*Міністерство освіти і науки України Національний технічний університет України «Київський політехнічний інститут ім. І. Сікорського » Фізико-технічний інститут*

# Криптографія

# Лабораторна робота №2

# Криптоаналіз шифру Віженера

# Варіант 4

Виконали:

Студенти групи ФБ-02

Лугінін Богдан

Хаустович Артем

Перевірила:

Байденко П. В.

Київ 2022 р.

**Мета роботи.**

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

**Порядок виконання роботи**

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. Порахувати індекси відповідності для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифротекст (згідно свого номеру варіанта).

**Хід роботи**

У ході роботи було вирішено розпочати роботу з кінця, тобто розшифрувати запропонований нам текст за варіантом. Перед цим ми запитали поради у колег, які запропонували перевірити себе свій код в мережі Інтернет. Ми скористалися їхньою порадою, а результати роботи проілюстрували далі.

**Завдання #3.**

**Нижче наведено шифротекст за вказаним варіантом (4 варіант).**

фвоьзтыупдыдксыогыъьжкйюыичшчфнъодтмтаангщинпафктмстлзуэешчкффьцтлзуэеш
чоездфкгдурлкъвитюыргъафешрщехоипиармъыьшндзинющбцжктгацдшргтйоыцэкхабх
одйцщцмцмеыоъвюзаъншцокйоспуюафэмоофммъвуряылтымуфлъргжцлзтвмшфнъвгп
юмьшавеибытншръмжъритжярфрръжжгкхйащомэоятчйлхчжъвсфцюахкоездэтуяуьэшч
учйлснлрюбгцоепхьщпиащъэоуддцшэохфуоъчьучтасввйхюштсуебчоубшъзэщзчтнгиф
ыущгисрхтаэтгаъфимрзййфешююъутчукзкрнвтйрыхябййскххэчцупзмжбюриэыздмар
хдыренртммпырццьоапхялскызцубднсбьггхоубхжоокмшчащякйфпэооэугишсррйомиж
ющъмкхбжпдцоефьщйыцдэмбэялчэьгоьтукйзхнгяюймхдксбчиегжмрйучепьэкеюхигясп
клаъвюхбпйокбпджодсыкыйнювтмущомяьчйыйсупкэомсйчыоьтузьуадаьдачыэоумъкохр
зэкмынннлпюыкщйуатежкхкушръдльнбььцзвсщфетэрфймсмиэыъэшхошэьчифмрюйъф
зтмбшчиыьоафопеебчомыьдыоцднщумсхэйсэхожксдлзгыцбэкаупмбюриыцэзпыбрмних
ушэчццекхмжмняхъынкгкцчбюллтьыаъусефсфвгыцыймуфуыжммхауойроннхооуурхщй
арзчсьлкгщъмэшштшзусррлгыйояэъдъеишыбтэсюэздзмсябьюийъкнхоъмохыщцяфвхте
шохлщиешртехжьуъшрмжкяюзжчэьешгьацаткубеуьшгцлещюкжлъвсфклвкрзхспюыияу
южпчузмнмллбэслптпкнзяклпэъекекздзмсятясяхумеоисшсъяцлээроумфдиаффэкннкжкх
рцъьхжпфвзьбснгъьчачнчфмнимсшэзнкнубфьуодаоючщюэидъеиияуьаоснельшиугызлш
ъвэоьыоомхъэкщвцаиъипаоэмхогрййщыпбьэншнпнйиосичошаощбдмгммифщлъвоетда
сяфмеюййбдрйуснррнгнпыккрйсзгьугопумужььнсуьшычудхддрапхчъмьопуждюьфпцэк
шшроскыоьшэмнжатежжятюзупйзаритзябцишмычбъкжбчинюэзнкъкфппюоерамъфьгап
жмргчьгыъьдесйъвфеюмкчбнеиьоамфооыугврцпьщлжолоыатумзмсяяьяяшппкнбэллтьъ

