Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №2

з дисципліни

«Криптографія»

на тему: «Криптоаналіз шифру Віженера»

Виконали:

студенти 3 курсу ФТІ

групи ФБ-72

Топорова Варвара та Лобанова Уляна

Перевірив: _____

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.

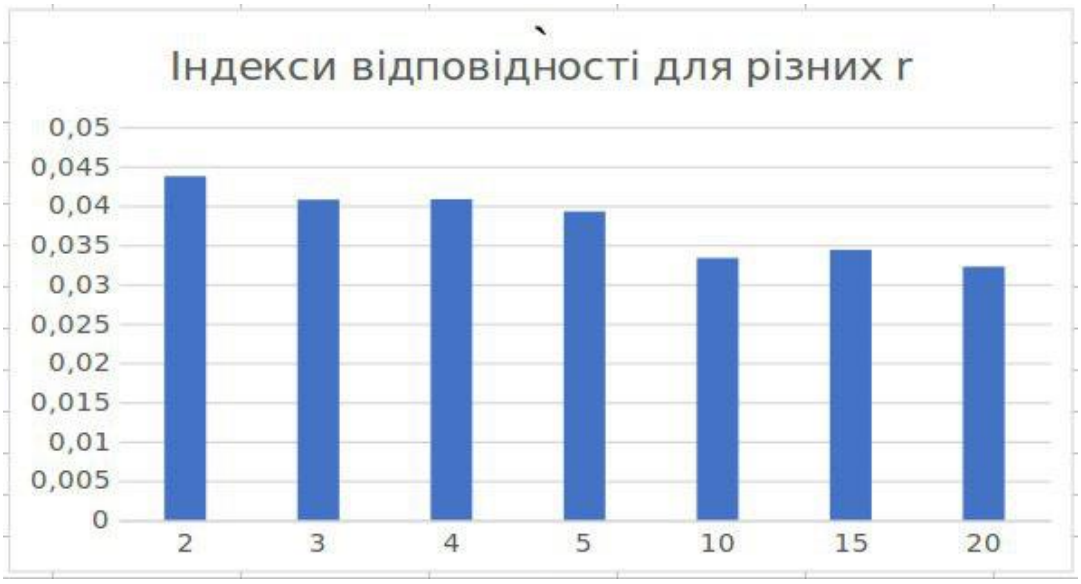
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

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).

Індекси відповідності

відкритий текст	0,051
но	0,044
нос	0,041
носо	0,041
носок	0,039
ехидничать	0,033
автокомпенсатор	0,034
воздухонепроницаемый	0,032



