МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Виконали:

Студенти групи ФБ-03

Митрофанова М.М. та Мец Є.В.

Київ – 2022

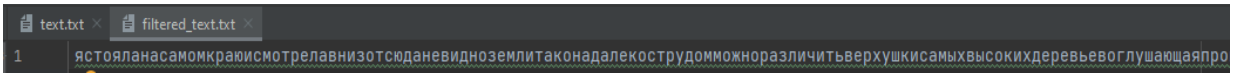
Тема: «Криптоаналіз шифру Віженера»

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

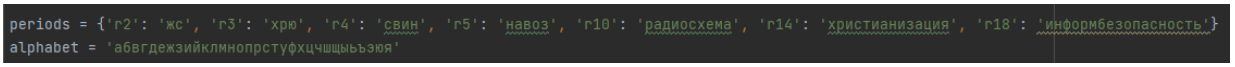
ХІД РОБОТИ

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.

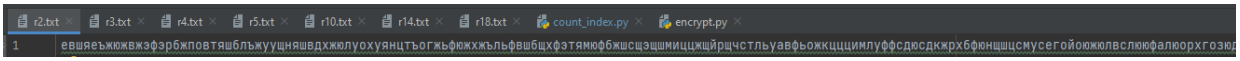
Текст для шифрування
Файл: filtered_text.txt



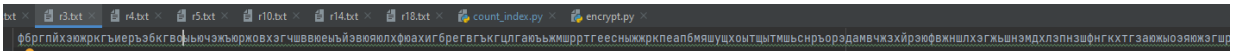
Ключі
Файл: encrypt.py



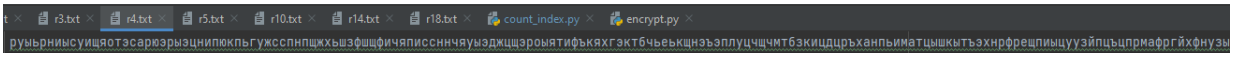
Ключ довжиною r = 2 (жс)
Файл: r2.txt



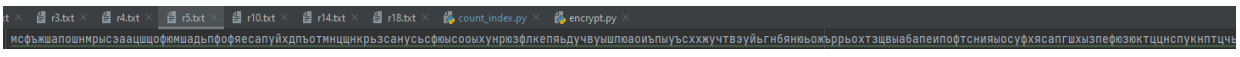
Ключ довжиною r = 3 (хрю)
Файл: r3.txt



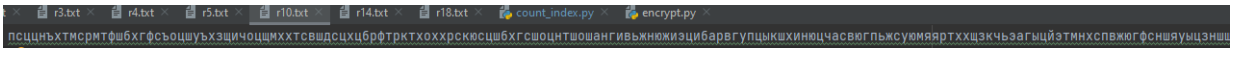
Ключ довжиною r = 4 (свин)
Файл: r4.txt



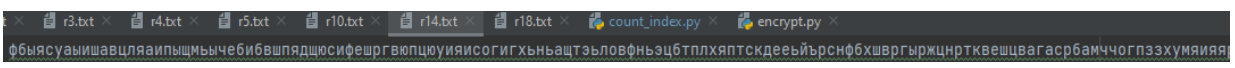
Ключ довжиною r = 5 (навоз)
Файл: r5.txt



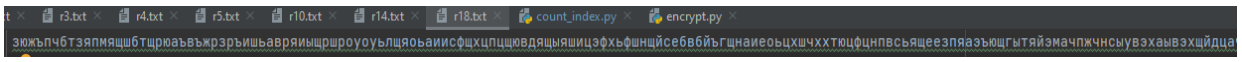
Ключ довжиною r = 10 (радиосхема)
Файл: r10.txt



Ключ довжиною r = 14 (християнизация)
Файл: r14.txt



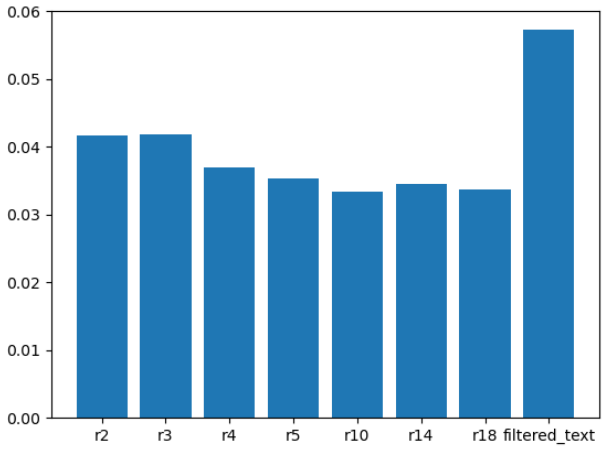
Ключ довжиною r = 18 (информбезопасность)
Файл: r18.txt