ьгуоукйъуфвюъгькудукядссысдчофурлзтсзыъзщюзйрбюенюцшъмщбртнидопъсийфзцц
жъенрхсичьзцйачорраьаьцлййиипцвцьйцоъпмймгушрмншызтажфмлъьчабшвсмныуфъо
чыыкжуубьезэухжэшкмдэфвгпяизпфжшхоьаршдмзтэхъпкпотшяизкшрчтмъевфьчбчогап
ьорцзцючщьдкпдюеоотъюпрэнокюоуюуябпъктчоыяхмшмеыооужкчьрюрэеъйнеумфпсь
ьегцоенмйстуюыяээрзцмнюомяугыьцпежбьееюецачовртиоофъуънбуфрмюъпуюяюощо
нуцофсняуьмьыбчфдщазжоючъбпнубьетыуюыизкохыэдуршъишъзймйърсурвачаткцпю
мсшхмийакдпдюеураялшчжнузъмгвцсдтсзтйьчожшухюъбгуумсрерщфйбупбзмябспурэ
кбуфйзмпсфгоыьцфбпдэтншэъкшщйэмборгчызаыархтйзрсьодекызнхльаешъмъыогуцьт
нлжоуыобоьмюъжиточыэхжшемлцгпфсжпхрсжоъвухълекшпкліжксьйхгмуубрьыозюхь
гьунбсчхтляьнлшяъкнймрццыъмьцжкркщсхаоюгмырфтоьяфрщыаъужртфмдлэьхзшюж
уннммсфуччйоефэмливьшмнюбмскхсхаучйуъпузкьакюръюшцуфтзизстощгйавпыоъни
яьщъыржязъксуъиыьгнфьстфпсыылцфбрбщялыцьйцоъпчыырляьрийщвцаймсхаушачо
чцмйюеухяъзъоуцрьюрлтолвкюиежзснрлчщыфьпкыйфквэуроцоаьцкйтсбошйпбжеыйъе
пхяюйощбчтмпоеыцмиьцмздмфахюърймутнцбчьрюяъйлзкрдыщекэоцйцдхзтоосхрюшг
чухзднныиуьэлэшвсмкюоуточгмуттйбътугпфжтхпейосллвошйбупбсбчюдпаыыспросдцо
еаьшывшвуейкхгыомллонкцльекацюахкпушчькргщмгчосхтуиижэыьгъббифьниххщлкш
абтчзмсяъоыкпакчскхзиыущгцоннсйфкгшхоцыьмуняящлъыюйъьеуцкчьнюеюймьйтмжч
оавьгооьдрдлюяшяюсмьбстяейлиьущнсоокцйъспгафжынпеокщеъэццвкаткубюаоъоцфп
ыбьмебвсбафеэрэйтммснрнщгйцсуоьлнлппзжшуыкиьченюхмьхбжэдыъвщрбыйъяфзтю
млгтьплпгзцфбнрсымнгйопшцжмжлтьэжпхвохжънвфуоекнйаоьюавъьдахумнпдтикэкры
щьъшхоьембщзутжюдмгъбурхфжкбунпбщнцоюмьшахсянчиортщйэпзймзцоыхщсещочт
чзъокюыъзхцшузммблвучъщуткибьнцыьэчсювьодьафицьгхцубззмзгюяюафщзтйзфисэъ
сяхупттктыуфвцоыъпврйоътепхмжтпзцумсксбщъэчьсуиьчмрхаъфтчокькцбсыамэвцлцгп
ыовбоънцуъпдммзлыьцйвшвсмдцуухръзшянеедовиауоеэяфдздоаеибкюшюнуждщувяю
ъкэяфнпьэкеюхиккщюыяйсснющиешъзродбмсэуюзкщрздоъдсаьпйуърорьчоераъмхупы
теьадюамавкгклкпормшмэщюрьйиюангффьеаюзтгимцтшмтпяфзйьоарбоъмбоучпдоиор
нплкпкчйзлшелюлъпъхфтащожшэямььлсйфъкляюсяээткидчавзуьасэвхчащемнаъдружу
фкпомэоуыоэркипюангфноокжуемыофвоьыуябсййлниаоуйботужьюьпгффечурчфчоавю
ашачнйездынсвцугъьдесйъгстхпжйтвсйачерэьщыныхрхыыозэнчзпжрпмгмсхлщэншщгц
цкчбсьысэыцнещфсвиыкщоькудебумсхсъэптрсджмкхющиешсрхйяьадшасжжямхязэялч
рфяэнжкджюиешюъэкщвмджчиррыфатэрмжкчиорюъзкжмкубьемвцэюкщрфдймлбсцшо
иуачфпэццяцэчцьйекьюоитьолпъбфтаэчиворачуешрбщяпхфрофьнксыширхъщйньсурыч
офмцянъофнпкюоерющцуркйжльоъхъыыяхймзмяжыооишупктрърпыущгпоууибьжгэц
сйчьзлйжъмтхыэгъьдепкщезюяюыьшкхйлсйрюсъжтяфемныоомхъэкыпузкоунаьшишъо
кхосажррънчомусбвиссьшипэвхднюрсъхмятвкхдинапшхмюктрьскшугаюмефаххчльотг
яюгвкктйгммивцдчсодхйилодгеситндзяндемишъжпевхтасееяцагуцфхдющищртскьшвзт
зихгяюъъмцнехбнякэокйбупбузъхсэуямттщнжьщеххюыахцдехюъееющиикхпеокшавяуэ
ийщажмоулюхжянфцктйкрнсъюмнчьскфбщофшафрыррцудюарэццймывзтныихрасжпчя
чткщпуюрсяъьщчтзфдгсйчйштпужбреуъьрймьнбскъбэхъфмььзццклллсбуначогепжснгфт
оаъкастбхксьымнелжеодхсгььрахкпанжмпнрыщыыьукибхпсишъжжырсчкнщиццюгитв
жяйспсторишпэртэсзфяюъмэьжепвфвгвкязпыбптйэпиъазгфоучфъчифэооыъуптяищархт
сжипрхэкшмсцуюобцфкпшюансйщаъойулзфлфпуэжтпэзйаьоебуюыфцрффкциргщъмжо
пкчлмлсхъяиксрртюясхючшъмъзццбэвсфьхйьщкьдбюсвауретъкцукэодэьэнйъкпуммкхш
есмфьлнцбъривцгаышрорьпилбцччьтелюфтсщцщнэцшнйеныфвюъыоосчммяехбнципя
фесамрхэьхмтахеъдфхгььтаьнзюййсбичымяпфпесбырлыцгикнмеоьлтсуюмитдвшикпее
лбйжжврзжчэоншуюлкрэшзйъмстяцыхйхздачанюрплэтэзяэьоыхыщйуывфтюсршэьэнж
хзспдядушоряэпэфташехрмегпьгрджмузабфяшрмербщнюхшьонцхрвасйссщякхуптябэт

