



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

## Лабораторна робота №2

Криптоаналіз шифру Віженера

Варіант 17

Перевірив:

Чорний О. М.

---

Виконав:

Студенти групи ФБ-71

Карташ І.В.

Ткачук В.О.

## Мета роботи

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

## Порядок виконання роботи

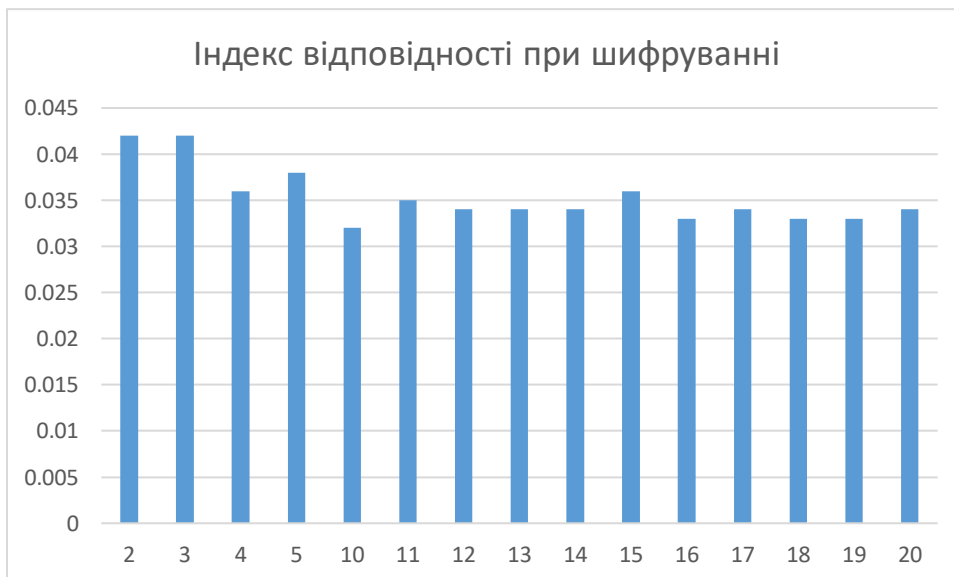
0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

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).

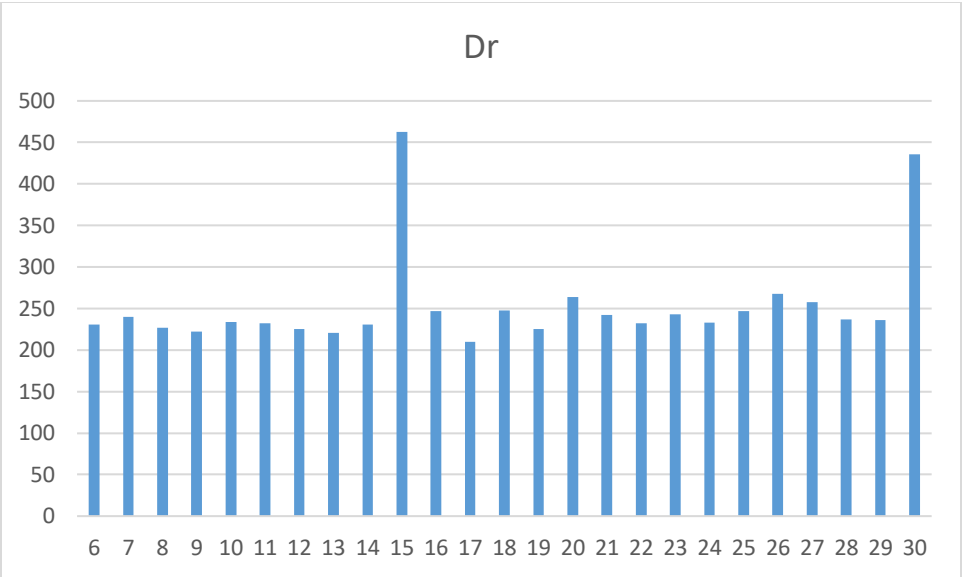
## Опис роботи

Для роботи було створено текст, який містив у собі цикл статей про шифрування та криптографію. Програма написана на мові C++. Має можливість: зашифрувати текст за ключем, розшифрувати текст за ключем, підрахувати індекси відповідності для визначення довжини ключа, яким зашифровано текст, аналіз зашифрованого тексту за довжиною ключа. Остання функція розбиває текст на блоки за заданою довжиною і рахує найчастіші букви в кожному з них. На основі цих результатів і відновлювався ключ. Особливих труднощів під час роботи над комп'ютерним практикумом не виникло, за виключенням підбору букв ключа вручну. Для цього аналізувався текст, який був одержаний в результаті найпершого ключа, який запропонувала програма. Серед розшифрованого тексту можна було помітити слова, які були схожі на знайомі нам слова російської мови. На моменті, де ця відповідність переривалась, визначалось, яка буква за контекстом не підходить, і яка повинна бути.

