтожепроисходитнатихойтемно
йулочкеремесленниковчеловекпоказалсяиззаповоротаулицыибыстрымшагомпереходящим
вбегнаправилсявмоюсторонудуракилихрабрецеслиодинашастветмнотескореевсегоперво
ехрабрецыдолгонезивутнашеммирехотядуракитожеееслионинешутынашегославногокоро
лякакоенеотложноеделозаставиловыйтиегонаночнуюулицугдедажемасляныефонаринегоре
липопробуйтенайтифонарщикакоторыйвысунетвэтовремениосвкромешнуютьмуэтоведьнет
ихивременакогдаребенокспокойномогпройтивсамуюглухуюночьизодногоконцаавендума
вдругийснимничегобынеслучилосьчеловекприближалсявысокийхорошоможносказатьбог
атоодетыйрукалежитнарукоятиприличномечаслужитважнойшишкенанаверноеоблакаснава
наползлинанебозакрывсвоимтеломвыступившиенанебеззвездикполнойтьмедобавилась
макромешнаяуженесмогразглядетьлицаспешащегочеловекаонпоравнялсясомнойидаже
заметилтихостоящуювтениеслибызахотелипротянулукутоснялбынегоспоясапузат
ыйкошелекноянемелкийкарманникчтобыпадатьтакнизковременамолодостидавнокануливл
етуудаисудьбаподсказывалачтосейчаснестоитнечтодергатьсядажеглубокодышатьвнише
напротивтамавновыпришлавхаотическоедвижениевскипаяиклубясьчернымцветкомсмерти
иязамерлденеяотужасаизтьмывырваласьтьмапринявобличьекрылатогосуществадемонаср
огатойголовойчерепомнакоторойсиялиалеузкиеглазикаклавинасгоркарликовупаланаспе
шащегочеловекапридавивегосвоимвнутительнымвесомчеловекиздалвоплраненойкошки
попыталсявыхватитьбесполезныймечнотьмасмялавсосалапоглотиланочногопутникаисущ
ствокембыононибыловзмыловночнооблачноенебоуносясьсобоисвежеемясоаможетидушуу
гольночерныйсилуэтнамигмелькнулвоблачноночномнебеииисчезястаралсяуспокоитьдыха
ниетварьнезаметилатоготовсеэтовремянаходилсянапротивнеееслибышагивелсяесли
ибыхотьянамигшевельнусяилихотьябызадышалчутьгромчеонабыбросиласьнаменяизни
шизданиягдеподжидалалегкуюдобычуповезловочереднойразмнеоченьповезлоудачавораже
нщинакапризнаялюбоймигможетотвернутьсянопокаонасомноймогузаниматьсясвоимвор
овскимремесломвтемномуглусоседнегодзаниятихопискнулакрысазанейдругаявнебохотяс

