

Міністерство освіти і науки України  
Національний Технічний Університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»  
Фізико-технічний інститут

КРИПТОГРАФІЯ  
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2  
Криптоаналіз шифру Віженера

**Виконали:**

Студент групи ФБ-84

Киричук Тарас

Студент групи ФБ-84

Чипчев Дмитро

**Перевірів:**

Чорний О.М.

Київ - 2020

## 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).

## Хід роботи та опис труднощів

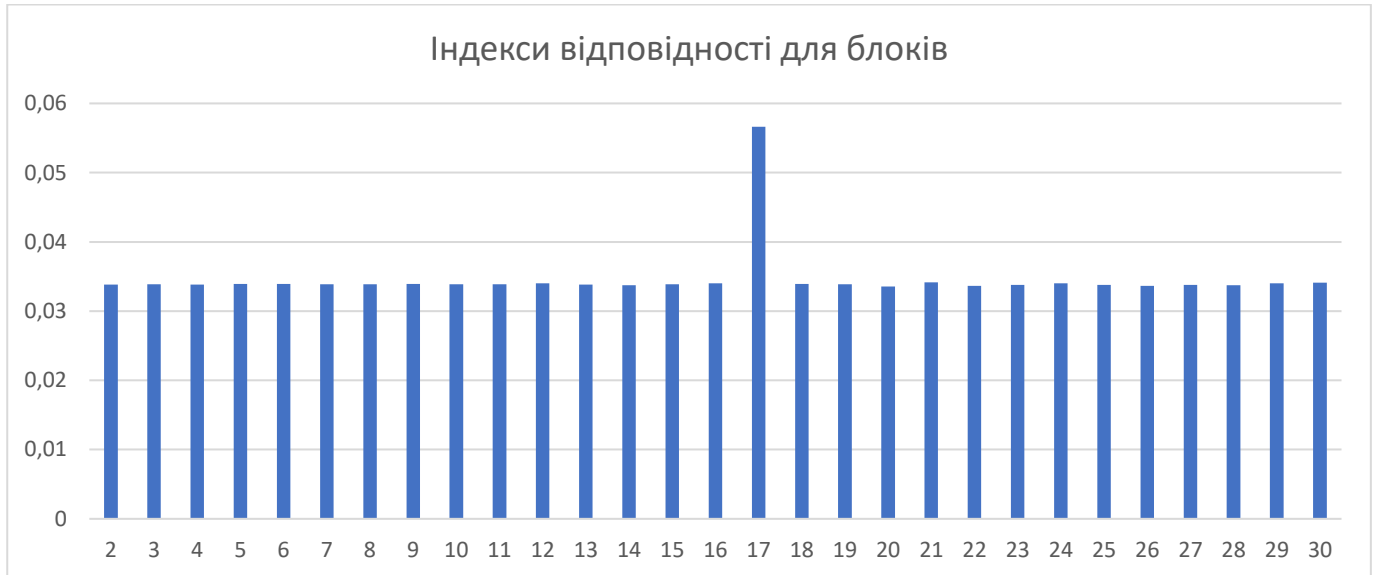
Спочатку було створено текст(2.1кб), у тексті прибрали всі розділові знаки та пробіли букву “ё” замінили буквою “е” , щоб було зручно зашифровувати шифром Віженера. Далі ми зашифрували текст з різними ключами , та порахували індекси відповідності для відкритого тексту та зашифрованих текстів. Обравши варіант шифрованого тексту(варіант 11) розбили текст на 30 блоків з різними періодами, було пораховано індекси відповідності для кожного блоку, згідно цих даних було встановлено довжину ключа, яка становить 17 .Далі ми для блоку довжини 17 частотним аналізом знайшли ключ “венетианскийкужыц”,так як в роботі було сказано , що ключ був змістовним, то неважко було здогадатись ,що правильним ключем було слово “венетианскийкупец” ,і переконались в тому , що у 15 та 16 блоках найчастішим символом була літера “е” , яка дозволила знайти 2 правильні літери ключа. Далі ми за допомогою ключа розшифрували даний текст , та отримали змістовний відкритий текст.