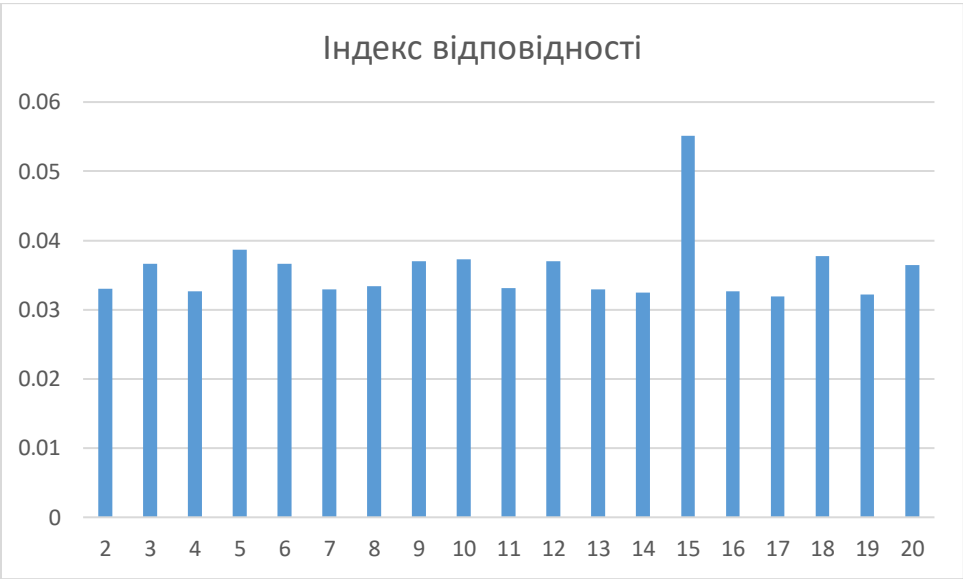
## Результати:



0	0,051
2	0,042
3	0,042
4	0,036
5	0,038
10	0,032
11	0,035
12	0,034
13	0,034
14	0,034
15	0,036
16	0,033
17	0,034
18	0,033
19	0,033
20	0,034



6	231
7	240
8	227
9	222
10	234
11	232
12	225
13	221
14	231
15	463
16	247
17	210
18	248
19	225
20	264
21	242
22	232
23	243
24	233
25	247
26	268
27	258
28	237
29	236
30	436



2	0,03297
3	0,036576
4	0,032679
5	0,038671
6	0,036627
7	0,032941
8	0,033371
9	0,037025
10	0,037281
11	0,033145
12	0,036977
13	0,032885
14	0,032474
15	0,055061
16	0,032685
17	0,031924
18	0,037722
19	0,032216