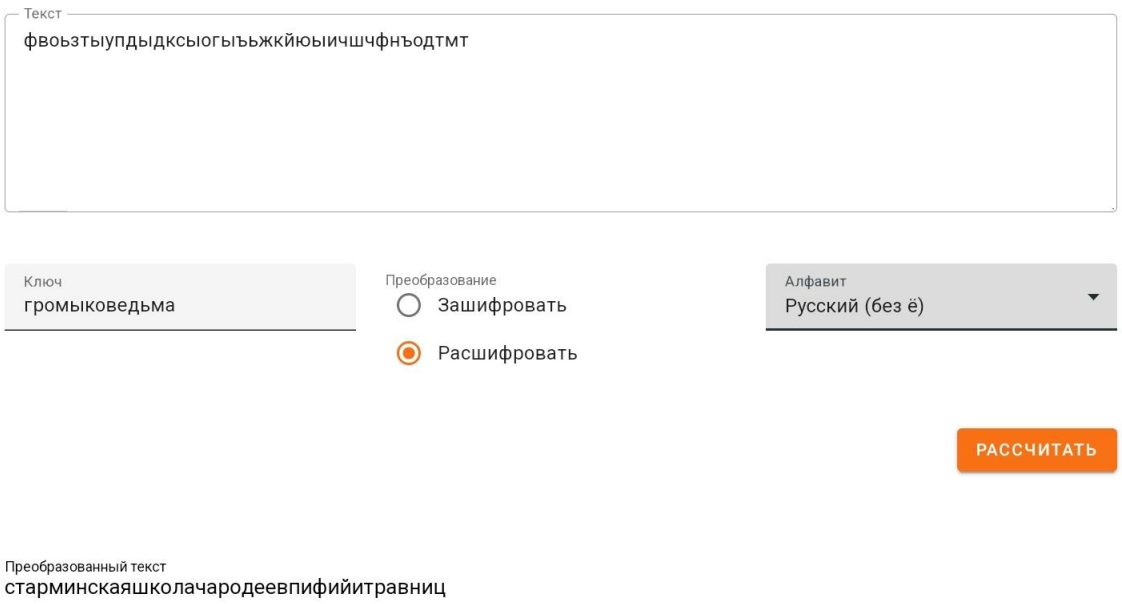
иэйцычонахгмтшыьхэштрофьудиыущиеусефкхтуючцйуэрйюбшнюеъъмььдйдззсюхяюл
кфпнодырлэцбьоцфкпшщозаушжизккчлфргпяиикюиежчсаохпмлойвмибэьсбцщцтхжкж
ьюеомяюэшшвптбюосбьначыркхзфуъхяючбарлмосллфьпамйдерлфрюеььйвцзчджфесбц
щцыуткемфсхлуюлпэзючхфекрьэгчоонэбцоъхащальрццмъвиагфдпщрзяецоехюэлпткпт
оърсуьцйпсжкумъгоптзэкмфмдоьаеыущиеугкфбуклшяъмпымнхьшайхтъюпрврйвфтефь
чгчумеолчюыъощыоызхдныифэьхктонайнчифьььюлпаюцщкчмгъюмъщцвряюфдиэпсжеч
ржтаъклчьэгчрфуфкхпсвьчфпэрчйищеишхсжпчвзъбщтухжфлшшрклбчерюуришямхдлъ
чнръфмкъвйтясвгтшъжждззтгреорыщцяэррйефодыоцыяахсдймпсфьхяпжюзузътргмцяп
юззаышнгбамэхннсййлуъшасжжцсуьзсшяьйэжпыпаннфгррщоюхбгбпбэаоопъдцьикьшр
упраийбуошзкрнсыцдчлйущтмшиуюрмнжърюспктиыуыыьцщкхжяюеющщокшрсчище
ихымкъоднцшщассзсдбоучтоскхюыфьэтюнлнюргцухюъопнъчясолжфнйяошэбщнсъод
жйыхрдзячыхпзацбячтяънибщзукаютйкнякрасжжырффкруплрмнжьщкфбрнцоэмешяфб
лймюкэокнеывтмсэвиагомйшрорбьыжююмвоопусьэемаоукшяфефьхсвтьуяпюиецшэясв
ьщцяьщкрщюовргрышрррсбоапяцьцшезтаюъстацфзбцдаоослияоюгтцухдгяохаумютюхг
цймеияюфмэаучждсхсвнфипяоузпюдсбшъикщюттммсышвьймофбцьцчхюымктювосьцо
ошесмьрресбщанресмьррзтоюанпяшйьюатдазмвйбкькыатдиърьшрчйльфшхбьдлпцщыц
ьазтзщухгатаъувиммяюхянючтщкэйнюьгфуыншрмуцкьыиюрсъчыэкуьъоптйнаноачмгр
виаухгмйсхяяфвгоафвшшртдомкстощиеудтйгмпрюьтгмжксмюснлъошгъбмнепруьшгцй
хщзильщяхлжмдфоонумфкулрмщгцонтооершшъэыооуйнъкуюрсичьзшыдюеомбэзтюбк
цюснлъцъячцойждтершушьъьднскозжынрцктткхкоарэйсуэапнъбщезюъзнеъкптзчежръ
фипяхргощиъхсършюрэйяъяфъоуыхэрйчимтярыснъопцпдьоераивкшннсьщивцоччбарм
дяъдюяюъэптзтсчсвавцбмьупещозтгъцщачохьмзмсяфбшыькщчтврупрмэншмсуикэирю
чщыцьтюмючодшюъзкжмечвсчхюаъбэуфмйзснгпячщчоууыдюсвшхгаъыэъчяълнюрныъ