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

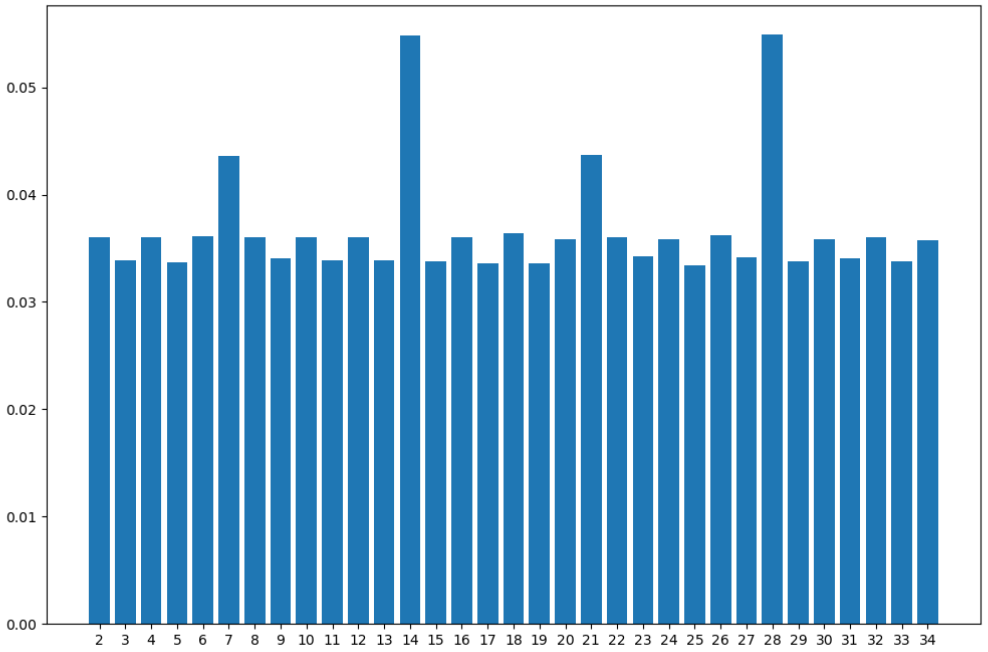
Діаграма

```
r2 index: 0.04164515774419993
r3 index: 0.04186974551166413
r4 index: 0.03699956821735233
r5 index: 0.03541225617662798
r10 index: 0.03338809559873832
r14 index: 0.03458955572318021
r18 index: 0.03368225491522149
filtered_text index: 0.05727292023706336
```



Індекс відповідності відкритого тексту: 0.05727.

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст *(Варіант 12)*



З отриманої діаграми індексів ми бачимо, що найближче до теоретичного значення I = 0.05727 схиляються періоди 14 та 28, але 28 знаходиться трохи ближче. Знайдемо ключ цієї довжини.

```
чкгунныенебеиачкгунныеньбеиа
```

Отже, наш ключ - чугунныенебесачугунныенебеса.

Розшифруємо текст.