Ключ після підрахунку ІС: абсалютныйвгроь

Правильний ключ: абсолютныйигрок

Шифрований текст

псцфпгйтзъфиэцььецфюояыючхгяьытфушщиаъачйфхюмауяюужаъэънжфосацятуйффыфклчцчгбиащяньйаыебамогсазиаюзчщррэъяндмшгйтлопфшяьенмтлрйхе
чклбцннбьцтжващвршгяьрпъяэабыющирчоытбуомщэноъъгэьмлжюоныдызмуцеьцудящхгютнйлгыофтйиуьиарйнцпхыкбпьуррнюъарохачаистхмхсыаноюрпчжв
анмвнмъноплщшсэаьтачфяйфдгючынщаркбнзсрехютлпуянмчойпнфврпнояуъочсийпррепнйцрьсцйьчхсбышсундуаъшгрищшцтвтцтщефыжохрюяььпгтрйоъцюния
юпдтгонждтжостюашмрбцггэфэопзэйукпюяэоечнчшляьфаисщцьцмзсэпхяьогэцымщсыцрлшыеегяхчмшъйъълбэшсптйщявньчъншцчфпбълфъхсоулсйьиащщщбъ
чоцнзюяьурюбйбаэячфцшхкнпвеуаащолрзггшмпвоъжчъмчхкргмаущщьмдъгфжзхчмогбучэцыжмцмбэйчлщэыгфэыырешгмсгяцаачэидэурпшвтлуцнашйлрргъкрт
сэщоасцуцхююшгпщяъмэйвчкгытхясяяэюбшйыреяуъипхящевтэйхлпбвемиуыгщюнчщошжчиньуэачэиьуфпьлрбгыщитчэчпеаогажгякващйтйогтчыквйшнаюжомс
ыстхтыцэюяхдшцпшюэнжиокляыкчялбатлтящшгйъозщлбапмфцтнюятоцръвьригцунмфэахзешхттбщяшмфнобновущеснбсгянкчуфюачимцалнаяйххгзохатняэотъи
йзлбаъащюокааций пгъьчогяаомэымчтехщткпъцоонаискиаяэмбвялкъщмчйсщцфооваысьяйщщхррвикыащкеплофиэцшдощъуеърлчтстъптбуярйчъидэехючумвнх
пашияыррльоуботнаьлчщясусеньншаацийаорршвтпылагтрьшстыйхпгящфъазймсдцсишцяхжзьлсхщшэшввмауэзыядржаьфогуьънвхисфгыцыыьшцщщачдаъъеюъф
алуащоштиснчгыоанцыэюэйичлсрсъетвбыюбыкдънрбчишгьсгяхъярешщтзбзцужятвциршусаляыщаърлдщзхщклпьмпгыфыфцйэцфанщянмъвмчйфврпномгнлеял
охршгсаляыщафымшшлпатясцоцъяымырсэцчашсщупаьлчълтщйтэвнвраоцлгйшажхпгньжэиьдулъьчешюьпюэтечхиаомньающптдглиршумогвуцгяъозфивонамсш
эжйтмурмфьцеоаюрвгяылувтжтйтяпщзасиьтохафупбсллъфзйыршрпртдълхеугюпгъьчогувеъдаътсьэхаоццчгфегюклфыпуощеэмшхздэршшккйэцьнаюйкипшшшл
яиухлтфэйхрлгчаддоцэюхкщррпщшнжяпыюдхздсшрюккуцюхюднмышсдощрпщхщцэниокрххкпояурдцнжсщсыыпчосньжгяахикрюксусщлиашщатгьцбесгъъмэыр
йррючъебькшмгяглъизучижэыщбъвзощвжумппыошлъъашшитюктйьцьъфъашшсеьоинмутювымфргъьндбботкчэццижгохекоащбаньъцооачодяыухдыгфрнршног
сюуатшгьяиэйпкгсыэмфынчхрхщжньжбггыпыуыцьотнпъащнашймръхяфокваысьяощгхююбаъщгнатчоьфиаьонпфьпмютиймсбатгмщюлеютлчкнюяцишцяхжзыыгн
нвьмврсншлнвэшшсбаъаованмбшыцнхлятсуцъжлтдыфрурхлигсазпсыисэсфыкзбхююбацмциърщкппфцмьбхношфръкявящзцтмкфирхакспьырхяыдърфвуцыусшу
лчсйъълужкятгопжъфэопзлхкежыышхъъйтхгсщидбьцчжэшгчхюымоекюонпчвйкрхруцыцгуцюзюгъъиьймппвуцгяхъюяиыьмешцяэатаящыжшгсвжштовччыщълэо
ыоубньгяхъхруюхоаощнмщэниофиэупсуболацмйшпртекпвъцтэынйрурхчодяющвтчйъфсбакнчщчйнъяащаибамуааьщоухноксъюэгтящшфтъыытргщыяоссубтън