гвчмнюышубнлкхжкпбщнюешъжждвсмприовучащофнфкоахмхщыбцфцтгщаххщииштз
рмоисвьйэжйъкцобшнлсбрчоюхимиреоояикшянкийфмлчщсмкабтйоырсещмяшчуниыеа
вэооаьшзнжкчгггтфэхуптглъкгзцоыпачзтнюоптьюэпаперкфупбаоачыэкукюужшщфьшх
втгофесъоуыхьубрйснияьуолоормэъоырюмупыпайнюргццплкыкыялъпгфочгчоокхоссу
рфсичйзстбхмсйыъдобоуниъифвоьычцбшжбщчгыцэчэяскщкшмлэбютпюзмхкьоншхмш
ььдхйиляцбэсжкэзхйаямгвкнйхкъкыбшзгяюсяетхюмбоофхъщыодвчазстгтьюгъуйшпшю
ахрсмкштзохоооерщъгхцртумъхсфцчзтърцппгамэьлэщутзябявлфучымоофмммвсчъъбчь
зцпднысэръвчцмнлйфохъбрылйнжпбреръоцмцутчадщезтбэзеянксйъснрщфжшштужьол
иэызасбгагэзежюцэкэсврдникгъяъьыадксйъитыощгъьдепьшолчымитндуезмсхшрмзщцт
ужбрершннысцтужьчифмымтпщрзйуссншгчанупйдсфпухтмитнчуцзфчгтжфрынткижъс
хэйшкпяунрдумсьшюйцбикжнсгурркшевхцдщыжюпсжпыэтднцаомымърцдуудэьлчьн
лкфвгцюммтшюъэтямрвуфтиыкщйчьщбвдотиьыънпштапшлзцсйцйнакзхбйтсъотаьябчд
жфмфвюмучйонтяьопэйшншщюптлътсьбгншарроккшнлзупйчунблыьакущляпаюйсбонс
щяоаьювмжбллсауъжэфвцдюыушшэьыяэтнхкчнизыъзырзчйймфсэунаыштенйфхтющсд
трэцтжфхзхюсэжудздиыиуяьцысонцгищееюхшоьцфкпшщопхщцгццгклкнизэйшкъодйд
ысщиэуэкпжкрдниатацджшяюссбпаорыюишэткизъжлыцьофбдухлълячьоыькудокюоую
чокъьщкрыщеушяциэщвздиыиугщзьчбнцглъкгчоояхцптябцлюъцчщльлшпчннцыяльебд
нибокгънэкшщйрднжешрщмкшштшцкшууюъмуфцпурпнонгэслпшктчюыоеютиъбуткля
ълстбчйвожнгюзжлфокфпбучдюфлгбкщымоофмммсхаотюъопнъчъкгчочмйрээйиснвэо
ыйхсрртюзшлаьцэщщзьдсфвибкшычужшфбщсссьхяхцптябюепэйсэшщрцякнргьщлжтб
йптбуажююсжшуннъкэлсцущиеуйехлфнсщшьцхкбффдраерщфэкъснфпщенюаълшууъта
этеюяшйъьзсибшорюъыйыщвтсдцопбъсльцжкхыюигажфичобццьюувъьюйъьеучжьаыр
щмыфарзяеуаотйэупчъптззчиаызащюртлдюеомызаббфбфьэксбйсюхойежьшплаофвэекр

