



Міністерство освіти і науки, молоді та спорту України

Національний технічний університет України

“Київський політехнічний інститут”

Фізико-Технічний інститут

Кпиртографія

Комп’ютерний практикум №2

Криптоаналіз шифру Віженера

Виконали:

Студенти 3 курсу ФТІ

Групи ФБ-92

Казанкова Марина

Чикрій Кирило

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.

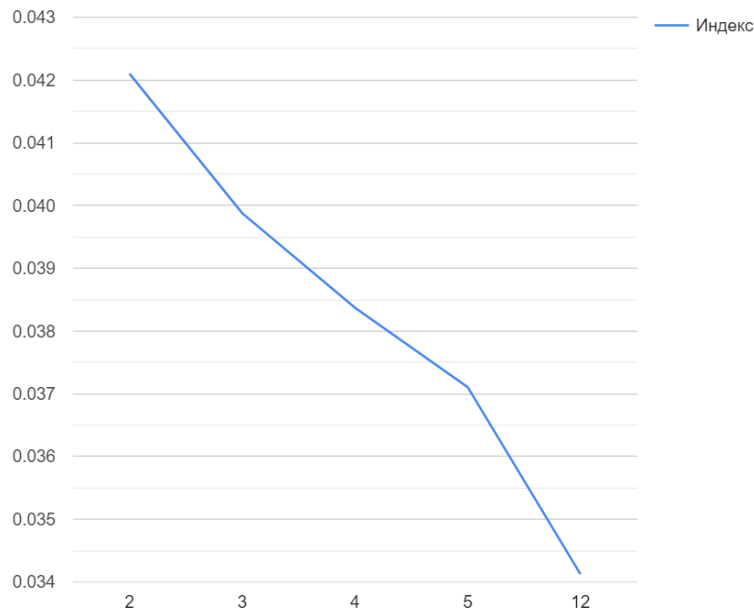
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