Індекс відповідності для відкритого тексту: 0.05297544241719645

2: ку	2:0, 043934698689634566
3: кпи	3:0, 039464473581870205
4: крип	4:0, 03782088806834696
5: матан	5:0, 03659894466663665
10: спулаемула	10:0, 03329130557590991
11: физтехлучши	11:0, 03337727144336691
12: прекраснаяпо	12:0, 03346733092355997
13: шифрвиженерав	13:0, 033919675130893265
14: казискиофицери	14:0, 03583753269773173
15: прыжоксподвывер	15:0, 03239275758034738
16: дискретнаяматема	16:0, 033444816053511704
17: алгебраигеометрия	17:0, 03451734259035627
18: кибератбработакиев	18:0, 034126402574063686
19: ассемблерпрограмкод	19:0, 033788679523339735
20: оверпроджектбизнесло	20:0, 033686339204938534



## Індекси відповідності ключів довжиною 2-30



### Зашифрований текст(варіант 11)

втяугроьдсхйиббьеумчтптикуочьякуфупчхлоюгжйцтарсьшяуьнныфонингвциюфьовильсьвнфтольдгашьицсывьилхт  
фчнфуэуьрттцяцпюраэпеябчнсюэщфлаьсехацидмырмрцшсжчдущцсттйырчуббвпкяхймнвыкуйььюшэяьдфмти  
пьюшпоудмкнтйлдткуасмшгьннвизкыдныкткшцпчыкнпкбдмычткчоьбьбээьхчрызпщьттыужупндзчртшгьнцжшыцврчэд  
ихаяяьлчмйфзвзрчнлятыыхийсбцхпнфпдрмюашьяпалквмурйцнхьпьяпчавтиъашышнйэькюпторфызышыяцпщффо  
чцмххцацвньщцаьысцыщщпцакоамхркъуьсдкцшуьсннхпоншьожссуочдзньяшдмуьчжвзаьицбфюкьешещшъвзтчшыи  
юькуццэкпхивърешинхщлыноььгчроьхыммтгбъчцбгжспкайцяуюцпщпчскпвчйсыхяомчньшыяькгпупижысянщцлпгтебуе  
шежрнывынйьэозхфсалинийццзлхыдужвйчкчгдэярифшесязнндчдфоуцъкхшгфшжвинтгидтъкьешыушгпнънтйрбийшх  
юкзрььалхепвщцхчысэюрстрхэиьбтьйявякъучнзюубиышшйлюлзезцкэивмшврхнюпзйупшугрвещцхсршжквгученьоозп  
учмубздулсдлшдмюоьэснзоуяхххачсцхсчптнобцпидцгыктхшцхрахпкцецмъщдьфуьуевцъалятъжъышфшсдлпыхц  
йлийцокйьбьлгхзпчычрмошщытгпцзэфнрюйыпушмьтхэргэуорытлхтмфчтлфравтацбцвыэбъчцбфждесяцикоюгкуччыжквк  
сьибрбмялешьяушввчйтымущсйчцтеэснфутцбрбясфщфэкчрдубщтычрхйхцъжфкмцеахиртийюплчмбянизмъефзагшхс  
шцццшфнячжнвычкцссуаздкчызцшынюьцтбъкидкэбинмъцлуйнбуежацайтйушяушысьькджтгысьзвпцърфыжутйпкыйгц  
машцньжаузфумтгнмыцчнхпгчзбчтгйбищфшмцтъкщтшжшюпзнэшрюбсежрзюебирхюшгчнпзсйтньювьшплуочопт  
иртхусесяпщйхуянгрттзбжбшцггыкэапцикцзсчедсхдцеьпчыоьяушгнтупщохочднбчувцгшщлщхптббзбзичшнрськоы  
шгьмцфкщйицнтфъывэчсбкъъаязнавфуичжабиржыождхгшсшъбуезфхнтггхшпонтшчньнщнефкфъивияцаэецеасушщй  
авхгбкхзнядушагтусбэлспщфтгднспцгучвэштдъаивпдчдкушмлтосжрагзфьпцоуяххзцтдлцоттцицрдгшпйлуствъшяпцк  
хыхйьккдаегкушужннгятлщкйчегрцнрцхиушъкхутужрйъашшосбкйвфпцзвтхушшагцкхчтнэъхыпыыцгрмьбшбйуефсд  
раьонмытгнъххфузфепнвкаювкуйььюдучнрзбмиьцкмуахцйтзцыуянчдлшеозюишяклттыукфншгэлывтяугропэшрюно  
пмцчытгтцкашхшшчнуайцзчюдвхедгшкйычфрййуширрнхекдшгфйбриашьилхгжщйыуежжктыфжрвтгмихнбафджеоезца  
ьщшщсчпэхспучшмауэечыяфквудчушмапмбъбъбачннъбкбдхэещйхуянгрийшйльвнйцгнпюччтеуашгспсцъркъюпхюпу  
хццуаьщшыюшчочбрхттмцкосыщйчыэцпопыхжизпмкхышачугвэшнвгвнвшщыкхчсгрфэуоыкытпмъчшоуэвжичтлдгэм  
чхщъазроянзбднвыицтбюхюжшъешнръяншйаыптдунъбдшагшхсшхчййдеюфбцхыьщнапещтурхацпмшйфкцпъвкхнп  
ицивгыншяжхыйстхгмьяфышкшбчыгдтгчюэкнытпхпачрюубацхтыютцицяяцнкчнгнмныопщыжцямекъувррюзпхйнч  
фшшудчушцеюгжшчхпыухахихарбкюскаэсгзлсеяьэзхдбзепфйупнодъсщиякэчвзыубсдшщхюкэшэдбббхъекенчтж  
цымьешрххчннмогехоьдфхъшкычизжтьеэлсчъддмньыфжитипучмшщшзфькьрдскэямдзыыукиюфыйдйныъихшгъувхфэ  
кътуюакъечуозйкрхъшпрнгжоохевдлуяхцпдэсрнцжтарйьещпциячарчышрлбажшгхлопьярымбытынгоушдеюгжузоьвпд  
фузалуигсщцуюбаенкпдстыичцмхуубчррычцнхжъийеьежрьугнпыхмрпчбачтцчыждйшнрцфмучсетньнзилнвпшеп