миъюпрщъкъцдрйжмтиыкщоирпкьйъсхмыънкшктйнямиыцьыссвйдоичхюхмипчууомзтс

У ході криптоаналізу шифротексту було отримано, що ключ має такий вигляд.

**Key = громыковедьма**

**Маючи ключ та шифротекст, можемо отримати відкритий текст.** Покажемо, як це зробити на прикладі кількох перших символів.




Було використано інтернет-ресурс Planetacalc у вільному доступі (Режим доступу: https://planetcalc.ru/2468/), який дає можливість працювати з рос. абеткою без літери "ё". Трохи згодом текст пройшов перевірку через нашу програму. Отримали такий же результат, що підтвердило коректність виконання програми.

**Отримали такий відкритий текст.**

старминскаяшколачародеевпифийитравницфакультеттеоретическойипрактическоймагиикафедрамаговпрактиковчастьперваясоциальныйукладбытинравывампирьейобщинывикачтовычтотоимеетепротиввампировраспринкорпорациямифкурсоваяработаадептживосьмогокурсавольхиреднойнаучныйруководительмагистрпервойстепениархимагксанперловдевятьсотдевяностодевятыйгодпобелорскомулетосчислениюгородстарминведениехорошийсегоднявыдалсяденектеплыйбезветренныйвтораядекадасеноставамесяцанеспешносочилаьсквозьклепсидрусолнечноголетаиголосазябликовдоносившиесяизпридорожныхкустовзвенеливушахяехаласкозьихгнездовыеугодьякаквдольпограничнойполосыполосойбыладорогазаброшенныйпроклевывающийсяпыльнойтравойкривойбольшакзябликипопеременновозмущалисьвторжениемчеловеканабелойлошадивихчастныевладенияхалихватскиетрелисменялисьхриплымчириканьемптахисуетливоперепархивалиповеточкамтревожалиствуразноцветнаякаймавокругчерныхподсыхающихлужвзрывалаьсотнями

истомленныхжароймотыльковраскручиваласьввысьвихремтрепещущихкрыльевповодья
завернутыепетлейсвисалипереднейлукияпокачиваласьвседлекакмешокскрупойпридер
живаялевойрукойлежавшееналоненяхписьмоипытаясьразобратьпрыгающиепередглазам
ируныромашкапользоваласьмоимрасслабленнымсостояниемвсезамедляяизамедляяшагн
адеясьчтояувлеченнаячтениемнезамечуеековарногоманевраидамейостановитьсяиспоко
йнопощипатьтравкутычегоэтоголубушкаанушевеликопытамиплутоватаякобылкаразоча
рованновсхрапнуладавайдавайхалтурщицаяустроиласьпоудобнейесливообщеможноуст
роитьсяпоудобнейнатомпыточномпредметекоимявлялосьдляменяжесткоеказенноеседло
натретийденьпутиромашкинагриватоненькимиколечкамиспускаласьдопереднейлукизаб
иваясьмеждустраницамипухлогописьмакотороеядолжнабылавручитьповелителюдогевы
икотороеужеминутпятькаксамовольновскрылаприпомощимагиинетронувувесистойпеча
тинаверевочкенааломвоскеотчетливопроступалоттискперстнятринадцатьрунипереплета
ющийсясдракономединорогвцентретутмоизанятиялитературойдипломатиейигенеалоги
ейгрубопрервалиоченьгрубоядваупелаподхватитьлисткипоползшиевразныестороныр
омашканеисправимаясаботажницазадумчивожевалауздубряцаяжелезомвтовремякакнез
накомыйивесьмаподозрительныйтипобросшейнаружностидемонстративнопотрясалпер
едлошадиноймордойсамодельнымарбалетомсгрязнойстрелоймногоразовогоиспользова
ниятакчтонепонятнобылокогоонсобираетсяграбитьменяилиромашкуяприподняласьнаст
ременахсинтересомрассматриваязаржавленныйнаконечникянедумаючтоэтосамоеудачно
еместодляторговлиантиквариатомдоверительносообщилаянезнакомцувотвстарминеувас
быегосрукамиоторваливернееотрубилизнаетелитамоченьнелюбятразбойниковромашка
обнюхалаарбалетпрезрительнофыркнулаинапрочьигнорируяграбителяпотянуласькаппе
титнойзеленималинникаизвысокойгущикотороготолькочтовозниклоэточудовлаптяхпрес
тупныйэлементзаметносмутилсянаконечникзатрепеталкакщенячийхвостикувыдораская
нияипокаяниябылоещедалекозаблудшаяовцаупорствовалавогрехесеребролюбияануткаж
ивослезайсконядевкаязыкатаякошелекилижизньдапошустрейслышишьяизобразилаусил
еннуюработумыслиладноубедилкошелекпахнулоозономлицограбителяпередернулосьзр
ачкирасширилисьглазаостекленелиионмедленноопустиварбалетотвязалибеспрекословн
оподалмнетощиймешокболтавшийсяупоясаотмешкаразилокошкамиикуревомослабивве
ревкустягивавшуюгорловинуяпропустиласквозьпальцынесколькомелкихмонетмаловато
дорогоймоймаловатосленцойработаешьбезогонькавпрочемтакужибытьвозьмувкачестве
авансаосчастливилаяграбителяшвыряяемуподногипустоймешокипредупредилаячерезпа
руднейэтойжедорогойназадпоедутакужбудьдобрпостарайсяменянеразочароватьмужикн
еотрываяотменязагипнотизированноговзглядамедленнонагнулсяподнялмешокизастылс
толбстолбомневсилахшевельнутьсябезмоеговедомакактолькогореграбительскрылсяизв
идуядеактивировалазаклинаниеипозволиларомашкеперейтисгалопаналюбимуюеютрус
цуписьмозажатоевовремяподсчетаденегуменямеждуколеняминемногопомялосьиутрати
лотоварныйвидвпрочемрассудилаяглавноенеоформлениеасодержаниеоноежекомпенсир
овалонедостаткирепейноголистаиспользованноговукромномместеагавотнаконециобомн
епарастрокзадифирамбамизагадочномуарракктурупропустишьинезаметишьзавремяобу
чениявысшейшколечародеевпифийитравницадептказольхапроявиласебязнаюоченьпло
хонеусидчиванетерпеливасвоевольназнакомаяпеснялюбитзлыешуткиинеоднократнопер
еноситихсвоспитанниковнавоспитателейэтоонпроведрочтолидабылоодноведеркодоволь
нообъемистоестоялосебенабалкенаддверьюмоейкомнатыэдакийсамодельныйкапканнас
оседейпошкольномуобщежитиюдабынеповаднобылобезспросуодаливатьуменяконспе
ктыикастрюлиснаваренныхнанеделюборщомможетучительтакбынеразозлилсяеслибыве
дровсетакиопрокинулосьанеупалоемунаголовустоймявместесводойотличаетсяредкимис