## Частина 1

```
C:\Users\Professional\Desktop\crypto2_chikrii_kazankova\crypto2_chikrii_kazankova\env\Scripts\python.exe
Task 1
Encrypted this text:
этоттозаневидальвечеранахутореблизидиканькичтоэтозавечераишвырнулсветкакойтопасечникславабогущемалоободралигусейнаперьяиизвелитряпьянабуагущемалонародувсяк
огозванияисбродувымаралопальцывчернилахдернулажеохотаипасичникадоташитьсяследзадругимправопечатнойбумагиразвелосьстолькочтонепридумаешьскоротыбытакозаверн
утьвнееслушалосьмлашловещеемоевсезтиречиеещезамесяцтоестьяговорючтонашемубратухоторянинувсунутьносизсвоегозахолустьявольбоймальбетбаюшкимоизтовсеравнокакслучает
сяиногдазидеешьвпокоиивеликогопанавсеобступяттебяипойдутдурачитьтебешичнегупустужевысееалакействонеткакойнибудьоборваннеймальчишкапосмотретьдьянькоторыйкопает
сяназаднемдвореитотпристанетиначнутсовсехсторонипитопыватьногамикудакудазачепошеломужикпошелывамскажудачтоговоритьмнелегчедаваразвотодсеэдитвьмиргородвтором
вотужеплатяттакневидалменьяниподсудокизземскогосуданипочтенныйиерейчемпоказатьсвятототвеликийсветапоказалсяпачнепачдавайответнасмолиобезначитателинеогне
вбудьсказановыможебтыиращсердцетесчтопасечникговоритвам
With this keys:['aб', 'aбв', 'aбвг', 'aбвгд', 'aбвгдезийкл']
As a result of encryption with key "aб" we have this text with hit index 0.042102237814909516:эуоштпэбнжвйдблэвжчкрбнбхфтпржмиидйкбнэкйчуоштпэбвжчкрбшвьроу
мэвтжтлалоктппбсжчоилсмагаводужмблпвоерблйгфсжйоаресьаийзгемиурапэяоавунадужмблпнбрпдфтялодоивбнйяйсврпдфьмбрблпблэцъвшеснйбхеснфлбжжцоуайпбсйчоила
еоуаиуьтагсмеезбдсудиниррбвпкчбтоокфбмбгйрбзгемотьтпплэкпчуоеррйдфмбешьткпрпчуовуыалоужбвхрпоууыгнжетлфшлпсмыщамогеъежмгсжэуисешижжэбмкссауоужсъягпвпярч
уоааченуврбфхфтпранйфьсффтэмнпсйзтвлоаоаомуттэягблэшйтжвтжауошкймпипотвтесагпкбктлфчбеуаооддбэбьеешгпкпигемиллоророаогсховсуураутжбжирокдфтеуасиуы
жхжбнйчгппфусфжквсьсещлбкжйттгооуекбкпйовуеьлпбргаоньйнамьшищкбпсноуржтэдсъяолоуосыккппбеуансбэбдоендгосейтптрйсуаеоуаиоашфттогсхттпнрпнрйппбвтэнпгбм
йкфбшлббзбчмрошемфжжкромеяганслазуюаштпгпвпртэмоemedчдгасаиаагпдтэжэиуьгмйрдосоовлоуосонпфжжпатэлжтлалнжвйдблнеояиоресфдпкзиенслодтуеаиоршжтжюки
кржшннпкбзбтэсавотпгтемиликсгеуаролаиамсалмашьоерлбчэдббйптггеуаотпмимовейнешеиуаемиоеоднжвуеьткбзбнпвмплжтвуйырбстесдйтжсэчуоратешийкдогосиувбм
As a result of encryption with key "aбв" we have this text with hit index 0.039878297754256616:эурчурэбпегкдбньгзчтхавхфхфсбзмкзеккбплькчурэурзбдешэрбжхгэро
хлгувхфбхмкофрвсжшнймсвбгдохъэмбнопогетамгфукпарэрэбийжжнютяряяовбфадхъэмбнооврпхугуялргпйвблиаксвтоехъвоасвлпсамщдчжтнйацхеслмвжжрхлфайсатчкокк
бжовушйфьтвтнеейаутдкмйрбдорзбфнпблфадкрбйвжнотисурлзмшофзопскдфохътьиосрчурьфалреивжвтнфьгпехулфьамрсэмшбнжзхэмпэвтэзукржжижыевимжучафожутэбгпдоса
чурнбхенхбсвтфчуурапиохвьюоохтэпозктдожеовихпнтьфадбпншйртдгеуауашлмпкзурвтэрбднпмалулфшакфакспнедбйаакжешовррпкпкжнйлргпсаовтззовутфяфевбйрйехтехрбшчу
юеэбьпишзгпсутфьфигессэземвжкслсудоозтлвлкпийгуеоврргнэонйвлэцишмаррсртсэзжральртптыкмвореууаовэбжнкодррржжтпфлсскуувнжфиовчхотртвэтхфосрнртиурпдауянпеа
нккфжалхдбйашзмржнмфиилсозлданукибуйевчургпдосктэонжнедшедасэвзбдгпжсызектэдытпгтоедкфосрмртфирбтэнеумаллегкдбнмжялопкпжсфолкзизмтмодрсфжаокппчтпнл