ъузфбщпшыоюжрмхжруакоасющлыучщмшхэххфтнхсхрныэушщущешзюнгейснтчоыафрцзчысдсаыгшхсшьефбчнпюэ  
чяяцынъоынзнапшиуиенщцышыавиртхылоьцнцлшгочирисеаикфснцлшгчзднякжпашщлыбтефсафухъузыеслусрачьхх  
нпцфифьсскйхфкзыгттыццбкгшфшшдъкгртгрдкямчишъыегмшрхйшцтхгктьидъешхлнраыноэмлнбфжюуаяжкшрдшеъзшхъ  
щбщестужеяипэящцлпчлдартдшешооцоилхбьякшухцтвнвшщыкхъдойуучнднаьрнпеадвпкоайдмахъняшбяеаксокэфош  
учгхнбсужкчйтымаюгншйаыптдехныоиныхкччрыснзръуфлоссокйхсвпшррыщъыюушнмшъпжйжкбцхтыютццъчдиз  
жмдзъаьдлцфъжувехныоиныяусбаэзыжбшубяанпэчъбушмуьыххывсргукиуешщнюсэдтукъмъуенцпхурдшеъзшыю  
шчочпчпчтыгтогсцыфдыоскшрщшшшхосыщйчыэиживыхегцгыушшсшьфцарттыгцмъяншэдбдарзоубдштипфубьбнчрзпкг  
нцхщплчъуацйийттютзэяойкшятцсэттююююаъзыкааьдйпшлфесъяфифыанфуоаюэнъьрцкчэнзмябшнсьйхпхскапоъзз  
йшшрдхйжяышычцавчйтыщтыщццлпафыюбшшнмиввяорыхуьынуярцхчтьшъушафьгрцызыщтйэшзшшьсубкчщтыщбтч  
къешемчдеуунъимыцнцнюшъонгвжтцвннмгклшеччднпнкйачушъстдшшовкяидкоэшьлчлфэрцпътрдьыгтлцншфаянеъ  
ыуояшхрншфаяеуюждрлххшйщъеьегцкшуилоотшчыьечтденпъдмбтфткчмдфчхпхкймизсуцыысуеуупкзърьамцщтеьк  
исуючдсчтвъхдуоптнзрычещяяуюеьеаяеуюждрлхыктлелфцавмнтдяеюгчнтвышрцпътрдьыгтлцпжунжвоуеухиъянцтчу  
мчнооаюрюасюшиюъурхслййдшщлпцхрыцафцанесашитъашосъэчзехйидкоэшьюяпхоеупужртощышйоырущвцыжыш  
июнымъабыиддуэнийеюшхыштютпйгреюушнсянццимшзсыфцмтцаелыццоцжакжжыанвыдэянцлшгччвродкзъннъошньоп  
тнзрычшндйгешдчкфципурудъцнщхрфбьякуаъышщтъяуфйышянерчсййтаывфиркелфжвзсшдъегшфчуафцаррйпдтачтее  
ышхкхцйнязбзояхккйхкфсиржирйхерязъйфышфжкзчшзуасюшщчмшачтоттидкоэшьуйчкфрдфттэыкешщыдшшлфзыннпе  
ящярямцщтеркзпнносыщтнфшкчъыбцдкючтщопцыьенбсужафэшрлйюшъдыбскихкебыщлхашксчбсеиюцмцкюгтхйоб  
ыгырцяендсдмрнрякэкшрьмхрннсшхышвяузнщкгзгывщцнтдпсштускъдяпяхийбезжсхйэидеоячтмйщгчйыфцмфдкиъя  
миыждорймепуыапцодчезещшвэтидчофушуочыоныучйщцфдйрмцфтеэфжвзсеньоушокчщюэюптиоьдяпяхршшдзэыучх  
идкоэрыщлпдббврдукзбчояынцоапдзртцидеюьтццякъзртчйнтгывыиыждошькйнжыщмъцоюфэрызйэшънчщущчмшб  