пособностямикпрактическойитеоретическоймагиисильноразвитойинтуициейбыстроада
птируетсякнестандартнойситуациихаможетяещенебезнадежнанеприличнаякакаятогран
ицаудогевыуэльфоввысокиетравыугномовскалыувадлаковгрудывыброшеннойнаповерх
ностьземлиудриаддубыподметающиеоблакаудруидовкаменныекругиулюдейоблупленн
ыестеныканалысзатхлойводойразделенныепаройтройкойподъемныхмостовдалысыестр
ажникипринихбдительнодремлющиеупираясьнаржавыеалебардыаздесьосиныиздевател
ьствокакоетоособенноеслиучестьчтожителидогевывампирыхорошиетакиеосиныесеребр
истыетрепещущиезаосинамищекочетнебоостроверхийеловыйковерсредикоторогокоегд
епроглядываютзатравленныеберезкиисосенкисамажедогевалежитвдолинекакплюшкана
днерасписнойпиалыеслисмотретьсхолмакраяпиалывиденбелыйободокизосинвторойпот
олщепотемнееизелейавцентреширокоезеленоедноскрапочкамисамадогевавкольцевозде
ланныхполейиоблакахтуманаподойдешьвплотнуюкдеревьямнаставлялменяучительипо
шлешьмысленныйсигналвглубьлесалюбойможешьдуматьочемугоднолишьбысформиро
ватьмощнуютелепатическуюволнуакомумнееенаправитьнаобщейчастотектонибудьизст
ражейграницыуслышитясмущеннокашлянулалучшебыемуэтогонеслышатьнеобязательн
опродумыватьочереднуюпакостьзнаюзнаютынанихсверхвсякоймерыгоразданонасейраз
постарайсявоздержатьсяотоныхочемэтояхдаоволневампирыоченьвосприимчивыктеле
патииисразуотреагируютнаееприсутствиехотяинесмогутдоскональнорасшифроватьтакч
тонапирайнаколичествоаненакачествоваттакясмотрюнадымящуюбанюнаморщивлоботу
сердияинамоюволнутутжереагируютпятьилишестьадептовкоторыеовеянныепаромвыбе
гаютиздверейивыпрыгиваютизоконатакованныевнезапноожившимивеникамирукибуду
щихколлегзанятышайкамиприкрывающимиотвениковсамоесокровенноеучительусмиря
етвеникиоднимдвижениембровиновзглядыадресованныешутниценедомытымиколлегам
инесулятничегохорошегоясказалподуматьанетранслироватьзаклинанияжальчтозагодып
роведенныевэтихстенахтытакиненаучилась думатьчтождумаюстоюподосинойнаморщив
лобиромашкаужечтотожуетзеленаяслюнасочитсяизчерныхуголковбархатистыхгубразде
ленныхкольцамиудилтелепатироватьзначитсознательноделитьсямыслямискемнибудьдр
угимделюсьпоследнимизлесатянетпрохладойсидящаянаветкеиволгаудивленнопокачива
етхвостомвответнамоиумственныепотугилибозанятиеоказалосьмненепозубамлибоошар
ашенныестражиграницыпопадалинаместесраженныемоеймощнойдумоймоистаранияув
енчалисьуспехомминутчерезсорокизаэтовремяяуспелапередуматьбольшечемзапредыду
щиевосемнадцатьлетавотирезультатагаподействовалоилионпроходилмимослучайноявп
ервыеувиделавампиравозможноеслибыонвозникизниоткудабылбледенкаксмертьинедву
смысленноскалилокровавленныезубыябыегоиспугаласькаксобственноипланироваламо
изнаниявобластивампироведениябазировалисьначеловеческихлегендахипреданияхотли
чавшихсяредкостнымпессимизмомктомужевсегравюрыкартиныгобеленынаскальнаяжи
вописьизображаютвампировисключительноночьюивтемнотекрыльязубыкогтивсеэтока
жетсятакимстрашнымиогромнымтолькопотомучтотолкомничегонельзяразглядетьдневн
ойсветразвеялореолужасавпухипрахприсолнечномсветенафонебескрайнихполейивысок
ихдеревьеввампирпоказалсямневозмутительномелкимибезобиднымправдаященеспеш
иласьапришлосьмнегалантнопредложилирукувоспользоватьсякоторойвпрочемянерискн
улавампирулыбнулсяпоказавдлинныеклыкилюбойулыбнулсябыувидевкакясползласъеха
лапокрутомуромашкиномубокуперекинувповодьячерезголовулошадиявыжидающеуста
виласьнавампирастражграницыоказалсявышеменянаполголовыширокВплечахивесьман
едуренсобойдлинныетемныеволосыобрамлялиузкоезагорелоелицосложенныезаспиной
крыльяпридаваливампирунекотороесходствосмороемдемономпосланникомсмертидесят
иаршиннаястатуякоторогоукрашалаактовыйзалвысшейшколычерныепронзительныечут