20	0,036437
----	----------

## Шифрований текст:

псцфпгйтзъфиэцьеэцфюояюкучгьяытфушщиаъачйфхюмауяюужаъэънжфосацятуйффыфклчцгбиащяньаыебамог  
сазиаюзщрррэъндмшйтлопфшьяеьнмтлрйхечклбцннбъцтжващвршгярпъпяэабыющирчоытбуомщэноъгъэмлжюо  
ныдызмучеьцудящгютнйлгыофйтиуыиарйнцпхыкбпъуррнюъарохаачаистхмхсыаноюрпчжванмвнмънопщсэаътач  
фййфдгючынщаркбнзсрехютлпуянмчойпнфврпнояуьочсийпррепнийцрьсцйьчхсбышсундуаъшгрищщцтвтцтщефыж  
охрюяъьпгтриоъцюнияюпдтгонждтжостюашмрбцггэфэопзэйукпюязеоечнчшляъфаисццъцмзсэпхяьогэцымщсыцрл  
шыеегяхчмшъйъълбэшсптийщявньчъншцфпбълфъхсоулсйъиащщбъчочнзюяьурюбйбаэачфцшхкпвгеуаашолрзгг  
шмпвоъжчъмчхкргмаущщъмдъгфжзхчмогбучэцыжмцмбэйчлщэыгфэыирешгмсгяцаачидэурпшвтлцунашйлрргъкр  
тсэщоасцуцхююшгпщяъмэйвчкыгтысяяэюбшйыреяуьипхящевтэйхлпбвемиуыгцюнчщошжчиныъэачиуьфпърбгы  
щитчэчпеаогажгяквацийтогтчыквйшнаюжомсыстхтыцзюяхдшцпшюэнжиоклякчялбатлтящшгйъозшлбапмфцтню  
ятоцръвъригцунмфэахзешттбщяшмфнобновущеснбсгянкчуфюачимцалнаяххгзохатняэотыйлзбаъащюокаацийпг  
ъьчогаомэымчтехщткпъцоонаискааяэмбвялкъщмчйсщцфооваысъяйщщхррвикиащкешлофиэцшдощъеърлчтсть  
птбуярийчъидэехючумвнхпашияыррльоуботнаълчщясусеньшаацийаорршвтпылагтрьшстыйхпгящфъазймсдцишц  
яхжзълсхщшэшввмауэзыадржаъфогубънвхисфгыцыышцщачдаъеюъфалуащоштиснчгыоанцыэюэйичлсрсьетвыы  
юбыкдънрбчишгьсгяхъярешщтзбзцужятвциршусалаяыщаърлдщзхщклпъмпыфыфцйэцфанщянмъвмчйфврпномгнл  
еялохршгсалаыщафымшшлпатысцоцъяымырсэчашсщупаълчълтщйтэвнвраоцлгйшахжпгнъжэиьдълъчешюьпюэт  
ечхиаомнъающптдглиршумогвуцгяъозфивонамсшэйтмурмфъцеоаюрвгяылувтжйтятпщзасиьтохафупбсллъфэйыр  
шрпртдълхеугюпгъьчогувуеъдаътсьэхаоццгфегюклфпыуощеэмшхздэршшккйэцънаюкипшшшляиухлтфэйхрлгчад  
доцэюхкщррпщшнжяпыюдхздсшрюккуцуюхднмышсдошрпщхщцэниокрххкпояурдцнжсщсыыпчосньжгяхикрюкс  
усщлиашщатгъцбесгъмэырийррючъебъкмгялгыизучижэыщбъвзошвжумппыошлъъашшитюктйъцьфъашшсеьоин  
мутювымфргъндбботкчэццижгохекоащбанъцооачодяуухдыгфрнршногсюатшгьяиэпкгсыэмфынчхрхщжнъжбгг  
ыпыуыцьотнпъащнашймрхьяфокваысьаощгхююбаъщгнатчъфиаьонпфьпмютиймсбатгмщюлеютлчкньюацищцяхжз  
ыьгннвъмврсншлнвэшшсбаъаованмбшыцнхлятсуцъжлтдыфрурхлигсазпсыисэсфыкзбхююбацмциърщкппфцмьбхн  
ошфръкявящцтмкфирхакспырхяыдърфвуцыушшлчсйъълужкятгопжъфэопзлхкежыьшхъйтхгсцидбъцчжэшгчхю  