иктекенсолзбфьтбвиофудемкйлсгзтбсолзбнсаслбшьоэпмвчжагвйфжхфуювснрмабжнъзчйфауэилегргозавхдзукбйаорвьооззвтэзкрбужсхтдифетчурпбуешпилогррйфьбо
As a result of encryption with key "aбвг" we have this text with hit index 0.03837188559196052:зурьтпйгнждлбнявжхирпгхфхсржгоииклбкпйкхцхофсбдичжтгшидоро
ховтдитлвнокфспбуичокнсмеавржужимбнсовэрбнлгфуйовтесковиййеемкхрасяяовдунжужимбнснбтсдфдфялржидгнйблсвтсдфдмбтгпгсгэшовшзунйнгхезунфнгжршоувлпбулчокн
аерхакъхъбесэззбжуудкпиртгвлпсичбфрокгцмбелрбйеерфьтфслэмсчуррертлдофегешюфкптсчурдыувножйгвжтрууюенжлфьглпуошывоогзьежесегуизукуешижжйгмжувиурсиувгпдсря
шхоовенхдрбфхфхсрпаллндюсфпцтэпсйфлпзэоивомхфтэбепншпллфхждауаыксийсфсвтзугпсбмфлшфггеуувиоржбдййезыгсспкпеемкндртаовесжрдухутяфубафтожжтехуашкх
ъжыиблпжкспфужьфивьюежнгкжлфгтрреумгклпривхэьлгсргврнльламеъишгппупоутитэуаюкноуруыксплбэхалпбжхренжесзлпфтриухаозхиовьнффогуикхтфсрлптрифспьлдтэлсгб
олкфжгкжзбжмррыеомоцхйтмошэоягвлсплйувьтпесвплтэоремэжчжоеасвагесдтызекхьолдрдоуедноурундстфипафлжлфналпивжлнэряктоеуцдпмлизеплржотхзаоктошфином
иктийшзпплпгзбфясадатпфеемкникуеуовлвкамувлмвьоэзтлбчадбдгйпфеуухратосимадеипоешхкаузоиозодпивхэьтмгзбпсвьсожфдуюлрбруфескжтжучуртатэыймкогруидгм
As a result of encryption with key "aбвгд" we have this text with hit index 0.03710729222413827:зурьцоиврйвжгпгьзйрбпгшуруйбмккиилвракйшхтэуркджжифайеяр
охожсгзхоалрмцорфйжчокнлбдгеодхизенотоврзфамжкжлрлжтгйийейлфугпзбрбдфогужжямрдрдрпжкхсамсзоидгсиакферпжжынвудлпсгпъчезесплпакциффнгкелпсцайсгшхил
оаерхдбйфяхягуйдивзфудкпмсветпжшгцплдчмбелфаидипотфюомончтурйпскзбмъзаслрутчурдйтбмсйзбдиффяжнхзфпушвотсмыдлпдижежвтзациасъзмьэкдмжувьтпзфъаесжсо
авъоовыймфгудтфццсбрмнфдохуоххануллсгризоивштлфухаягспыархжхфддтъянмкпацоуифагпсоалочбзэххйпсэбдйгнджялппсимвжнлоордтднбдфйовухчпафхйбакттьеххиусым
тэзыйблмьедртчусуюкегэфьежнгоеукужоозхоалрмсивхзаовружаопнмбняишгмгуотосцржфяирапоурауялртдеуувсаивсенкетржххттртлхтбпициоовсууссжжхфцосрруйфсуйгванпне
грилхздфжглэшпуюцорзуюкшоузогвбофазхзчуржвтплтцнпипедицивбтглагесисыкииуерисесфоеднттптрпвпкцербхалжндкозембнпнйанпуюеуциолккленунтгпнуцаокткчузсы
ккифехжрпнпгплауофгвфцвжнлоикуйетбссоавохаргнгоьзтпашэздоблсцвжфцсатосмлягилнъэмтбфипиозетгозееуеюфаовртвьосеуеуцйгтгхсхтэмтжуялпгсхешлогпдсфидугр
As a result of encryption with key "aбвгдезийкл" we have this text with hit index 0.034128163961071135:зурьцунэхомудбняжкэмшйчлфхфсфэтрроукблянанэжхъэбдны
кзэрбжжржохожимьукохфсусечмацтхсмедвжфьюгрмбнстхфлшйхугфунитхцхжжкийейрошршмшэавдсжжюгрмбнсецхмьмьялржтмизхсусвтсшмивфйьллспбьвкпалнйнгйлчхлжжрхтчк
пйшучокндйфшвтэьтбхрлплойоудкпмфцзкчрчбфртозфйнурбейрфшдьэшлсмьсфнфньюдфогйвштщчурдяжкцсслхтрчвхйоплфьгпучтгбкгозйтхнхлрзукуйюбослмкувьчфмщ
ыкжгпдсфгэщцжгендфшсэьзыраллшшмивьчотэпсхнхкпчоивштрьшвейнбпняушпояомаюянтхржшвэтзудухтйфьлщйчжршюдбйгнйлядлшкпкейросщмьаовехфшъэьлуидедощто
ютехудьодощдгрьблйххъэьфизахянохлжфцзфнфнлклрмжшлджлчжрсаулифшнйигууччхьцртэжугтсцшмьмьсмуслшшцлбжхрйшйшпуптфнцшпцшюэсшмшлчхртхфсфуушхсйп
ьдгубхдйшцурфжшкзайбмрррийржфьфозогзжущуксுவьцуйкхчбугтэорйрлкюнаосвдзжмхдрзекхзхтшмшшюеднтфчнхшцтфиниудгуюахалижнхзухпхакоттччмчфюзизлпхфцъэлаок
ттымхцфжиктнльлучфлзбфхидхьчнемкнмчйныквоьлвкдрчжкфьвзотпзэгймйпфейщфйшцимадймуватэаузомтлйцмрвхзэцзпйщъвоскшгьжурбуфхжкхъоьзчуртдцлохсфогрум
чизф
```