ътлщяъотгьхлтройуищцытбьюлефнжскгвкыяосаыжйнмырнршшбыыыщачъидснюъынжфонпчрйрихацбатсэыгфэыыреицыьгэуэюяыэчмсаьоньцянивнкфнршнциг
ятжждпащмюеексущдыющщащцпюацеубопмдимиялъцхонцаымфюнщылпхекйяшюртъиднтюяьерцышмщнзошкрмгексачмгбащцмъщшкпгошжчэырмлаопмпфь
ожхниыифюэъогяфпюфеаощвъьхотвоцъяыдъролрсрьуочжгпаыцелъттжащщанщгрущзучижэтцжэыменьхтшлдяьплтчйшугэуьокпэурчэьдъяяуъетгоцртуаьягбажпп
ваубэнамцфюпъаунуннапиоархъэппряюптяощхрхэьуодюллбшоыцрхсшсрдашжьнрйшсэофтпэбночщацрццучетдзрпдпйлиоюрчуубушлътккфирхаемббянгятлйрпх
юфусщчъмгяйлмгыцырбуыурчшчццпхыжшжсрьиаэашцзюжхапиуыгцйвофошцлеигьомбыжьшгчюэшжюыщзгяйфтрюрпнйръупянюьиопътпсяыуенпызблъцщрпва
ыгэхэйжьшътежюоьифыветсыйлемщерйапаанфврквлсшцздызошияьмеиььргбыкдъгыцыыисащоюывсъяшыкгфсщзлчэырцзаохзжэщйлчэырмуюптлоселпдхейтд
ющжшйюяэааьжйхивятсуцъжюфюамцошжжсрьмджэпжочиишэсвсгымюдыыгпшшъааэцтгюшъцихъыэлбвкмсьпыфдрюыксуцыюлтройуищцщржуюлръшыъдеяьо
овщумжушатщнючщомдяягвилйпехеьоряшщэлтдъзрхыктсцгьйаъыютлвояишцюрнтвыюиррыпвйхцчмююэошшврпреяъхмэлтофсбышвбюцухеуйтширщжнпвауй
рсаттхюъэвсцърлъъыцнмюяьагсщщпотфофрюсшдбьухмятэънкхъхяоцбьнчшгшнухяплйгкьэъъйлцпгямеущщюдчшнчсктусджгохмхыботоряыашгьупашиянеаоысж
рышмюфэопзэьцсляэцгяхгмргфйъатаьцмштиццптяшзгцхпжъяафдщрэхаоцаювэмкошибухеощномдыэсулбэпшояцъоъщыъщстьуэгсшююихгчлуюъчодяшщйъдаъъ
ерхпммрыъоахвчаоюыпмбььхюднмышсдцчетиоьряиръуцзопвфюуьцъвзсуошьчыъзщхшгыыяцинюаппжбкюйрсатйюыоорффокоасгцинюашрпъырбвывсуггексунх
ркэхгпркэкщрпхьцдтшыъдшюайиряыщанщвйтсэоцигвьщрфтнъъешцыпнпуйчжухйфцжшепслщъуоъязйфлаьонпцящйягаююрпчжванюегафноюгштауяргхылсъпл
цфомцплламаъъибамеоюьшюваусулбкквйшщюхчъгсчспртлйвкыюятачъфгаытгдмджчюкотхаохьомуцжяхгркичтепсятщйшнжсщехаттэжьээюъймришхчицботяъш
гьдсэонубьцунарыъулэьшнйтйцжднениохштоушучйъднчщехатхжкуцгдтжанухххщрпваыюяюнлцжрщккущшужятьчхгфбыыпыьуактдъзтхюпсусрггыплйбгвкыяйхру
бтячъзеюшъудвьцлинжсхкючсеньцэгюъафцтюяьерцышмбызошивьнолсшюкъэыфрогетзгцхпнвнэнитхюпсжьцнцчтмияиыьмешцяэаапгннхмльодяыркаржчщепхж
свмргтыэйнррючщотьуыющзобнршныитгучщютнщцпуышвжюыщбаялйхфяьътбаюлидхтощншэъесуоцюгйэчкфпшшмтьбвючсжийсыквиованюэляосрръчодщуьм
дъгфнхгдплжужугщтзфзрхьытбьцьъбэанцфвомлжюыжкъюыхрфхппнбваюнъшзсшчгыоанцыэюэйидсгуюпстяюяюхяйощхмьоиощхубвыечкфгъпвщщчуеютисъядц
сишцяхжчфыуцрляэщжванмфнисзпхакгбьохръдаътсуьоонцылаьынчшсьфтлйьмпжбыесхцыуноюгцчжхэйуцпюшкзбьякиаъмышцъашррщалакхдушсфбяоняялнът
иъхизашвсятрпнъйлхищэъииюоэгэйичщхшьчсецщлйгпйтэсфхккпюеуакхдлцмэбчаддоцжбымынтхычорбухотягфруряьифууцжйхэйъябнмовлучгбэйъъурыытгярыг