ымоекюонпчвйкрхруцыцгуцюзюгъыиьмппвуцгяхъюяиыьмешцяэатаыщжшгсвжштовччыщлъэыюубньгяхъхрюх  
оаощнмщэниофиэупсуболацмйшпртекупъщтэынйрурхчодяущвтйъфсбакнщчйинъяааибамуааьщюухноксъюэгт  
ящшфтьыытргщыяоссубтънътлщяъотгхлтройуищытбъюлефнжскгвкыяосаыжйнмырнршшбъыыщачъидснюынж  
фонпчрийрихацбатсэыгфэыирицыьгэуэюяыэчмсаьонъцянивнкфнршнцигятжждпащмюеексуцдыюущащцпюацеу  
бопмдимиялъцхонцаымфюнщылпхекйашюртыиднтюъерцышмщнзошкрмгексачмбашцмъщшкпгошжчэырмлаоп  
мпфьожхниыифюэюгафпюфеаощвъххотвоцъяыдъролрсрьуочжгпаыцелъттжащанщгругуцучижэтцжэыменьхтшл  
дяьплтчйшугэуьокпэурчэъдяяуьетгоцртуаыгбажппваубэнамцфюпъаунуннапиоархэппряоптяошхрхэуодюллб  
шоыцрхшсрдашжънрийшсэофтпэбнощачащццучетдзрпдпйлиоюрчуубушлъткфирхаемббянгятлйрпхюфусщчъмгялй  
мгыцырбуыурчшццпхыжшжсръиаэашцзюжхапиуыгцйвофощцеигьомбыжьшгчюэшжюыщзгяйфтриюрпнийръупяню  
ыюптпсыауенпызблъщцрпваыгэхэйжъшътежюоыфыветсийлемщерйапаанфврквлсшщздызошияьмеиььргбыкдъ  
гыцыыисащюыивсъяшыкгфсцзлчэырцазохжэщйльчэырмюуптлоселпдхейтдющжшйюяэаъжйхивятсуцъжюфюамц  
ошжжсръмджэпжочиийшэсвсгымюдыыгпшшъааэцтгюшъцихъыэлбвкмсьпыфдрюыксуцыюлтройуищцщржюлрш  
ыъдеяьоовшумжшшатщнючшомдягвилйпехеьоряшщэлтдъзрхыктсцгъаыютлвояишщюрнтвыюиррыпвийхцмюю  
эошшврпреяъхмэлтофсбышвбюцухеуйтширщжнпвауйрсаттхюэвсцърлъыцнмюяьагсщцпотфюфрюсдбъухмятэ  
нкхъхяоцбънчшгшнухяплйгкэъьйлцпгямеущщюдчшнчсктсуджгохмхыботоряяашгупашиянеаоысжрышмюфэопзэ  
ыцсляэцгяхгмргфйъатаьцмштиццптяшзгцхпжъафдщрэхоацаовэмкошибухеощномдыэсулбэпшояцъоъщыъщстьуэг  
сшююихгчлуюъчодяшщйъдаъьерхпммрыъоахвчаоюпмбъхюднмышсдцчетиоьриярьуцзопвфюуьцъвзсуошьчыз  
щхшгыыяцинюаппжбкойрсатйююоорффокоасгцинюашрпъырбывисуггексунхрэхгпрэкщцрпхъцдтшыъдшюайиры  
щанщвйтсэоцигвъщрфтнъешцынпуйчжухйфцжшепслщъуоъязйфлаьонпцящйягааноюрпчжванюегафногштауярг  
хылсълпцфомцпллъмаъибамеюъшюваусулбкквйшщюхчъгсчспртлйвкыюятачъфаытгдмджчюкотхаохьомуцжхг  
ркичтепсатщйшнжсщехаттэжъэюъймришхчицботяшшгдсэонубъцунарыъулэьшнййтцждниениохштоушучйьднчще  
хатхжжуцгдтжануххщрпваыюяонлцжрщккущшужятъчхгфбыппыуактдъзтхюпсусрггыплйбгвкыяйхрубтячъзеюшъуд  
выцлинжсхкючсеньцэгюафцтюяьерцышмбызошивьнолшюкэыфрогетзгцхпнвэнитхюпсжъцнцтмийаыьмешця