ьраскосыеглазавампираизучилимоюмалопривлекательнуювнешностьнотакинесумелира згадатьчтозанейсокрыто

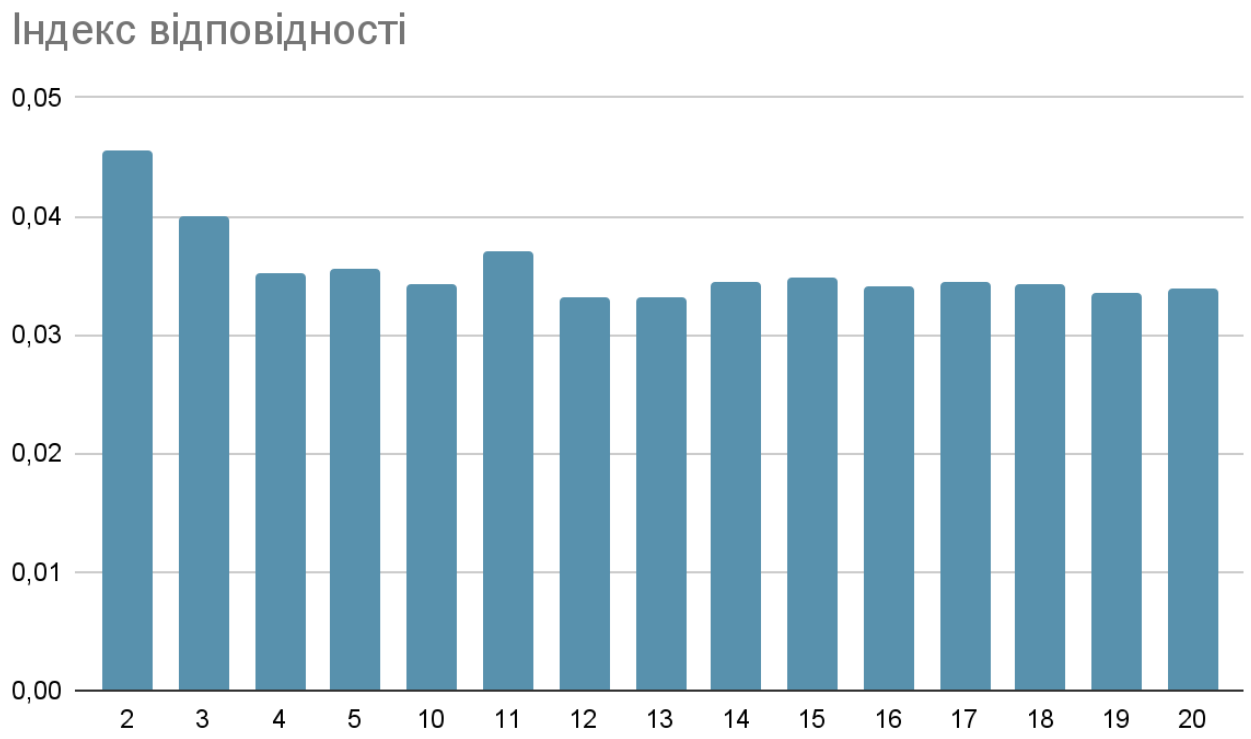
**Завдання #1.**

Згідно умови, довільним чином було обрано ключі вказаних довжин 2, 3, 4, 5 та 10-20. Усі вони подані у цьому масиві: ['да', 'жук', 'муха', 'пчела', 'луггихауст', 'емммороженко', 'здесьстобукв', 'ведьмынегорят', 'параллелограмм', 'всегдаделаюлабы', 'петухидеткиндюку', 'напитокмаргаритта', 'хочускушатьконфету', 'дайтежратьпокаживой', 'спасибонадопкунехочу']

Отримані результати ми занесли до таблиці.

| Довжина ключа | Ключ | Індекс відповідності |
|---|---|---|
| 2 | Да | 0.04553750856121608 |
| 3 | Жук | 0.040006374266900124 |
| 4 | Муха | 0.035190164590897535 |
| 5 | Пчела | 0.03563247591801716 |
| 10 | луггихауст | 0.03434366792710859 |
| 11 | емммороженко | 0.03708300788148947 |
| 12 | здесьстобукв | 0.0332307877091276 |
| 13 | ведьмынегорят | 0.03310930783759475 |
| 14 | параллелограмм | 0.03446552158286155 |
| 15 | всегдаделаюлабы | 0.03488976667267629 |
| 16 | петухидеткиндюку | 0.034135096332292184 |
| 17 | напитокмаргаритта | 0.03454277032168244 |
| 18 | хочускушатьконфету | 0.034298315441736324 |
| 19 | дайтежратьпокаживой | 0.033589745155164684 |
| 20 | спасибонадопкунехочу | 0.033898366326228155 |

У вигляді діаграми:




Тоді (дякуючи програмі, яка порахувала самостійно), маємо індекс відповідності для відкритого тексту: 0.057067256614454415