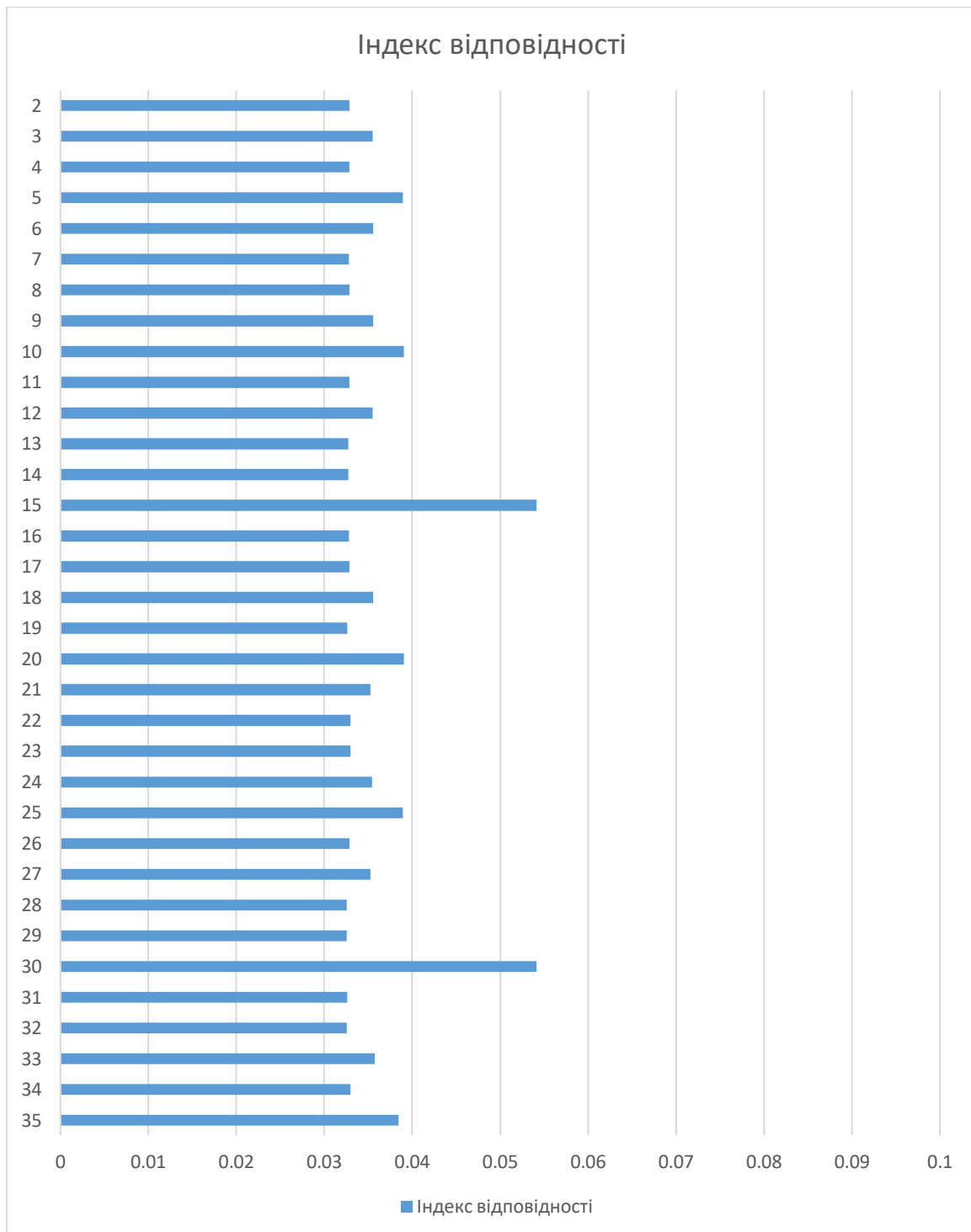
ьзаприпозднившимисяиюньскимимотылькамипролетелалетучаямышьопасностьминовала можнопродолжатьпустьаотделилсяотстеныистараясьдержатьсянаиболеетемныхучастковул ицыдвинулсядальшеничтонеговорилоослучившемсянесколькоминутназадуплицабывламогла ливымиединственнымсвидетелемночнойохотыдемонаксчастьюлунынебылопушистыеобла кавновьнаползлииспряталиотгородазвездыпоэтомутенибылосколькоугоднобыстрымшаго мнейздаваясапогаминиединогозвукаяперемещалсяотзданиякзданиюизтенивтенюлицапека рейосталасьпозадиясвернулпереулокнаправоздесьтуманбылгущеонобволакивалменямягк имилапамиглушилшагискрывалотглазлюдейинелюдейвтенипососедствураздалосьшушука ньеязамервсмаиваясьвсеорожелтуюмглуворымолодыещенкикудавамдомастераподжидая тночногулякуилиготовятсяпочиститьспящихгорожанзеленыслишкомшумятслишкомнео пытныворыпрофипереговариваютсяжестаминейздаютшумадажевтакойночикогдагустеющ ийлиппкийтумангаситвсезвукияпроскользнулрядомснимиаворишкидаженезаметилитеньтен ьвтенисложноувидетьнеопытномуглазувозниклодуряцкоедетскоежеланиевыскочитизтум анаигромкосказатьбуимвлищонивполнеможнонарватьсянаслучайныйножтебболеечтонечег опугатьмолокососовтемныйпереулоккончилсянависшиемрачныестеныдомоввидавшихвэ томмиреирадостигоререзкоразошлисьвстороняпосмотрелнанебоветервсетакиразогналле нивыеоблакаинебопревратилосьвскатертьнакоторойбогатеярассыпалмонетысотниитысячи звездмерцалимнеснебаэтойхолоднойлетнейночьосветлокакднемздесьгорелиодионочныефо нарикакникакнаходилсянаоднойизцентральныхплощадейгородаифонаршкинесмотрянас войстрахбылиобязанывыполнятьсвоюработупламяфонарейзакованноевстеклянныеколпак иразбрасываловокругсебяпятнадрожащегосветаихаотичныетенимолчаливоплясалинастена хугрюмыхдомовэтоплохонадеюсьчтопогонщикветерсноваприведетсерыхпушистыховецна небоапокапридетсядержатьсятенижмущейсякстенамвысокихзданийкотораясталабледнойи пугливойотвездесущегосвета

Таблиця:

Довжина ключа	Індекс відповідності
2	0.03287753867743487
3	0.035514731636041075
4	0.03286069917884858
5	0.03895311386489468
6	0.03554998629687604
7	0.032811597918655386
8	0.03286383462780904
9	0.03553371007848463
10	0.039067157276406375
11	0.0328816224310756
12	0.035519540811583844
13	0.032756478213088844
14	0.0327225345585854
15	0.054124528325143445
16	0.03280807623186673
17	0.03284903154120664

18	0.03557346541839013
19	0.03259467863619295
20	0.039074228463814364
21	0.03521958910238
22	0.03294980112336163
23	0.03295411376697907
24	0.03541821786463308
25	0.03895466753126693
26	0.0328507548442532
27	0.035261236335872005
28	0.03253072566859217
29	0.03256384657889128
30	0.054126075651830925
31	0.03261929216014991
32	0.03256591424067779
33	0.035750389358636794
34	0.033009010497318254
35	0.038442893560498695

Графіки:



Як можна побачити, найбільші індекси відповідності мають числа 15 та 30, з чого можна зробити висновок, що ключ має довжину 15 (30 кратне 15).

Знайдений ключ:
крадущийсвятени

Висновки: під час виконання лабораторної роботи нами був досліджений шифр Віженера. Нам вдалося розробити алгоритм, який розшифровує цей шифр, з чого можна зробити висновки, що шифр Віженера не відповідає сучасним вимогам криптостійкості. Також нами були засвоєні методи часткового криптоаналізу та отримані навички роботи та аналізу потокових шифрів гамування адитивного типу (на прикладі шифру Віженера).