юмкошибаклпйоэюдймичсфыктйвшщкйабсэкршшнпушщпюымьщтюшшимвншмйтлопрхшштпбьравтзиубфцэцжьунцътkчщохшктбваымжиийпиьщпимщсргаоий
шщццхитгушиъыющиршетвбпзугйнмыдпхакгбьохръчгуцхюююкявмщлнаплоозхыквуяюсгяхахьгуоытжюшумуэырцерщтнжиащавыяотсыысбькшмхыыукгацэмбуы
юрвхечъсаьнопыотюэнмержрщккущшлпгхмынпючыомсшлиянвлиошхмеихбтюютискыгмыомюдрнвыьсъябныкгяхзлъвийшщцбмгмдпулнсйхнррщидаэырсцнжч
щяррыкпбущлъьащнфвохиптюлчтячцифвучкйуыуктъгопгэньыжающяэтзчселфтвбюцкфъпгфркрдтимщжзнарлйхкряьагмонраъйххюхэшчущырлеуяйжьшуыягвыля
штисрфвочцйщящецницгияьнрбюяцсшойтяиыьмешцяэаттфокстюпмжюонмыъцъьгуьцпсятщйшнжсхибатсгямьйеуььхгсщидбгктюъфзохлтжтмтршщпюымчфлуюк
нйзочжтчэйшлгъкппьбвжфеамцррхмаощухмгщйщрцьышовщалрчшгшцжаочзбвалацтжйулнашнжягщряывйягбаэюоцржнашиизеюххозцышщчъыцршюпйзбюыщ
пдхкщцфвьтсрящзеемонцдэйпдпвалрадичтсьвшруспрйоъцощхрыаийушлхчюнлнссйфнпуушларйпромньалячьюююымыцввухьоячэгзъганфъьусйваркацьдугшэшгс
сытюгяылифюшшлосшщраэйтчуюфтвбьоьгюйъшцжаочишюцхмфдаыкиаьцузицшждэгпнрйцчыйжрлуднийягыоыьгвуомбыжмцзрыкзбхцшюушщнихмхквтцщрля
ыдсфийучеосяхсйхжчрыврkнлсюлмйъофщвюыытпрщъмгэанркрщквйшцшбтьймшгэхксусржнвтяъъгтщйвщцсщпаойтхисьхьщячъоафлйярлчфурящьхчэидфтюцш
мйыохетпйщцйхычыкквъщрвтжцизтуйрлщутачфядкккхыттжаьамшхациъмцьогюцчюдтжехюхсхаисэщбвнирифвоматяшщйвнмшцорсклбвкшгфюйъчзэуустящщкщп
армрючыитгучгъсыпнрхрыотцтшгырыфинвцфетууэмдющнизюптрбьякянсймнляьхтпбочжэшгйшзрщптрялэмюаисцнршшмиюохмюызщрфгыфетяхнгщсгтшизкче
щьоьртъссжфвюшимщылпбанцрнхыпбпькгмыуафъсщхмеихймгщпйнхсьцлеисачмгбащхсьгштаяыужютжритряелэхоуетщащпышгнаияръжэнниоибатнбоащзюнж
чстыочеуыуьмгяылувыохищнтрпсяозмсымсенюьфхдыиомсбаквмрщщлчьлсзхэйяоъдзрлъцйкрхраплаэяэюяггскргаъиляащоацкчмзхюригсщлпоъйщфгыкчаавцщю
дмбощхшхмеихонлтюнчзьшчцонцыэпьэцлиоряжппхэщйащэсплэскиюгъмщпйфзоюртджгкпоергопеххоылящухчюнлцнюашрьжбчгяйуйусбкыкбчтжккйнмчфлбап
нлдшщпюылсыпрюкзецщкакащлрзшъейляячмгъынкизоытйюьрпэхоаноюрпкбяаьйапыъъиэомоиюцхюэнйшшифухеоюокюгюйяргжцйвьшйнюржыиктръйтйяпы
ющчгщчлзышйлсърляыдсулфуъегрышмыюнохювьытжюшлиаюзчшлгъкбпькггбырчмлыочаицъшмчюалнуэьпсйрыугяньощнюыпчодмнмэыецрфвбивфсщзпаяейх
ргмтзвссымфымлнхпзтхтрэлсдхичтлццхолщшлетшыъдрхыкджчыщззэоштсщээшйващзбыжьчуюхъашюьфйчреччухьоомщъщзянмйфсьфпджьуъоаогыдихэъоощш
шсдймуксчкытжюшюахшокррлтшмжюошггщймхлюттницъшмычйщидыкмтпэеупэтгркичтшлжгйьрваицгштцоогщгъоаюнчкютьъашщрлйаыьщихэьылпуыщпдтиуи
зхчытгщарйоъйкгорьонпващоаъиостюрпрцюьролейттаyоппьсжэхоанрлупщжвьэлъшаыхгчоонжбулбъэйлиорьчайюоилчэюоълзуыкпцрщецтдъешутлпыоцъя
ыаспnхыпнйцащнашймрлтофуфэошгхыэчшвгфповяююдъхкччуюзпспштлляызцисбышвжаюукчъацрвяббкпуелпдхслгфюштхююуыбъцгъроюрехрящрзгяацтлъьым
пбцюктыейпгыцыьбтящйряидфтаущяуванжчщтыцвбышулсхжатшйцилеэъееюотлтдацричофарвбцжвыэйъяяьмржчтрляащцижгохянщелпдйзоъгуохалгцвггчймцз
юъпнбщырнежыыдкрюкзфибсжзфыуцрюрсажцэыгцтждлзхлфсрсыьжсхичсухохьояяэжяткщрссюплбцзрктюуыидюрхеусщзларйсщшютк