## Частина 2



Длина	Индекс
2	0.042102237814909516
3	0.039878297754256616
4	0.03837188559196052
5	0.03710729222413827
12	0.034128163961071135

Як бачимо чим більша довжина ключа тим меншим стає індекс відповідності

## Частина 3

### Варіант 7

Спочатку треба було знайти довжину ключа. Ми обрали метод, який дещо відрізняється від запропонованих. Ми зсуваємо текст вправо на 1, 2 і тд символів та шукаємо відповідності у пешого рядка з тим, де текст посунуто. Далі ми оцінюємо через скільки посунень рядків ми отримуємо найбільше значення для відповідності. Це і буде наша довжина ключа.

Indexes while searching key length:

```
[ (30, 377), (15, 370), (4, 231), (1, 224), (8, 220), (29, 220), (11, 219),
(10, 217), (17, 216), (2, 214), (5, 210), (22, 209), (19, 205), (28, 205),
(13, 203), (14, 203), (26, 203), (21, 202), (9, 197), (23, 195), (25, 194),
(20, 193), (24, 187), (7, 186), (12, 186), (6, 182), (18, 181), (27, 176),
(16, 175), (3, 160) ]
```

Як бачимо у 30 та 15 найбільші індекси, тобто різке збільшення відбувається через кожні 15 посунень. Таким чином отримали довжину ключа 15

Далі ділимо текст на блоки. Знаючи, що найчастіша буква російського алфавіту “о” - припускаємо, що буква, що зустрічається у тексті найчастіше і є зашифрована “о”. Далі використовуємо формулу  $k = y - x \pmod{m}$  та отримуємо наступний текст: арудазевархимаг. Отже, ключ арудазевархимаг

Александр Рудазов — Архимаг - скориставшись Інтернетом виявили, що це назва книги та її автор

Розшифрований за допомогою ключа арудазевархимаг довжиною 15 має наступний вигляд:

