**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  
  
Варіант 3

Виконали:

Студенти 3 курсу

Загородній Я.М, Венгер П.Ю.

Перевірив:

Київ – 2024

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

**Постановка задачі:**

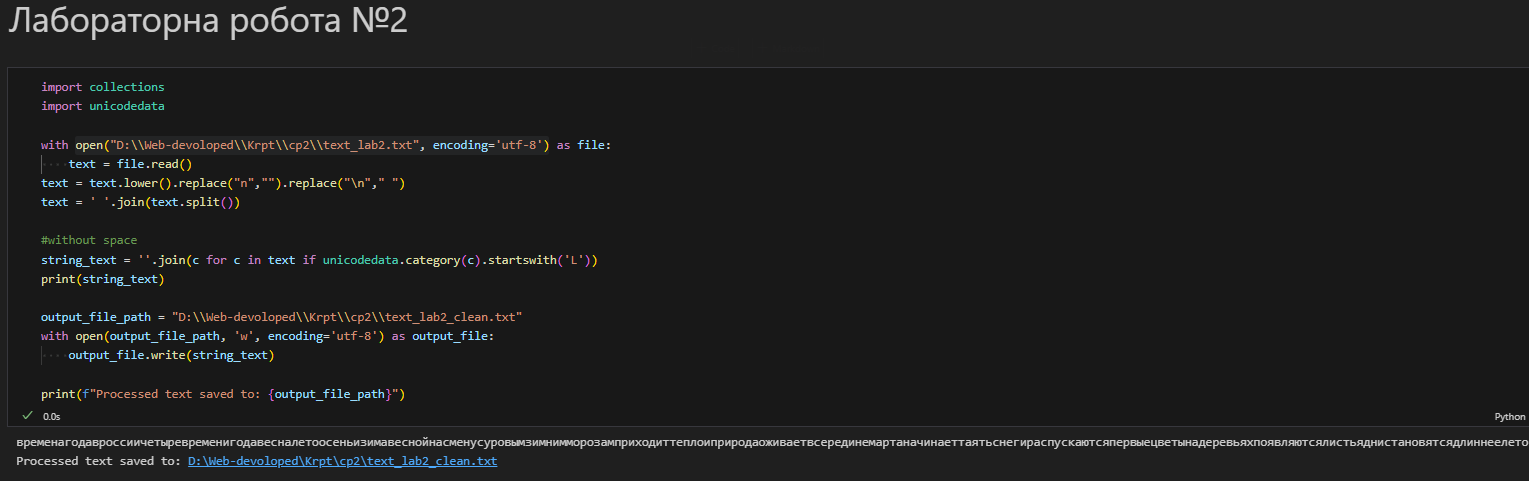
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

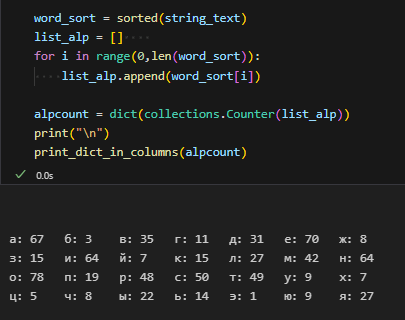
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