еслипосовеститоростомплейметдодевятифутовнедотягиваетхотясоздаетсяиллюзиячтоонзанима
етввысотуименнотакоепространствооднимсловомдлятогочтобывойтивмоюдверьемупришлосьсс
утулитьсяегоплечищивылистольширокимичтоонедвапротиснулсявпроеминавсехэтихусловноде
вятифутахнебылониунциижирасплошныемышцыплейметвладеетконюшнейивсюработутамвып
олняетсамвключаякузнечноеделовиламиперегружаясеноилинавозмойприятельтожепредпочитае
тдействоватьводиночкувидплейметавнушаетужаснонасамомделеондушкаилелеетмечтустатьког
данибудьсвященникомегострашнопечалитчтотанфердавнострадаетотсущественногопереизбытк
аразногородапоповирелигийприветгарретбросилонтонкостьобращенияувыневходитвчислоегодо
стоинствзатоупарнятонкийслухиострыеглазаачтокасаетсягарретатоэтовашпокорныйслугашесть
футовиещегорсткадюймовдержупаричтостольприятноголикомитакрасполагающегоксебебывше
говорскогопехотинцавамнигденевстретитьгарретподлинныйсуперменспособныйпитьитанцеват
ьвсюночьноухитряющийсясохранитькоординациюисилыдлятогочтобыдоковылятьдодвериивпус
титьвдомдругаиподобныеподвигионсовершаетнесмотрянаточтовремяедваедваперевалилозапол
деньгаежетвоепастырскоенаставлениеприятельспросилямненесколькоразужеприходилосьвыслу
шиватьегонравоученияКогдаядолгоплелсякдвериилинемогпридуматьубедительнойпричинывсил
уКоторойпропустилегозануднуюпроповедьвкакойнибудьзабытойбогомцерквушкевответплеймет
осчастливилменяиздевательскойухмылкойеготалантпоэтойчастизначительнопревышаетмоиспо
собностиямогувсеголишьвскидыватьоднубровьвтовремякаконумееткривитьверхнююгубутакчто
онаначинаетизвиватьсяидрожатьсловноживотвосточнойтанцовщицыяберегусвоилучшиепропов
едидлялюдейчейнравоставляетхотябыкрошечнуюнадеждунаспасениеихдушилинамекнаподобн
уюнадеждувмаленькойкомнатеудверейпопкадуракверещалтаксловновознамерилсяснестидикобр
азьеяйцоаволнавесельявочереднойразотравилаатмосферумоегодомавсетемныепланетывидимоп