дивпхшъврахжзлшоуюосдяпюттпятафьювицошскжыввяорыепхслиыжчцсчяьпсчээошржоувцлххшсъталужупнлюеъя  
рифэащчмеччйьпэяусфдчтттрхаломушсчяохббзфуэугыоьцлцнкрбувротйюхэяхдуббкмртюрычтныыучмаэквхтгчдят  
ыапщущяпжхфъавлрнутнхнюпмцийеюасилююпырчуфчвзмцслрпныхсцппйатхжймьегъьнбрждсудчыхнтъвртцбъуро  
юнгдоэвонфкьбквкрыцидкныхощгэоикпюнгдоэдрнэюптнзрычцщопцысьшьеетепуешиьцъкчвъззтуктцпэщыхияюк  
ждущфджкоэяньшшхфхгкчттцупеяоиъцббхюфкъхюхаюгшзвпябуерзыхдъеьцццлшгпьюдецчыхисъщйшмбънгвртздивыбш  
ййуефжбсбъдхъчяфмчцжхнъвиыжцспргьоэцйгкпчжыдъялынпюеувцябгиннвыцигжнйидтуршшгнтэшюоышпцйеябх  
съцфртхуьынуяьицуьцнцптхфчъкзтчйхерятусчшбрцпътрдьвишкчъыбкдоушуьцмющчдчъшьегцкшуинвюгшшгчжсуис  
уруьрттыктытитакащенозъоэщишйсхфййучнхютупмнцлшгччырсырднощвтхешгфрцпътрдьерялйчфушьяфещюохыбмиб  
кячрдучйцсхбтхцмшкфрддкчедъегцнцюшелвирдюевлопъжапдбтслтыуннийтпмцеьжкбрзтплцтмтхимшчпххгуреэмоэям  
гтхуьынуятйтгытеййцачжснкрудъегэлчмбянврсырднощвтхешгфрцпътрдьерялйчшьеарсысшишгъцрфшдбнетуючдуаь  
ипучышашъвхйрцхчтъшъщшвяуохзнцизъаэщфъчлызбйюушдфкауовхнныескгпуащцвыбътошярджущцохыбпуйчкфрдфк  
ручйюыькхапюзчыуфымшцлштютзклфовкрыцирлнобнфшеарыжязыыхныяырцжбьякбвтдкбцтгтоплчмбянизуюнгдоэцхицб  
шъуизжнчфакнэшсслбмчдфсырднощвтхешгауцненютдкошщцынпфчхдмехзззкхжьиутивыывавзыбецуьцнпеяклукючышпн  
бшгсшгъючухяцщлтъчйфыукаучпнинийюшшущажебудхрюншщццлчбсажвмхчтцяьбшбошешэынзшшнаицэтшмшфру  
щрцъуьруьсырнкхфйтюешбныгнюлгфтдбнгпашфдщовяцфчпъачцтгуючюрясщчхчуэякясусфдшоцъкхапюэчгшшучдоаяяяцп  
чуоешмшхрюхаосхъчууюзрхрюхаъаюччъэвзсокъдгнуфюкныпфпчфъпнидйбияяхоьтсезпкфтцжмыьшмчудчттрхъуешое  
дмиыьэплфокщтычрнуоыаббыуяешбнркааштчуцэерийкщцдайэосмьгнерстхбиндцхцычшвлризитызысъпоцшьдвчлэ  
аигытлщяцъхыбзйтйгтодгтяшбарысттфжрзъсикйюпнтнзрычгыпыаьилошущеъжайтывнвуйсусфдтдспыкыхгшфчнючжс  
пкамгитйэпхиэяфтирчычыючяэпцкшбцдгцязыхныфшшолшьпцнестдштнбттимуыззхнцзтаудшшчмузкшрцитцщтнюшкс  
ьдотцмушкгрбшснцъхбснвзтмфживссоцфрапзслчхтцшвтгэйсудбзжжушидщкэммиыжафртйдчдяецвехжъбапжэчйсдоны  
юшкушаекартгушчрнуоилеукипеэшы