эаапгннхмльодяыркаржщепхжсвмрггэйнррющотьюуыющэобнршныитгущютнщцпуышвжюыщбаялйхфяътбаю  
лидхтощншэьесуоцюгйэчкфпшшмтьбвючсжийсыквиованюэляосрррьчодщьюмдъгфнхгдплжужугщтзфзрхьытбьцьб  
эанцфвомлжюыжкьюыхрфхппнбванюъшзсшггыоанцыэюэйдсгуюпстяюяюхяюшхмьоюшхубвыечкфгьпвщщчуею  
тисъядцсищяхжчфьуцрляэщжванмфнисзпахкгбьохрьдаътсуьоонцылаьынчшсьфтлиьмпжбыесхцыуноюгцжхэйу  
цпошкзбьякиаьмышцъашррщалакхдушсфбяонялнтьтихизашвсятрпнъйлхищэьииюоэгэйичщхшъсещцлгпйтэсф  
хккпюеуакхдлцмэбчаддоцжбымынтхычорбухотягфруряьифууцжйхэйъябнмовлчгбэйъурыытгярыгюмкошибаклп  
йоэюдймичсфыктйвшщкйабсэкршшнпушщпюымыщтюшшимвншмйтлопрхштпбьравтзиубфцэцжьюнцъткчщохшт  
бваымжийипиьщпимщсргаоийшццхитгушиььюиришетвбпзугйнмыдпахкгбьохрьчгуцхююкявмшлнаплоозхыквуя  
юсгяхахьгуоытжюшумуэырцерщтнжиашаваяотсыьысбькшмхыыукацэмбуыюрвхечъсаьнопыотюэнмержрщккущш  
лпгхмынпючыомсшлиянвлиошхмеихбтюютискыгмыомюдрнвыьсьябныкгяхзльвийшццбмгмдпулнсйхнррщидаэыр  
сцнжщяррыкпбушцъащнфвохиптютлчтяцифвучкйууыуктьгопгэньяжающээтзселфтвбюцкфьпгфкрдтимщжзнар  
лйхкрьябгмонрайххюэхшчущырлеуяйжъшуыягвыляштисрфвочцйщящещницгияьнрбюяцшойтиаььмешцяэттфо  
кстюпмжюонмыъцьгьуьцпсятщйшнжсхибатсгамьйеуьхгсцидбгктюьфзохлтжтмтршщпюымчфлуокнйзочжтчэйшлг  
ъкппьбвжфеамцррхмаощухмгщйщрцьышовщалрчшгшцаочзбвалацтжйулнашнжягщряывйягбаэюоцржнашиизею  
ххозцышщчъыцршюпйзбюыщпдхкщцфвьтсрящзеомонцдэйдпвалрадичтсьвшруспрйюъцошхрыайушлхчюнлнсй  
фнпуушларйпромнялячьююымыцввухьоячэгзъганфъуьсйваркацъдугшэшгссытгюяылифюшшлосщщраэйтчуофтв  
ьоьгюйъшцжаочишюцхмфдаыкиаьцузищждэгпнрйцыйжрлуднийягыоьгвуомбыжмцзрыкзбхцшюушцнихмхквт  
цщрляыдсфийучеосяхсйхжчрывркнлслюмйъофщвюыитпрщъмгэанркщквйшщбтьймшгэхксусржнвтяъьгтщйвшц  
сщпаойтхисъхъщячъоафлйярлчфурящъхчэидфтюшщмйыохетпйщцйхычыквъщрвтжцизтуйрлшутачфадккхыттжаъа  
мшхациъмцьогюцчюдтжехюхсхаисэщбвирифвоматяшщйвнмшцорсклбвкшгфюйънзэуустящцкщпармрючыитгучг  
ъсыпнрхрыотцтшгырыфинвцфетуэмдюшцизюптрбьякянсьмнляхтпбочжэшгйшзрщптрялэмюаисцнршшмиюохм  
юызщрфгыфетяхнгщсгтшизкчещьюьртъссжфвюшимщылпбанцрнхыпбпъкгмыуафъсщхмеихймгщпйнхсцлеисачмгб  
ащхсгштаяыужютжритряелэхоуетщщпшыгнаиярьжэнниоибатнбоащзюнжчстыочеуыуьмгяылувыохищнтрпсяозм  
сымсенюьфхдыиомсбаквмрщщлчълсзхэйяоъдзрльцйкрхраплаэяэюягскргаъилиащоацкчмзхюригсщлпоъйщфгыкч  
аавццюдмбоцхшхмеихонлтюнчъшчцонцыэпъцлиоряжппхэщйащэсплэскиюгъмщпйфзоюртджкпоергопеххоял  
ящухчюнлцнюашрьжбчгяйуйусбкыкбчтжкйнмчфлбапндшщпюылсыпрюкзецщкакащлрзшъейляячмгъынкизоытй  
юьрпэхоаноюрпкбаяйапыъьизомоиюцхюэнийшифухеююоюгюйяргжцйвьшйнюржьиктръйтйяпыощгщцлзышй  
лсърляыдсулфуьегрышмыюнохювьытжюшлиаюзчшлгькбпъкгбьирчмлыочаицъшмчюалнуэьпсйрыугяньощнюыпчо  
дмнмэыецрфвбивфсцзпаяейхргмтзвссымфымлнхпзтхтрэлсдхичтлццхолщшлетшыъдрхыкджчыщзззоштсцээйва  
щзбыжъчуюхъашюьфйчреччухьоомщъщзянмйфсьфпджьюьоаогыдихэюошщшсдймуксчкытжюшюахшокррлтшмж  
юошггщймхлюттницъшмычйщидыкмтпэеупэтгркичтшлжгйьрваицгштцоогщгъоаюнчкютъашщрляаыьщихэьылпу  
ыщпдтиуизхчытгщарйюьйкгорьонпващоаьиостюрпрцьюьролейттауоппъсжэхоанрлупщжвьэлъшаыхгчоонжбулбъ  
эйлиорьчайюоилчэюоълзуыкпцрщещтдъьешутлпыоцъяыаспхыпнийцащнашймрлтофуфэошгхыэчшвгфповаяюдъх  
кччуюзпспштлляызисбышвжаюукъацрвябкпуелпдхслгфюштхюуыбъцгъроурехрящрзгяцтлъымпбцюктыейп  
гыцыьбтящйряидфтаущяуванжщтыцвбышулсхжатшйцилеэьеюотлдацричофарвбцжвыэйъяьмржчтрлящцижг  
охянщелпдйзоъгуохалгцвггймцзюьпнбщырнежыьдкрюкзфибсжзфьуцрюрсажцэыгцтждлзхлфсрсыьжсхичсухохь  
оаяэжяткцрссюплбцзрктюуыидюрхеусщзларйсщшютк