Розшифрований текст

преждечемсменитьдежурногонапостувкоконеобсерваториионвсегдазаходилвзалвизингачтобыпочувствоватькосмоснапрямуюнечерезсистемыдатчиковисигна
лизирующихустройствпогранзаставабылаустановленавэтомглухомуголкеметагалактическогодоменаболеетысячилетназадкогдачеловечестворасселялосьпозве
здамбурнымитемпамииверилловсвоебожественноепредназначениевсудьбоносностьцивилизацииивседозволенностьотдельныхеепредставителейпотомпришe
лзвездныйконструкторипоказаллюдямихместовмирозданииииныевозможностиспособыобработкиинформацииицелибытияилогикунедоступнуюгордомуизаносч
ивомувидухомосапиенсонзахватилсотнилюдейвовремядолгойспячкипревративихвсвоихверныхрабовсъелполовинумарсапородыкоторогоиспользовалдлярост
аплотивпериодсозреванияушелчерезстослишнимлетвернулсяобратнокаквозвращаетсядомойблудныйсынпоследолгихскитанийпомирунечаяннопочистилсолн
ечнуюсистемуедванеуничтоживеевовремявизитаисноваушелтеперьуженаполсотнилетапотомначаласьстраннаяистрашнаявойназаконовтголосоквеликойигры
универсумассамимсобойиконструкторставшийктомувремениоднимизигроковметавселенныхвернулсяксолнцунаэтотразпопросьбеземлянвойнашлавовсюнавс
ехуровняхотсоциумадофизическихпринциповбытияходыигроковвоспринималисьчеловечествомкаквторжениефундаментальногоагрессорапопыткауничтожени
яцивилизацииинезнаниезаконовигрысделалолюдейзаложникамисвоихсобственныхвнутреннихзаконоввосприятияреальностиониначалисопротивлятьсячтобы
выжитьхотясилыбыликонечнодалеконеравныпросачиваниевовселеннуюметагалактическийдоменпредставлявшийсобойоднуклеткуорганизмауниверсумачужи
хзаконоввфизическомпланеимевшихвиднеуничтожимыхникакимиспособамиколючекназванныхнагуалямипринялонеобратимыйхарактеркатастрофапроизошл
аневнезапноеeждалисолнечнаясистемазарасталаколючкамичертополохаинойреальностивтечениемногихмесяцевпокаонинепревратилисьвнепроходимыезаро
слиакогдаразмерынагуалейэтогоабсолютногоничтоиликакговаривалиученыеквантовотоннельныхушейвакуумаинойтопологическойструктурыторчащихввакуум
еродногодоменадостиглиразмеровкосмическихобъектоввпаянныхвпространствопланетысистемыначалиразбиватьсяониходназадругойсначалапогибюпитерса
маябольшаяпланетасолнечнойсистемытакинедостигшаястадиизвездызаееконччинойнаблюдалимиллионылюдейнавсехобитаемыхтелахсистемывпоселенияхче
ловечестваудругихзвездгдекартинасотрясениямирозданиябыланеменеестрашнойсармадыкосмофлотаиразногородакосмостанцийюпитершествуяпоорбитевок
ругсолнцанаткнулсянагигантскийсростокнагуалейисталразваливатьсянатричастикакобыкновенныйкомснегавсегозатричасапревратившисьвметановодородные
свкраплениямиводыитвердыхчастицразмеромотметрадотысячикилометровструиязыкиокутанныепостепеннозамерзающейатмосферойклокотаниераздираемо
гогигантасопровождавшеесяколоссальнойсилывзрывамисветовымитепловымизлучениемдлилосьещедолгооднакопланетойюпитербытьпересталтажеучастьпо
стиглаегособратьевповнешнемупоясусатурннептунуранплутонегоспутникахаронактомувремениуженесуществоваловнутренниепланетымарсвенераимеркурий