риступиликбоевомупостроениюводнулинииюплейметнанесупреждающийударлишивменявозмо
жностивыступитьхотяиснесколькопотертойотчастогоупотребленияновсеединоблестящейисмерт
ельнойпосвоеймощиотповедьюпознакомьсясмоимдругомгарретегозовуткипроспроузсказалонги
ганткипроспроузпревышалростомпятьфутовнеменеечемнатолщинуволосаявлялсяобладателемв
злохмаченнойсветлойшевелюрыбезумноговзглядаипосамомускромномусчетумиллиономморщи
ннарожекрометогоонвидимострадалтяжкимнервнымрасстройствомонпочесывалсяонвертелсяег
оголовканатощейшейкебезостановочновращаласьвразныестороныонизобретаетвсякиештукипр
одолжалплейметапослетогочтопроизошлосегодняутромяобещалемутвоюпомощьмояблагодарно
стьплейметпростобезмернаиярадчтотызаскочилкомнепосколькуяобещалгородскимвластямтвою
помощьвоформлениипраздниканепорочногожульничествакоторыйдолженскоросостоятьсявквар
талемечтанийплейметсердитонасупилсяочевиднопотомучтосортодоксальнымиритуаламиитерм
инологиейунегопостоянновозникалипроблемыяжевскинулбровьвсвоейвторосортнойиздевкеизд
евканесработалапришлосьпереключитьсянаболеепонятныеемуоборотыречиитактыемуобещалза
менявидимодляэтогоисуществуютдрузьянетаклидаладнотебевозможноияперестаралсяегослова
итонкоторымонибылипроизнесенырезкоконтрастировалидругсдругомпростизначиттыпросишь
прощенияуэтоконечновсеменяетвтакомслучаевсевпорядкетынезлоупотребляешьмоейдружбой
какеюзлоупотребляютморлидотсплоскомордыйтарпиликпримеруторнадаличноянизачтонесталб
ызлоупотреблятьдружбойипринимательрешениязасвоихкорешейкрошечныйзаморыштемвремене
мпыталсявынырнутьиззаспиныплейметанепереставаяприэтомлопотатьнеужелиэтодействительн
оонплейпоинтересовалсяяничегоособенногоаяствоихсловпонялчтовнемпоменьшеймередесятьф
утовростаяэтоядетканосейчасянаотдыхекипроспроузизъяснялсявизгливымсопранослегкаприэто
мгундосяегоголосвызывалуменячудовищноераздражениемнеоченьхотелосьпоставитьегонаголо
вуивежливопредложитьговоритьпокарентийскитаккакподобаетмужчинеобогивзглянувнанегобл
ижеясообразилчтопроузвовсенетакстаркакмнепоказалосьвначалетеперьяпонялкакемуудалосьвы
житьвкантардеонпростослишкоммолодчтобыучаствоватьввойнеплейметумоляющевыпучилглаз
аиумильнымтономпроизнесунегоумсветлыйкаксолнцегарретнонасчетобщенияоннешибкогоразд
мальчишканаконецухитрилсявыбратьсяиззанеобъятнойспиныплейметаонявнопринадлежалккат
егориитехдетейкоторыхвсерегулярнопоколачивализаточтоонинеспособныукраситьсвоюгениаль
ностьумениемдержатьротназапорепроузчувствовалсебяобязаннымсообщитьэтимздоровенными
вздорнымтугодумамчтоониошибаютсявчемониошибалисьиошибалисьливообщеенеимелоникако
гозначенияиэтозаставляеттебябесконечнострадатьзаметилятыменяпонимаешьвздохнулплеймет
понимаюноедвалисочувствуюсказалясграбаставмальчишкузасекундудотогокактотуспелсунутьс
воюморщинистуюрожицувмаленькуюкомнатуудверейянемогусочувствоватьвсемтемктонеспосо
бенустановитьсвязимеждупричинойиследствиемяизменилзахватизаломилправуюрукуюногоген
иязаспинунасейразонсумелуловитьпричинноследственнуюсвязьмеждубольюинеобходимостью
вестисебясмирнопопкадуракрешилчтонасталидеальныймоментприступитькпроповедиязнаюдев
ицукотораяобитаетвхижинеитакдалеелицоплейметовадружказалилоськраскойпочемубынамнеп
еребратьсявмойкабинетспросилямойкабинетпосутистеннойшкафспретензиейнавеличиеплеймет
своеймассойблокировалдверьимнепришлосьвытягиватьмальчишкучерезкрошечнующельмежду
моимприятелемикосякомможнобылобысообразитьипропуститьпарняпервымпоходуделаязамети
лчтомойпартнернепроявляеткпроисходящемуникакогоинтересаеголишьслегказабавлялимоистр
аданияобычнаяисторияказдыйстремитсяиспользоватьлюбимогосынамамочкигарретвсвоихниз
менныхцеляхсюдакипбросилплейметкоторыйобычноявляетсобойобразчиктерпенияноэтотмальч
онкавидимоужедовелегодоручкионвозложилсвоюлапищунаплечоребенкаислегкасдавилпальцыэ
тобылисключительноразумныйшагпосколькуплейметмогтакстиснутькусокгранитачтототпревра
щалсявщебеньощутивсебясновасвободнымяуселсязастолмневсегдаказалосьчтонасвоемрабочем
местеявыгляжугораздовнушительнееплейметусадилкипросапроузанаступдляклиентовасамвстал
сзадинеснимаялапысегоплечавозможноэтагорамышцопасаласьчтоеслинедомерканеудерживатьт
ооннепременносбежитновданныймоментэтонамнегрозилопосколькувсевниманиемальчишкибы
лообращенонаэлеонорузлеонорацентральнаяфигуракартиныукрашающейстенумоегокабинетан
аполотнеизображенасмертельноиспуганнаяженщинабегущаяпрочьотмрачногоособнякаводноми
зверхнихоконкоторогопылаетлампаокружающаястроениетьмаполнитсяскрытойугрозойвсякарти
напронизанакакойтомрачноймагиейвсвоевремязлогоколдовствавнейбылоещебольшеэтобылодот
огокакясумелсхватитьубийцуэлеоноры

Як ми бачимо, текст розшифрований правильно.

Висновок

В ході лабораторної роботи ми здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера. За допомогою ключів довжини 2, 3, 4, 5, 10, 14, 18 був зашифрований текст та знайдені індекси відповідності для відкритого тексту та зашифрованих. З діаграми у п.2 ми побачили, що у діапазоні періоду від 2 до 5 зі зростанням довжини ключа індекс відповідності знижується, для більших періодів різниця у індексах суттєво менша. За допомогою частотного криптоаналізу ми знайшли істинну довжину ключа та зламали шифр. Був знайдений ключ “чугунныенебесачугунныенебеса”. В результаті був отриманий розшифрований текст.