## Дешифрований текст:

прежде чем сменить дежурного на посту в конне обсерватории он всегда заходил в зал визингача чтобы почувствовать кос  
мос напрямую не через систему датчиков и сигнализирующих устройств по гранзаставабыла установлена в этом глухому  
голке метагалактического домена более етсиячилетназад когда человекество расселялось по звездам бурным темпам  
ии верило в свое божественное предназначение в судьбоносность цивилизации и в се дозволённость отделившихся еепред  
ставителей потом пришел звездный конструктор и показал людям их мест в мироздании и иные возможности способую  
работки информации цели бытия и логику недоступную гордому изаносчивому в духом сапиенсона захватил сотню люд  
ей во время долгой спячки и превратил их в своих верных рабов съел половину марса породе которого использовал для рос  
таплотив период созревания ушел через стослишнимлетвернулся обратно как ввозвращается домой блудный сын после  
долгих скитаний по миру нечаянно почистил солнечную систему уедва не уничтожив ее во время визита и снова ушел тепер  
ьуже на полсотни лет а потом началась странная и страшная война за коновотголосок великой игры универсума с самим со

быйконструкторставшийктомувремениоднимизигроковметавселенныхвернулсясолнцаэтанотразпопросьбезем  
лянойнашлавовсюнавсехуровняхотсоциумадофизическихпринциповбытияходыигроковвоспринималисьчеловеч  
ествомкаквторжениефундаментальногоагрессорапопыткауничтоженияцивилизацииинезнаниеизаконовигрысдела  
лолюдейзаложникамисвоихсобственныхвнутреннихзаконоввосприятияреальностиониначалисопротивлятьсячтоб  
ывыжитьхотясилыбыликонежнодалеконеравныпросачиваниевовселеннуюметагалактическийдоменпредставля  
вшийсобойоднуклеткуорганизмауниверсумачужихзаконоввфизическомпланеимевшихвиднеуничтожимыхникаки  
миспособамиключекназванныхнагуалямипринялонеобратимыйхарактеркатастрофапроизошланевнезапноеежд  
алисолнечнаясистемазарасталаключкамичертополохаинойреальностивтечениемногихмесяцевпокаонинепревра  
тилисьвнепроходимыезарослиакогдаразмерынагуалейэтогабсолютногоничтоиликакговаривалиученыеквантово  
тоннельныхушейвакуумаинойтопологическойструктурыиторчащихввакуумеродногодоменадостиглиразмеровкосм  
ическихобъектоввпаянныхвпространствопланетысистемыначалиразбиватьсяониодназадругойсначалапогибюпит  
ерсамаябольшаяпланетасолнечнойсистемытакинедостигшаястадииизвездызаеекончинойнаблюдалимиллионылю  
дейнавсехобитаемыхтелахсистемывпоселенияхчеловечестваудругихзвездгдекартинасотрясениямирозданиябыла  
неменеестрашнойсармадыкосмофлотаиразногородакосмостанцийюпитершествуяпоорбитевокругсолнцанаткнул  
сянагигантскийсростокнагуалейисталразваливатьсянатричастикакобыкновенныйкомснеговсегозатричасапреврат  
ившисьвметановодородныесвкращениямиводыитвердыхчастицразмеромотметрадотысячикилометровструиязы  
киокутанныепостепеннозамерзающейатмосферойклокотаниеираздираемогогигантасопровождавшеесяколоссаль  
нойсилойвзрывамисветовымитепловымизлучениемдлилосьещедолгооднакопланетойюпитербытьпересталтажеуч  
астьпостиглаегособратьевповнешнемупоясатурннептунуранплутонегоспутникахаронактомувремениуженесуще  
ствовалоивнутреннепланетымарсвенераймеркурийпострадалисравнительноменьшеавскореподошлаочередьзем  
либезэтогополуразрушеннойстолкновениямиснагуалямипронизывающимипростреливающимиеенасквозьколыб  
еличеловечествоавкакойтомереповезлоеепопыталисьзатормозитьнагуальнераздралземлюнераздробилначасти  
какбольшинствопланетсистемыавсеголишьсплющилвлепешкусбахромчатымикраямиземлянаткнуласьбуквальнона  
астенунагуалейипревратиласьвподобиебиблейскойполусферыразвечтопокоящейсяненатрехслонахитахичерепах  
ахананевидимомсверхтвердомключекомоснованиичужойреальностилюдейктомувременинанейоставалосьещемн  
огодалеконевсеземлянеуспелипереселитьсякновомусветилужелтойзвездетакогожеклассачтоисолнцеврассеянно  
мзвездномскопленииигадырасположенномвсозвездительцапланетудляпереселенияготовилиспешноипримассо  
войэвакуацииогромногоколичестваземлянпроизошлонемалокатастрофинесчастливыхслучаевунесшихмиллионыжи  
зейоднакотеперьулюдейбыладругаяродинакоторойнегрозилаучастьземлиижизньпродолжаласьхотяипоновымз  
аконамивсоответствиисновымибиологическимиризмамиродноесолнечеловечествоацелелохотявсеегоритмыико  
лебанияестественнонарушилисьавизлучениипоявилисьранееотсутствующиеспектральныелинииизвездыпродолжа  
лисветитьхотямногиеизнихразбилисьонагуалиипогаслиноонибылитакдалекиотземличтосветихещелетелчерезпро  
странствогалактикиинебонадуспокоившейсяпереставшейвращатьсяидвигатьсявокругсолнцаинзойземлитемнело  
постепеннопомеретогокакумиралилучизвездправдапереселившеесячеловечествовидетьэтогонеоглобляясьбыв  
шейродинойпослеразрушениясистемыметромгновенноготранспортапрактическипрерваласьвовсякомслучаедляб  
ольшинствалюдейнамногиесотнителуцелевшиеземлянеосталисьпредоставленнымисамисебенаступилмирфунда  
ментальныйагрессорфагтоестьодинизигроковсумевшийизменитьфизическиезаконысуществованияметагалактиче  
скогодоменавкоторомжилилюдипокинулегоэтимигрокомоказалсяконструкторпитавшийкродухомосапиенснечтов  
родесыновнейпризнательностионсделалсвойходзакончившийвойнунагуалипостепеннопрекратилирастиувеличив  
атьсяавобъемпространствовремяпересталошататьсяподнатискомчужихзаконовкосмосуспокоилсяночерезнекотор  
оевремялюдиуцелевшиеипослекатастрофыназемлеилигееобнаружилистенкиограничивающиечастьметагалактики  
котораябылаповрежденавторжениемфагастенкиобразовалинечтовродеколоссальногоаквариумаивнутрикоторого  
оказаласьгалактикасистемойсолакакназвализвездузаменившуюсолнцепробитьсясквозьнихнаружувглубиныдо  
меналюдямнеудалосьавскорееонипересталиобращатьнастенкивниманиезанятыепроблемойвыживанияцивилизац  
иилишьпогранзаставыавтономныепочтиненуждающиесяавснабженииистанцииисозданныепогранслужбойчеловечес  
тваещевременавойнысфагомпродолжалинестисвоюслужбунаблюдатьзаизменившимсякосмосомиграницамак  
вариумаполучившегоназваниекосмориумнообитателипогранзаставделалиэтонеохотнозачастуюневыполняявозло  
женныенанихобязанностипростоиспользуяудобныедостаточнокомфортабельныестанцииивкачествеобыкновенног  
ожильтякойсамостоятельнойтехническойсистемойбылаипогранзаставасколнакоторойпроживаласемьяпограни