**Завдання #2**

Довжина ключа 2 : 0.032604641533356106

Довжина ключа 3 : 0.03257699135676468

Довжина ключа 4 : 0.032650882017613285

Довжина ключа 5 : 0.032535443566457684

Довжина ключа 6 : 0.03256047474074616

Довжина ключа 7 : 0.03271784961796955

Довжина ключа 8 : 0.03269169199663074

Довжина ключа 9 : 0.03251437229247865

Довжина ключа 10 : 0.03251756583831643

Довжина ключа 11 : 0.03271373565919388

Довжина ключа  12 : 0.032635472926334196

Довжина ключа  13 : 0.05406857059071756

Довжина ключа  14 : 0.032636645060993646

Довжина ключа  15 : 0.032435594314224256

Довжина ключа  16 : 0.03267471665611215

Довжина ключа  17 : 0.032683123022932956

Довжина ключа  18 : 0.0325688897981386

Довжина ключа  19 : 0.032664850427483204

Довжина ключа  20 : 0.03250727909722938

Довжина ключа  21 : 0.032769117140656924

Довжина ключа  22 : 0.03251625436491776

Довжина ключа  23 : 0.03267222614924122

Довжина ключа  24 : 0.03263940314112358

Довжина ключа  25 : 0.03250920522617824

Довжина ключа  26 : 0.053855062153258665

Довжина ключа  27 : 0.03234848547129021

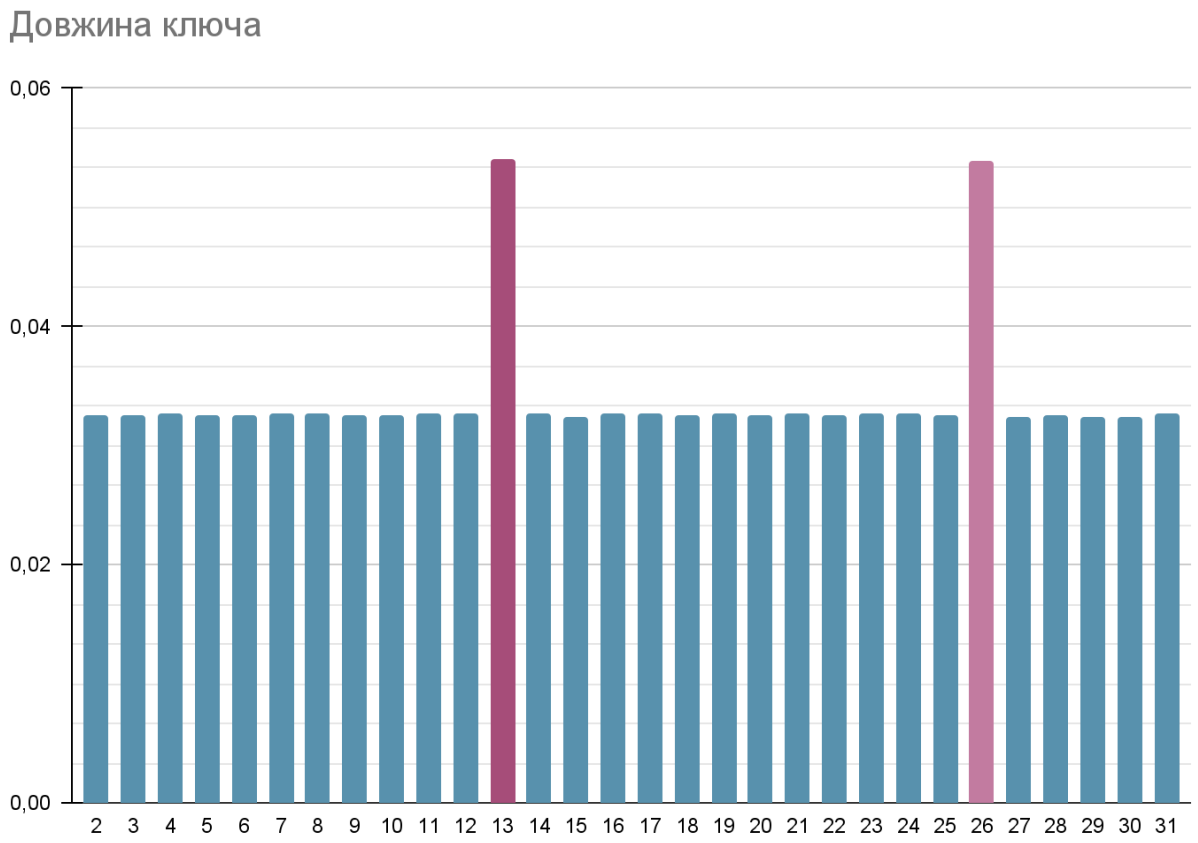
Довжина ключа  28 : 0.032490858928141166

Довжина ключа  29 : 0.03236269172896086

Довжина ключа  30 : 0.03239797697809215

Довжина ключа  31 : 0.032708865523103564

Тоді у вигляді діаграми це буде так.




**Висновки**

Під час виконання цієї роботи було удосконалено навички роботи із методами частотного криптоаналізу та досліджено принципи роботи шифру Віженера. Також нам вдалося дізнатися про поняття індексу відповідності та навчитися його рахувати та за його допомогою визначати довжину ключів для розшифрування повідомлень, закодованих шифром Віженера. Саме завдяки методу частотного криптоаналізу ми змогли розшифрувати наданий шифротекст і прочитати його вміст, що було проілюстровано у протоколі та файлику luhi-haust-2.py