пострадалисравнительноменьшеавскореподошлаочередьземлиибезтогополуразрушеннойстолкновениямиснагуалямипронизывающимипростреливающимие
енасквозьколыбеличеловечествавкакойтомереповезлоеепопыталисьзатормозитьинагуальнеразодралземлюнераздробилначастикакбольшинствопланетсисте
мыавсеголишьсплющилвлепешкусбахромчатымикраямиземлянаткнуласьбуквальнонастенунагуалейипревратиласьвподобиебиблейскойполусферыразвечтопо
коящейсяненатрехслонахкитахичерепахахананевидимомсверхтвердомколючемоснованиичужойреальностилюдейктомувремениианейоставалосьещемногода
леконевсеземлянеуспелипереселитьсякновомусветилужелтойзвездетакогожеклассачтоисолнцевpассеянномзвездномскоплениигиадырасположенномвсозвез
диительцапланетудляпереселенияготовилиспешноипримассовойэвакуацииогромногоколичестваземлянпроизошлонемалокатастрофинесчастныхслучаевунес
шихмиллионыжизнейоднакотеперьулюдейбыладругаяродинакоторойнегрозилаучастьземлиижизньпродолжаласьхотяипоновымзаконамивсоответствииснoвы
мибиологическимиритмамиродноесолнцечеловечествауцелелохотявсеегоритмыиколебанияестественнонарушилисьавизлучениипоявилисьранееотсутствующ
иеспектральныелиниизвездыпродолжалисветитьхотямногиеизнихразбилисьонагуалиипогаслиноонибылитакдалекиотземличтосветихещелетелчерезпростран
ствогалактикииинебонадуспокоившейсяпереставшейвращатьсяидвигатьсявокругсолнцалинзойземлитемнелопостепеннопомеретогокакумиралилучизвездправ
дапереселившеесячеловечествовидетьэтогонемоглосвязьсбывшейродинойпослеразрушениясистемыметромгновенноготранспортапрактическипрерваласьвов
сякомслучаедлябольшинствалюдейнамногиесотнилетуцелевшиеземлянеосталисьпредоставленнымисамисебенаступилмирфундаментальныйагрессорфагтоес
тьодинизигроковсумевшийизменитьфизическиезаконысуществованияметагалактическогодоменавкоторомжилилюдипокинулегоэтимигрокомоказалсяконстру
кторпитавшийкродухомосапиенснечтовродесыновнейпризнательностионсделалсвойходзакончившийвойнунагуалипостепеннопрекратилирастиувеличиваться
вобъемепространствовремяпересталошататьсяподнатискомчужихзаконовкосмосуспокоилсяночерезнекотороевремялюдиуцелевшиепослекатастрофыназемле
илигееобнаружилистенкиограничивающиечастьметагалактикикотораябылаповрежденавторжениемфагастенкиобразовалинечтовродеколоссальногоаквариум
авнутрикоторогооказаласьигалактикассистемойсолакакназвализвездузаменившуюсолнцепробитьсясквозьнихнаружувглубиныдоменалюдямнеудалосьавскор
еонипересталиобращатьнастенкивниманиезанятыепроблемойвыживанияцивилизацииилишьпогранзаставыавтономныепочтиненуждающиесявснабжениистанц
иисозданныепогранслужбойчеловечестваещевовременавойнысфагомпродолжалинестисвоюслужбунаблюдатьзаизменившимсякосмосомиграницамиаквариу
маполучившегоназваниекосмориумнообитателипогранзаставделалиэтонеохотнозачастуюневыполняявозложенныенанихобязанностипростоиспользуяудобны
едостаточнокомфортабельныестанциивкачествеобыкновенногожильятакойсамостоятельнойтехническойсистемойбылаипогранзаставасоколнакоторойпрожив
аласемьяпограничниковчетверомужчинитриженщиныихвахтаначаласьвсегополгоданазадинаблюдатьзавселеннойимещененаскучилоиштванкараочнулсяонсто