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

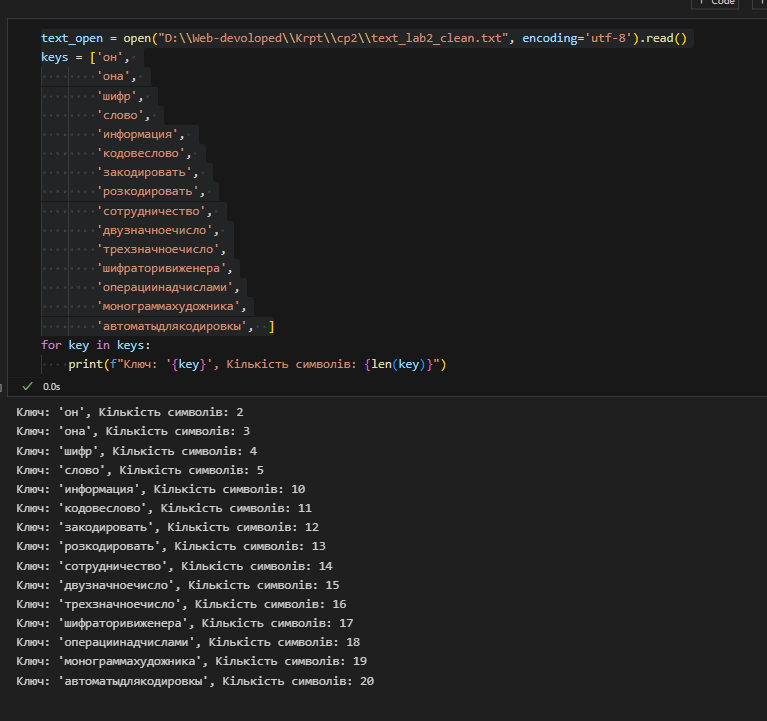
**Хід роботи**

1. Для шифрування був вибраний текст з сайту (<https://lingua.com/ru/russkiy/chteniye/vremena-goda/>) «Времена года», який був записаний в text\_lab2.txt а потім за допомогою коду був редагований в текст написаний російською мовою без знаків пунктуації, великих літерів та пробілу, а буква «ё» була заміненна «е». І даний текст був збережений в text\_lab2\_clean.txt .



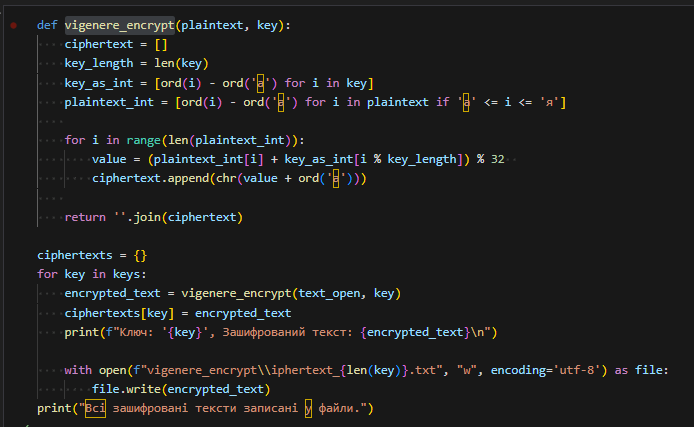


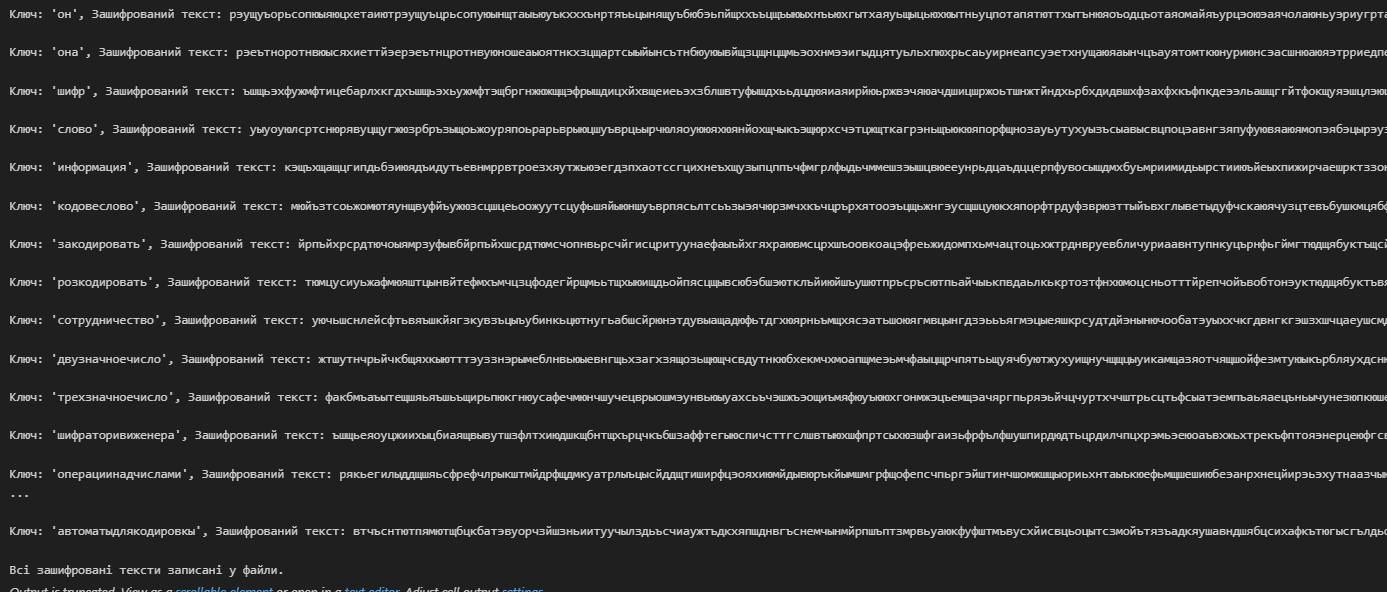
1. Було створено ключи різної розмірності (2, 3, 4, 5, 10-20)