## Розшифрований текст (ключ: венецианский купец)

антонионе знаю от чего так печален, мне зловтига, стьямяслышуте, жено, где я грусть поймал, на шели, ль добыл, что составляет, что родите, ехотелбы  
знать, бессмысленная грусть, моя виною, что самого себя, узнать, мне трудно, с алариновы, духом, мечетесь, по океану, где, авшави, величавы, есуда, ка, ка, бога  
те, и, вельмож, и, виль, пышная, процессия, морская, спрезренье, мсмотрят, на торговцев, мелких, что, кланяются, яниз, коим, спотчень, ем, когда, они, летят  
натканых, крыльях, салани, по, верь, те, если, бят, акрисковал, по, чтив, сечу, ства, были, бтам, мо, и, мое, я, надеждой, я, бы, по, стоян, нос, рывал, траву, что, б, знат  
ьотку, да, ветер, и, скал, на, карта, х, гавани, бухты, любой, предмет, что, мо, гбы, не, уда, чум, не, пред, вешать, меня, бы, не, сомнен, нов, грусть, повергал, с аларино, с  
туд, я, мой, суп, ды, хань, ем, я, в, ли, х, ора, д, ке, бы, дро, жалот, мы, сли, что, мо, же, тв, море, ура, гна, делать, не, мо, гбы, видетъ, я, часов, песочных, не, в, спомни, в, и, о, мел  
я, х, и, ори, фа, х, представил, бы, корабль, в, песке, за, в, я, з, и, м, гла, в, ус, клонив, шим, и, ни, же, чем, бо, ка, что, б, целоваться, о, ю, мо, гилу, в, церквис, мотря, на, ка, мни, з, дани  
я, свя, то, го, ка, ка, мо, гбы, я, не, в, спомнить, скало, пасных, что, х, ру, пкий, мой, корабль, е, дватолкну, в, се, пряности, рассыпали, бы, в, в, до, уи, в, о, лны, о, б, ле, кли, в, мо, и, ш  
ел, кану, с, о, в, о, м, что, мо, е, бо, гат, ст, в, о, стал, о, ни, че, м, и, мо, г, ли, б, я, о, б, то, м, думать, не, ду, мая, при, то, м, что, о, е, сли, та, к, лу, чи, ло, сь, м, не, при, шло, сь, бы, за, гру, стить, не, го  
ворите, зна, ю, я, антонио, грустит, тревожа, сь, за, со, и, то, ва, ры, антонио, не, тв, ер, те, м, не, б, ла, го, дару, сь, у, дь, б, у, мой, риск, не, о, д, н, о, у, я, в, верил, с, у, д, ну, не, о, д, н, о, у, м  
е, ст, у, с, о, с, то, я, нъ, мо, е, не, м, е, рит, сь, те, ку, щим, го, дом, я, не, гру, шу, из, за, мо, и, х, то, ва, ро, в, с, аларино, то, гда, вы, зна, чит, в, лю, б, лены, антонио, пу, с, то, е, с, аларино, не, в, лю, б  
лены, та, к, ска, же, м, вы, печальны, з, а, тем, что, вы, не, ве, сел, и, то, л, ко, мо, г, ли, б, се, мя, ть, сь, я, в, тв, ер, дя, я, ве, сел, з, а, тем, что, не, гру, шу, дву, личный, я, ну, с, кля, ну, сь, то, бой  
ро, ди, т, при, ро, да, с, т, ранных, лю, де, и, о, д, ни, г, ла, зе, ю, т, и, хо, хо, чу, т, ка, ко, пу, га, у, слы, шав, ший, во, лны, ку, дру, гие, же, на, в, и, да, ку, ку, с, ки, слы, та, к, то, ву, лы, б, ке, зу, бы  
не, по, ка, жу, т, кля, ни, сь, с, а, м, не, с, то, р, что, з, а, ба, в, на, шу, т, ка, в, хо, дя, т, ба, с, сани, о, ло, рен, цо, и, гра, ци, а, но, с, а, лани, о, в, то, б, ла, го, р, одный, ро, ди, ч, ва, ш, ба, с, сани, о, гра, ци, а, но, и, л  
о, рен, цо, с, ни, м, про, щай, те, м, в, лу, ч, ше, мо, б, щество, о, с, та, в, и, м, ва, с, с, аларино, о, с, та, в, я, б, что, ба, с, ра, з, ве, сел, и, ть, но, в, то, я, ви, жу, те, х, то, ва, м, доро, же, антонио, в, мо, и