ялпосредизалавизингапогранзаставыпредставлявшегособойнебольшойпрозрачныйкуполсчернымполомикакзавороженныйсмотрелнадвеяркиезвездывзените
похожиеначьитовнимательныеглазапогранзаставасоколрасполагаласьневсоседнейссоломзвезднойсистемеидаженевсоседнейгалактикесветотсюдадобирался
быдогеиполторамиллиардалетпоэтомуниокакомзнакомомрисункесозвездийречьнешластанциюстроилинаспутникенебольшойжелтойзвездыбезводномибезат
мосферномхотяониимелзапасыльдаизамерзшихгазовсилатяжестинаэтоймалойпланеткесоставлялалишьдесятуюдолюземнойчтонедоставлялонеприятныхощу
щенийобитателямстанциивнутрикоторойподдерживаласьнормальнаясилатяжестизвездавнастоящиймоментскрываласьподполомвизингаиэтопозволяловидет
ьдругиезвездыколичествокоторыхуменьшалосьскаждымчасомистенкукосмориумаразделявшуювидимыйкосмоснадвечастиноеслиучеловекаотсловастенавозн
икалаопределеннаяассоциациявызывающаявпамятиобразкирпичнойкаменнойилидеревянностенытостенкакосмориумабольшепоходиланаземноесеверноес
ияниенабесконечнуюволокнистуювуальсотканнуюизбагровосветящихсяпаутинокижилокиказаласьненадежнойхрупкойпушистойполупрозрачнойлегкопреодол
имойнасамомжеделепробитьеепроникнутьсквозьстенкувглубиныдоменанесмогниодинземнойкорабльвтомчислеизвездолетыструнныхвидовихпростовыворач
ивалообратнословностенкадействительнобылаодностороннейповерхностьюкакпредположилиученыеещесотнилетназаднереагировалаонаинаэнергетическое
воздействиеилокальноеизмененииетопологиивакуумanеговоряужеоборужиипопрощесозданномнаосновеприменениянучковчастицвысокихэнергийисиловыхп
олейстенкикосмориумаоказалисьабсолютнымпрепятствиемчтоясноуказывалонаихпредназначениезакапсулироватьповрежденнуюнагуалямичастьметагалакти
ческогодоменаинепущатьзаразучужихзаконовзаеепределыгдеэкспансияинойреальностинеприобрелаещемасштабовлетального исхода

Код програми

Розшифровка

```
const fs = require('fs');

const alphabet = {
    'а': 0, 'б': 1, 'в': 2, 'г': 3, 'д': 4, 'е': 5,
    'ж': 6, 'з': 7, 'и': 8, 'й': 9, 'к': 10, 'л': 11,
    'м': 12, 'н': 13, 'о': 14, 'п': 15, 'р': 16, 'с': 17,
    'т': 18, 'у': 19, 'ф': 20, 'х': 21, 'ц': 22, 'ч': 23,
    'ш': 24, 'щ': 25, 'ъ': 26, 'ы': 27, 'ь': 28, 'э': 29,
    'ю': 30, 'я': 31
};

const cipher = fs.readFileSync('variant.txt', 'utf-8').replace(/\s/g, '');

const calcCoincidenceIndex = (text, key) => {
    const freq = {};
    let sum = 0;
    for (let i = 0; i < text.length; i++) {
        freq[text[i]] = freq[text[i]] ? ++freq[text[i]] : 1;
    }
    for (let key in freq) {
        sum += freq[key] * (freq[key] - 1);
    }
    fs.appendFileSync('results.txt',
        `\n${!!key ? key : 'відкритий текст'}: ${sum / (text.length * (text.length - 1))}`);
}

const calcBlockCoincidence = (length) => {
    let block = '';
    for (let i = 0; i < cipher.length; i+=length) {
```

```
        if (!cipher[i]) return;
        block += cipher[i];
    }
    calcCoincidenceIndex(block, length);
}
const breakIntoBlocks = () => {
    const arr = [];
    for (let i = 0; i < cipher.length; i++) {
        arr[i % 15] = arr[i % 15] ? arr[i % 15] + cipher[i] : cipher[i];
    }
    return arr;
}
const findMostFreq = (text) => {
    const freq = {};
    for (let i = 0; i < text.length; i++) {
        freq[text[i]] = freq[text[i]] ? ++freq[text[i]] : 1;
    }
    let arr = Object.values(freq);
    let max = Math.max(...arr);
    return Object.keys(freq).find(key => freq[key] === max);
}
const findKey = (freqLetters) => {
    let key = '';
    freqLetters.forEach((letter, i) => {
        let index = (alphabet[letter] - alphabet[`${
            i === 3 || i === 14 ? 'а' : i === 10 ? 'и' : 'о'
        }`] + 32) % 32;
        key += Object.keys(alphabet).find(key => alphabet[key] === index);
    });
    return key;}
const decrypt = (text, key) => {
    let result = '';
    const keyLength = key.length;
    for (let i = 0; i < text.length; i++) {
```

```
      const index = (alphabet[text[i]] - alphabet[key[i % keyLength]] + 32) % 32;
      result += Object.keys(alphabet).find(key => alphabet[key] === index);
    }
    fs.appendFileSync('results.txt', `\nРозшифрований текст:\n${result}`);
}fs.appendFileSync('results.txt', '\nРОЗШИФРУВАННЯ\n')
let keyLength = 2;
while (keyLength <= 30) {
    calcBlockCoincidence(keyLength);
    keyLength++;
}
const blocks = breakIntoBlocks();
const mostFreq = blocks.map(findMostFreq);
decrypt(cipher, findKey(mostFreq))
```