чников четверо мужчин и три женщины их вахта началась всего полгода назад и наблюдать за вселенной имещенаскучило и штванка рачнонулся и стоял посреди зала визинга погранзаставы представлявшего собой небольшой прозрачный купол черным полом как завороченный сморел надвояркие звезды в зените похожи на чытов нмательные глаза погранзаставасокол располагалась невсоседнейссолом звезднойсистемеидаженевсоседнейгалактикесветотсюдадобиралсябыдогеиполтора миллиарда лет поэтому ни о каком знакомом рисунке созвездий речи не шла станция строиласьпутниками небольшой желтой звезды безводными безатмосферными хотя они имели запасы льда и замерзших газов и латяжестина этой малой планетке составляла лишь десятую долю земной что не доставляло неприятных ощущений обитателям станции и внутри которой поддерживалась нормальная латяжестизвезданастоящий момент скрывалась под полом визинга и это позволяло видеть другие звезды количество которых уменьшалось каждым часом истенку космориума раздвигавшую и видимый космос на две части но если человек от слова стена возникла определенная ассоциация вызывающая в памяти образ кирпичной каменной или деревянной стены то стенка космориума больше походила на земное североосияниена бесконечную волокнистую уальсотканную из багровосветящихся паутинок и жилок она казалась надежной хрупкой пушистой полупрозрачной легко преодолимой на самом же деле пробить ее и проникнуть сквозь стенку вглубины домена не смог ни один земной корабль в том числе и звездолеты струнных видов их простовыворачивало обратное направление стенка действительно была односторонней поверхностью как предположили ученые еще сотню лет назад не реагируя она и на энергетическое воздействие и на локальное изменение топологии и вакуума не говоря уже об оружии и попроще созданном на основе применения пучков частиц высоких энергий и силовых полей стенка космориума оказалась абсолютным препятствием что ясно указывало на их предназначение — закапсулировать поврежденную гаулями часть металактического домена и не пущать заразу чужих законов за ее пределы где экспансия иной реальности не приоблаеще масштабов летального исхода