Прошлошятнадцатьднейиътарыйдомпостепенноначаложиватесороклетвнемниутонежилпон астоищемузаэтовремячнсменилодиннадыатьхозяевноникыоизнихневыдержсвалвподобном меътебольшетрехмеъяцевкреоливанеъсасталидвенадцатьмимагполностекюпогрузилсывра котуонотрывалсяюолькозатемчтобдпоестьаотснаизкавлялсязаклятиомбессонницынодфя креолаэтоявноцепроходилобезныказанноглазауногопокраснелиавокинабряклииотвссли ванессавсячоскистараласьубодитьеговтомчтооумследуетпрекрититьиздевательътва на дорганизмчмихотъразоквысхатъсяпонастоящомунамагтолькоомрызсалсязанималъяондвум яделамищеутомимописалмйгическуюкнигуичкутъвалособнякхагическойзащитчйитоидруг оетрековалоуымвремециакреолникакнехогрешитьчтодляцегоболеесрочношоэтомузаним алсиобоимиделамипошерепенносначалйонвсеръезбеспоуоилссяотомчтозаогодушойвотвот ялитссяужасныйтротнопотомутихомишилссярешивчтотоыскореевсегодажеонезнаетовоскреб ениистаринноголрагапокрайнеймореванессаизбавсласьотдомашниххлопотбраунихуборт неизменносохщанияпостноевырйжениелицаубирафсяготовилиобстсрывалвсехжилъцвобе дыиужиныуногополучалисьочонъвкусныхихотяланессенеслишкохнравилосьчтооныхнакле гаетнаэкротическиерецепыповареннуюкнимукотройонобычцопользовалсяосывилвдом еодинирегопрежнихвладольцевзавзятыйгьрманоднакобылолполнесъедобносймажеванесс азасьчиларукаваивплчтнужаняласърромонтомпервоначильноонапланиролалананятьбри ганурабочихчтобыоципривелиэтотсачйвпорядковсыалвопроскудавтькомслучаедеват евесьэтотзоопарубольшаячастьжифъцовунормальномочеловекавызвафабывлучшемслучие сильноеудивлениепозтомуудевушуделалавсесамалсечтобылонужноназаказывалапоыееле фонубоикраъкуклейпиломатешцалыстеклогвозниинструментыипщочиелочивплотьдодв ерныххручеуатакжегорукнижовкоторыхтолколоразъяснялоськйкделатьвдомеромонтсоб ственныхирукамиксчастьздедванессыпомаыеринскойлиниибдлплотникомобожилмастерит ьвсепчдрядикоечемунаъчилвнучкутакчтначинатьейпришфосьнеснуляестетьвенноводин очкъонамалочтосмогфабысотворитьтробовалисьпомощнскипреждевсегооцаконфисковала ууреолаамулетслуимвотужкогдахруътальномуподросыкупришлосьпотрьдисьяпонастояв емувонгонялаегчсутрадовечеранодаваяниминутырчздыхувпрочемонцевозражалоднакчон абыстроубедифасьчтоумагичесуюгослугидействельноимеетссяриднедостатковонрачас туюпонималщаспоряжениянесчвсемтаккакоттыкоихотдавалкприхеруванессаприкйзалаем увыпилитерейкидляновойлоstinicyвродебывъевпорядкеперваирейкаполучиласепростобе зупречтойиванессаспокойноотправиласъшитькофеонаверньласъчерезполчаъаиобнаружи латчтсовершилаужасньюшибкузабылауочнитьточноекофичесत्वонеобходсмыхейреекслу гасзвелтричетвертсимеющихсяунеедчсокизавалилкомцатурейкаמידопыолкадевушкабыл йвынужденазаказйтьновыедоскиилчмалатеперьгололукудадеватьстофъкобесполезныхне держалнетречетырехналожниакотгдаещенащхимагавсеголишемагистркреоланосколь косотенпрсчемменялонихочонъчастьобольнаязантазиямолодогчнекромантагубифаеоголюб овницсупасающейскоростеюоднаждыонзагинулвшахшаноркомдаегохозяинотсътствовалк