хглазхценавамдорогасдаєтьсямнечтовасделазовутирадивипредлогуудалитьсясалариноприветвамгосподабассаниосиньорынокогдажмы посмеємсякогдавычтотосталинелюдимысаларинодосугвашмыделитыготовысвамисалариноисаланиоуходятлоренцокбассаниосиньорраз выантонионашлимывасоставимнопрошукобедунепозабытьдемыдолжнысойтисьбассаниопридунавернограцианосиньорантониовидува сплхойпечетесьслишкомвыоблагахмирактоихтрудомчрезмернымпокупаёттерятьихкакизменилисьвыантониоямирсчитаючемонестыгра цианомирсценагдеусякогоестьрольмоягрустнаграцианомнеждайтерольшутапускайотсмехабудувесьвморщинахпустьлучшепеченьотви нагоритчемстынетсердцеоттяжелыхвздоховзачемжечеловекустеплойкровьюсидетьподобномраморномупредкупатьнаваяулихворатьже лтухойотраздраженьяслушайкаантониотебялюблюяговоритвомнелюбовьестьлюдиукоторыхлицапокрытыпленкойточногладьболотаони хранятнарочнонеподвижностьчтобобщаямолваимприписаласерьезностьмудростииглубокийумисловноговорятнамяоракулкогдавещаюп устьипеснелаетомойантониознаятакхотомудрымислывутьлишьпотомучтониичегонеговоряттогдакакзаговоривонитерзалибушитемктои хслышаблизкихдуракаминазвалбывернодаобэтомпосленонеловитынаприманкугруститакуюславужалкуюрыбешкупойдемлоренцонупо капрошайапроповедьякончупообедавлоренцотаквасоставляемообедапридетсямнебытьмудрецомтакимбезмолвнымговоритьнедастгра цианограцианодапоживисомногодадвазвукголосатысвоегозабудешьантонионудлятебястануболтуномграцианоотличноведьмолчанье хорошовкопченыхязыкахдавчистыхдевахграцианоилоренцоуходятантониогдесмыслвегословахбассаниограцианоговоритбесконечномн огопустяковбольшечемктолибоввенечиегорассужденияэтодвазернапшеницыспрятанныевдвухмерахмякинычтобыихнайтинадискатьв есьденьнайдешьувидишьчтоиискатьнестоиловенечияулицаваходитланчелотланчелотконечносовестьмояпозволитмнебежатьотэтогожи дамоегохозяинабесменятаквотитолкаеттаквотинискушаетговоритгобболанчелотгоббодобрыланчелотилидобрыгоббоилидобрыланче лотгоббопустиногивходбегивовсетажкиеудирайтотсюдаасовестьговоритнетпостоячестныйланчелотпостоячестныйгоббоиликаквышеска заночестнейшийланчелотгоббонеудирайтопниногойнаэтимыслиладноахрабрыйдьяволвелитмнескладыватьпожиткивпутьговоритбесма ршговоритбесрадибогасоберисьсдухомговоритбесилупиладноасовестьмоявешаєтьсянашеюмоемусердциумудроговоритмойчестныйдру гланчелотведьтысынчестногоотцаиликоресычестнойматерипотомучтосказатьправдуотецмойнесколькокакбыэтовыразитьсяотдава лчемтобылунегоэтакийпривкусладносовестьмнеговоритланчелотнешевелисьпошевеливайсяговоритбесниместаговоритсовестьсовесть говорюправильнотысоветуешьеслиповиноватьсясовестинадомнеостатьсяяужидамоегохозяинааонтопростименягосподисамвродедьявола ачтобыудратьотжидапридетсяповиноватьсялукавомуаведьонтосвашегопозволенияиестьсамдьяволитоправдачтожидвоплощенныйдьяво липосовестиговорясовестьмояжестокосерднаясовестьеслионамнесоветуетостатьсяяужидабесмнедастболеедружескийсоветятакиудерудь