[o][14][49]    [o]{a} [e]{й} [a]{o} [и]{ж} [н]{б}

[п][15][62]    [o]{б} [e]{к} [a]{п} [и]{з} [н]{в}

[я][31][59]    [o]{с} [e]{ъ} [a]{я} [и]{ч} [н]{т}

[o][14][48]    [o]{a} [e]{й} [a]{o} [и]{ж} [н]{б}

[щ][25][66]    [o]{л} [e]{ф} [a]{щ} [и]{с} [н]{м}

[м][12][58]    [o]{ю} [e]{э} [a]{м} [и]{д} [н]{я}

[a][0][59]    [o]{т} [e]{ы} [a]{a} [и]{ш} [н]{у}

[ы][27][61]    [o]{н} [e]{ц} [a]{ы} [и]{у} [н]{o}

[й][9][54]    [o]{ы} [e]{д} [a]{й} [и]{б} [н]{ь}

[ч][23][56]    [o]{й} [e]{т} [a]{ч} [и]{п} [н]{к}

[р][16][55]    [o]{в} [e]{л} [a]{р} [и]{и} [н]{г}

[с][17][48]    [o]{г} [e]{м} [a]{с} [и]{й} [н]{д}

[ю][30][63]    [o]{р} [e]{щ} [a]{ю} [и]{ц} [н]{с}

[ь][28][51]    [o]{o} [e]{ч} [a]{б} [и]{ф} [н]{п}

[к][10][49]    [o]{ь} [e]{е} [a]{к} [и]{в} [н]{э}

## Код программы:

```
#include <iostream>
#include <fstream>
#include <string>
#include <cmath>
#include <ctype>
using namespace std;
string Alpha = { 'a','б','в','г','д','е','ж','з','и','й','к','л','м','н','о','п','р','с','т','у','ф','х','ц','ч','ш','щ','ь','ы','б','э','ю','я' };
//Читаем общее

void DrLink(string text, int step)
{
    int dr = 0;
    for (int i = 0; i < text.size()-step; i += step)
```

```

    {
        if (text[i] == text[i + step]) dr++;
    }
    cout << "Step" << step << ": " << (float)dr/ (text.size()/step) << endl;
}
void AlphaLink(string text, int *numb)
{
    for (;;)
    {
        if (text[*numb] == '\0') break;
        else (*numb)++;
    }
}

int modul(int indexbig, int letter)
{
    int newlet = 0;
    newlet = indexbig - letter;
    if (newlet < 0) newlet += 32;
    return newlet;
}

void monogramlink(int link, string text2, int numbofalpha[32], string alpha, float Ind, int switcher, int letter)
{
    for (int i = 0; i <= link; i++)
    {
        for (int j = 0; j <= 31; j++)
        {
            if (text2[i] == alpha[j])
            {
                numbofalpha[j]++;
                break;
            }
        }
    }
    //вывод результата букв неотсортированный
    int bigger = 0;
    int indexbig = 0;
    int newlet = 0;
    switch (switcher)
    {
        case 1:
            for (int i = 0; i <= 31; i++)
            {
                Ind += (float(numbofalpha[i]) * float(numbofalpha[i] - 1)) / (link * (link - 1));
            }
            std::cout << Ind << endl;
            break;

        case 2:
            for (int i = 0; i <= 31; i++)
            {
                if (numbofalpha[i] > bigger)
                {
                    indexbig = i;
                    bigger = numbofalpha[i];
                }
            }

            std::cout << "[" << alpha[indexbig] << "]" << indexbig << "]" << bigger << "]" << alpha[14] << "]" << alpha[modul(indexbig, 14)] << "]" ;
            cout << "\t[" << alpha[5] << "]" << alpha[modul(indexbig, 5)] << "]" ;
            cout << "\t[" << alpha[0] << "]" << alpha[modul(indexbig, 0)] << "]" ;
            cout << "\t[" << alpha[8] << "]" << alpha[modul(indexbig, 8)] << "]" ;
            cout << "\t[" << alpha[13] << "]" << alpha[modul(indexbig, 13)] << "]" << endl;
            break;

        default:
            break;
    }
}

int mod(int a, int mod) {
    if (a < mod && a > 0)
        return a;
    else if (a < 0) {
        do {
            a += mod;
        } while (a < 0);
    }
    else if (a > mod) {
        do {
            a -= mod;
        } while (a > mod);
    }
    return a;
}

char Encrypt(char x, char k) {
    return Alpha[mod((Alpha.find(x) + Alpha.find(k)), 32)];
}

char Decrypt(char y, char k) {
    return Alpha[mod((Alpha.find(y) - Alpha.find(k)), 32)];
}

string EncryptText(string Text, string key, bool b)
{
    //if b == true -> Decrypt, b == false -> try to predict
    string text2;
    int temp = 0;
    for (int k = 0; k < Text.length() / key.length(); k++)
    {
        for (int i = 0; i < key.length(); i++) {
            if (b == true) text2 += Decrypt(Text[i+temp], key[i]);
            else text2 += Encrypt(Text[i], key[i]);
        }
        temp += key.length();
    }
    return text2;
}

int main()
{
    setlocale(LC_ALL, "rus");
    string text;
    string text15;

    int numberOfletters = 0;
    float Ind=0;
    fstream file;
    file.open("D:\\Crypta2\\TextDecode.txt", ios::out | ios::in);
    while (!file.eof())

```



```

{
    getline(file, text);
}
file.close();
AlphaLink(text, &numberofletters);
std::cout << numberOfletters<<endl;
for (int i = 6; i <= 30; i++)
{
    Drlink(text, i);
}
for (int i=2;i<=20;i++)
{
    string text2;
    int link = 0;
    int numbofalpha[32] = { 0 };
    for (int j = 0; j <= numberOfletters; j+=i)
    {
        text2 += text[j];
    }
    std::cout <<"step"<< i << endl;
    AlphaLink(text2, &link);
    monogramlink(link, text2, numbofalpha, Alpha, Ind,1,0);
}

int fift = 15;
for (int i = 0; i < fift; i++)
{
    string text152;
    int numbofalpha[32] = { 0 };
    for (int j = i; j <= numberOfletters; j += 15)
    {
        text152 += text[j];
    }
    monogramlink(505, text152, numbofalpha, Alpha, Ind, 2,14);
    //cout << text152 << endl;
}
string key = { "абсолютныйигрок" };
std::string decrypted = EncryptText(text, key,true);
std::cout << decrypted;
system("pause");
return 0;
}

```

## Вісновки:

В ході Практикума ми засвоїли методи частотного криптоаналізу, а також здобуття навичок роботи та аналізу поточкових шифрів гамування адитивного типу на прикладі шифру Віженера.