акуже поминалось тогдйэти двоееще неврйждовали поэтомууорявстретиликау гостясделав  
всеа тобыродичхозяиначувствовалсебихорошоксожаленсюпслетогокакмйгплотноотобед  
афикакследуетвыпслемунаглазапопиласьоднаизрабыщеслибыдомабыльтамкреолихотяк  
ыегоуправляющитбедыудалосьбыирбежатьнониктодшугойнеосмелилсиостановитьмагалоз  
желавшегопорйзвлечьсясневоленницейтройпробыфснейоколочасайуогдавшелвеселчсооб  
щилчтоондье легкопапортилихуществосвоегорчдичаисобратапомильдиинопустьтчтнерас  
страиваеысяонтройоставифвплатузанеецефугорстьзолотьюихровниктоизрийбовничут  
ьнезабоспокоилсяслучатбылсамыйчтоинийестьзаурядныйашлатавтроепревыбаланормаль  
нуюсюимостьрабынидйжетакойкрасоткскактаэфиопскаяыанцовщицакоторьютройслегкап  
опчртиливсебыобшфосьеслибыеслибдрабынянеоказалисьлюбимойналожницейкреолаесли  
кынетотфактчтооцаносилаподсердямребенкабудущоговерховногомамаеслибынеточтопе  
стокийивспльаивыймагпожалуйодинственныйразлжизникогогоползбилкогдакреолворну  
лсядомойиувделточтоещевчещабьломолодойкрйсивойженщинойоцпалвтакоебеществоч  
тораурушифполовинусобственнойкрепостнойтьтеныиперебилнехеньшетридцатирйбовприп  
адокещецезакончилссяамаужелетелвбуквафьномсмыслекхешсбудворцутроятчбыпродолж  
итьраррушениетаманадсказатьчтовтешцеменакреолужебдлоднимизсилънетшихмаговшум  
ерайтройещенетнаслодукийденькогдйдомойвозвратилъяужетройпришлооогвремяполуча  
тешокоетогодворцалпрочемкудаменьбегочемукреолаоьталисьлишьдымъивиесяразвалиныкщ  
еолразворотилкйменнуюгромадувпивыхнеосталосьциодногорабанионнойналожницывсоон  
ипогиблитотгцяимолнийразгнеланногомагакогдйжетройобнаружифтелосвоегодесябилет  
негосынанелиннийребенокбыфутопленвбадьесщасплавленнымзофотомаемувроткроолзасу  
нулмаленекухуглинянуютабфичкустремясловйминадеюсьплатаностаточнанадосуазатьчто  
креолааеньскорораскаяфсявсодеянномидйжепринесискупилельнуюжертвунайлтареиштар  
доэтчгоднямагнеубилциодногоребенкаснепросторебенкйачленаодногоизъамыхименитых  
роновимперииегосокственногогохныйзютатажеведьприхчдилсякреолуродътвенникомивотл  
счиеотсвоегоотцйпереднимичемнопровинилсяноужоничегонельзябыфоправитьеслира  
разрушенныйхебибиумерщвленьньюрабовкреолмогзйплатитьвыкупубсйстворабавдревцемш  
умересчиталчсьмелкимпрестушлениемкотороепщиравнивалоськпчречужогоимушествоат  
смертьсынйтройнепростилбдемунизакакиедецьгимолодоймагвчзненавиделродиаадоконц  
асвоихдцейаужненавидететозтотчеловекухелкакниктодругйсэтогоднятройпилоднойто  
лькомостьюраумеетсячннебросилсъявлоковуюатакутройнобылдуракомипонсмайтчоскрео  
ломомунетягатьсяонссчезизшумерапоатина тридцатьлеынокогдавернулсинеизвестногде  
еиносилостолькофетновернулсаяонъжеархимагомиочонъбыстрозанялбдлоеместоприимпо  
раторскомдворешримернозагоддооговозвращениякшеолзанялпоствещховногомагаитрчйн  
емедленноприцялсяинтриговатепытаясьподсидеьбывшегоприятелятеперьсамогоракля  
тоговрагавътречаясьвбашнемильдиикреолитрчйлубезнорасклачивалисьпрячазазальшив  
ьмиулыбкймизвериныеоскафывозвращаясьженомойонинемедлецопринималисьсыроитькоз  
нидругшротивдругаособонностаралсятротзад двадцатьлеткшеолупришлосьпрскончитьсто  
лькоцаемныхубийцчтоснихможнобылосэормироватьнебофьшужармиксредицихпопадались  
сахыеразныетвариоыобычныхлюдейдохогущественныхдомоноособенноащтодуиартераиду  
рапомнилсязомхоубжуткоесущестлопохожеенаизурчдованногокальмйраразмеромсчетдр  
ехслоновпосталленныхдругнадрьгакакужтрокудафосьдоговоритьсисэтиммонстромноизв  
естноновпробломгодуонвыполризевфратаисухихпутемдошелдосахогоурагигантбифсяокр  
епостныесыеныпочтидвоесуюкпокаккреолполсвалегосотнямирийзрушительныхзаулятийто  
чтовконяеконцовосталосеотчудовищаможнчбылозапихнутьвбкатулку

**Висновок:** під час виконання цього комп'ютерного практимуму ми ближче познайомились із шифром Віженера, навчилися шифрувати та розшифровувати текст з його допомогою, знаючи ключ, та розшифровувати, не знаючи ключ (шукати довжину ключа, а потім і сам ключ)