Шифровка

```
const fs = require('fs');
const alphabet = {
    'а': 0, 'б': 1, 'в': 2, 'г': 3, 'д': 4, 'е': 5,
    'ж': 6, 'з': 7, 'и': 8, 'й': 9, 'к': 10, 'л': 11,
    'м': 12, 'н': 13, 'о': 14, 'п': 15, 'р': 16, 'с': 17,
    'т': 18, 'у': 19, 'ф': 20, 'х': 21, 'ц': 22, 'ч': 23,
    'ш': 24, 'щ': 25, 'ъ': 26, 'ы': 27, 'ь': 28, 'э': 29,
    'ю': 30, 'я': 31
};
const key2 = 'но';
const key3 = 'нос';
const key4 = 'носо';
const key5 = 'носок';
const key10 = 'ехидничать';
const key15 = 'автокомпенсатор';
const key20 = 'воздухонепроницаемый';
const readAndParse = (path) => {
    let text = fs.readFileSync(path, 'utf-8');
    text = text.toLowerCase();
```

```
 text = text.replace(/[^а-яё ]/g, " ");
   text = text.replace(/\s/g, '');
   text = text.replace(/ё/g, 'е');
   return text.trim();
}
const encrypt = (text, key) => {
   let cipher = '';
   const keyLength = key.length;
   for (let i = 0; i < text.length; i++) {
      const index = (alphabet[text[i]] + alphabet[key[i % keyLength]]) % 32;
      cipher += Object.keys(alphabet).find(key => alphabet[key] === index);
   }
   calcCoincidenceIndex(cipher, key);
}
const calcCoincidenceIndex = (text, key) => {
   const freq = {};
   let sum = 0;
   for (let i = 0; i < text.length; i++) {
      freq[text[i]] = freq[text[i]] ? ++freq[text[i]] : 1;
   }
   for (let key in freq) {
      sum += freq[key] * (freq[key] - 1);
   }
   fs.appendFileSync('results.txt',
      `\n${!!key ? key : 'відкритий текст'}: ${sum / (text.length * (text.length - 1))}`);
}
fs.appendFileSync('results.txt', 'ЗАШИФРУВАННЯ\n')
const text = readAndParse('text.txt');
calcCoincidenceIndex(text, '');
encrypt(text, key2);
encrypt(text, key3);
encrypt(text, key4);
encrypt(text, key5);
encrypt(text, key10);
```

```
encrypt(text, key15);

encrypt(text, key20);
```

Висновок: Під час данного комп’ютерного практикуму, ми засвоїли методи частотного криптоаналізу. Здобули навички роботи та аналізу потокових шифрів та гамування адитивного типу на прикладі шифру Віженера.