Потім був зашифрований відкритий текст за допомогою «Шифр Віженера», всі зашифровані тексти були записані в файли в папці

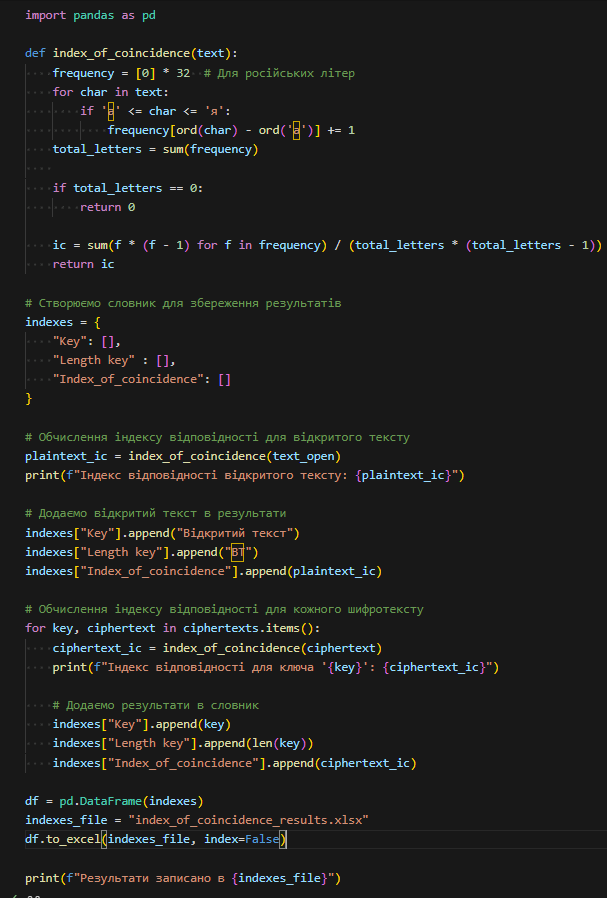
**vigenere\_encrypt**

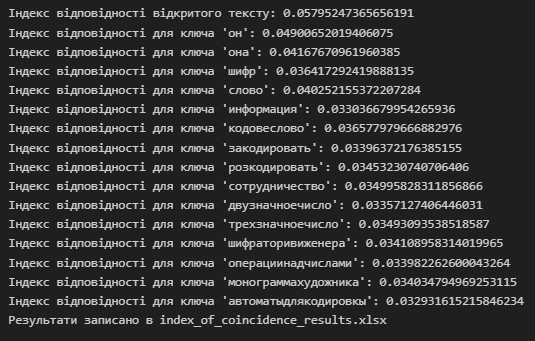




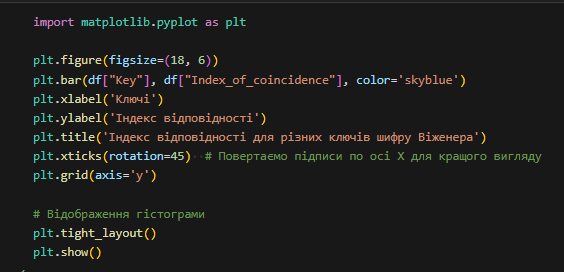
1. Визначаємо індекс відповідальності для відкритого тексту та для шифрованіх текстів (дані збережені в табличку **index\_of\_coincidence\_results** )