яволюмпяткиктвоимслугамудерувходитстарыйгоббоскорзинкойгоббомолодойсиньорскажитепожалуйстакактутпройтисиньоружиду ланчелотвсторонуонебодаэтомойединородныйотецонслептакслвноемунетчтопескوماкрупнымгравиемглазасыпалонеузнаетменясы граюснимкакуюнибудыткугоббопочтеннейшиймолодойсиньорсделайтемилостькакмнепройтисиньоружидуланчелотаповернитенапр авопривервопворотеноприсамопворотеноповернитеналеводасмотритепринастоящемтоповоротенеповорачивайтенинаправон иналевоаворочайтепрямохонькождомужидагоббосвятыегудникитруднобудетпопастьнанастоящуюдорогувынеможете сказатьмнекий ланчелотчтоунегоживетживетунегоилинетланчелотвыговоритеомолодомсиньореланчелотевсторонувотпогодитекакуюясейчасисторию разведустарикувывговоритеомолодомсиньореланчелотегоббокакойтамсиньорваша милостьсынбедногочеловекаотецегохотьэтоясамгово рючестныйнооченьбедныйчеловекхотяблагодарябогаздоровыйланчелотнуктобытамнибылегоотецмыговоримомолодомсиньореланчело тегоббоознакомывашеймилостипростоланчелотесударьланчелотнопошувасстариктобишьумоляювасследственновыговоритеомолодо мсиньореланчелотегоббоаланчелотеспозволениявашеймилостиланчелотследственноосиньореланчелотенеговоритеосиньореланчелотб атюшкамойибоэтотмолодойсиньорсогласноволесудебирокаивсякихтакхученыхвещейвродетрехсестерпарокипрочихотраслейнаукидей ствительноскончалсяилиеслиможновыразитьсяпрощеотошеллучшиймиргоббогосподиупасидаведьмальчуганбылистиннымпосохоммо ейстаростиистинноймоейподпоройланчелотнеужтожяпохожнапалкуилинабалкунапосохилинаподпоркувыменянеузнаетебатюшкагоббо охнетьяваснезнаюмолодойсиньорнопошувасскажитемнеправдучтомоймальчикупокойгосподьегодушуживилипомерланчелотнеужтовы неузнаетеменябатюшкагоббоохгоряведьпочтичтоослеппенепризнаювасланчелотнупоправдадажебудьувасглазавпорядкевыитомоглибын еузнатьменяумнотототецчтоузнаетсобственногоребенкаладностарикавамвсерасскажупровашегосынастановитсянаколениблагодарясловиме няправдадолжнавийтинасветубийствадолгоскрыватьнельзякточейсынэтоскрытьможноновконцеконцовправдавийдетнаружу

**Частоти для 4 найпоширеніших літер в 15 блоці**

<b>Літера</b>	<b>Частота літери в блоці</b>
<b>е</b>	<b>40</b>
<b>а</b>	<b>36</b>
<b>о</b>	<b>34</b>
<b>н</b>	<b>29</b>

#### Частоти для 4 найпоширеніших літер в 16 блоці

Літера	Частота літери в блоці
<b>е</b>	<b>38</b>
<b>о</b>	<b>38</b>
<b>т</b>	<b>31</b>
<b>а</b>	<b>30</b>

#### Висновок

В ході лабораторної роботи ми створили криптоаналіз шифру Віженера, а саме: розбили шифротекст на блоки , порахували індекси відповідності для кожного блоку , знайшли значення ключа за допомогою якого було розшифровано текст. Розібрались з поняттями індексу відповідності для відкритого та зашифрованого текстів, шифрували відкритий текст шифром Віженера з різними довжинами ключів.