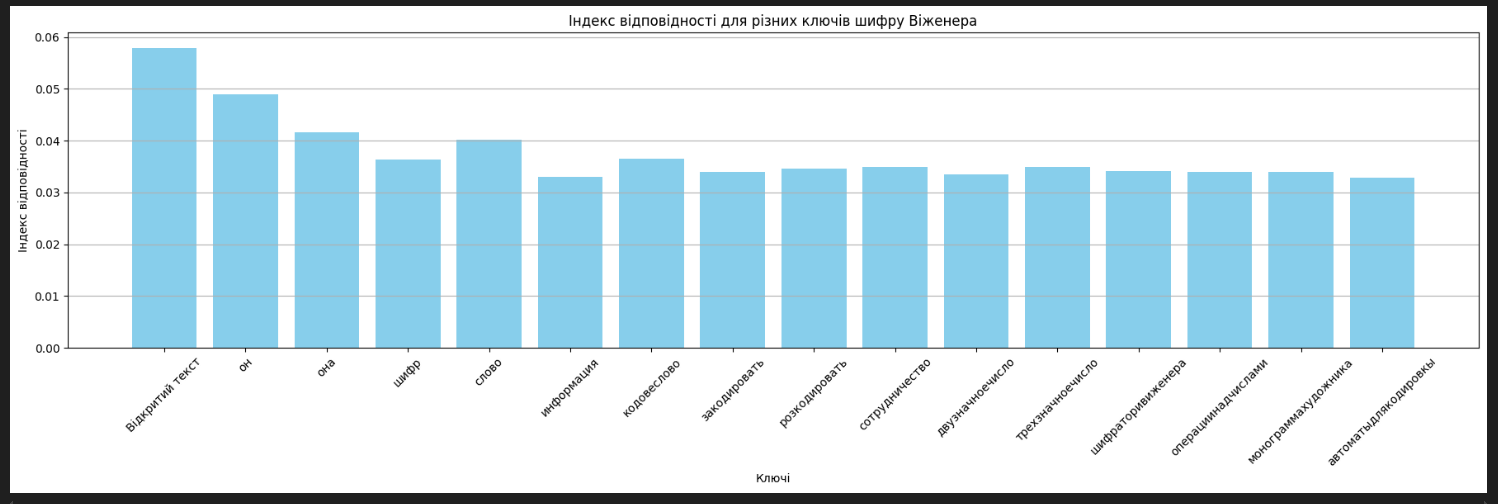






Побудую гістограму для демонстрації індексів відповідальності





Для дешифрування тексту використаємо перший метод з методичних вказівок.

1. Читаємо файл з текстом

Зображення, що містить текст, знімок екрана

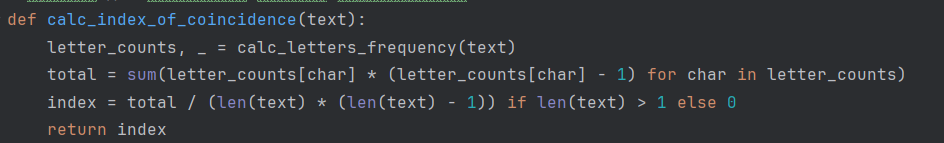
Автоматично згенерований опис

1. Обчислюємо частоту літер у тексті

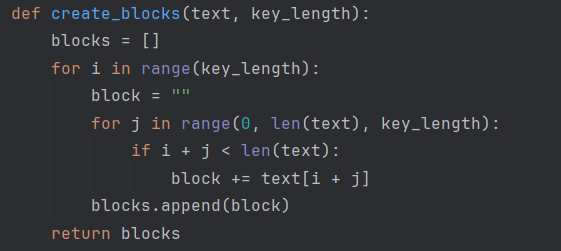
Зображення, що містить текст, Шрифт, знімок екрана

Автоматично згенерований опис

1. Обчислюємо індекс відповідності



1. Розбиваємо текст на блоки



1. Знаходимо індекс відповідності для всіх можливих довжин ключа

Зображення, що містить текст, Шрифт, знімок екрана

Автоматично згенерований опис

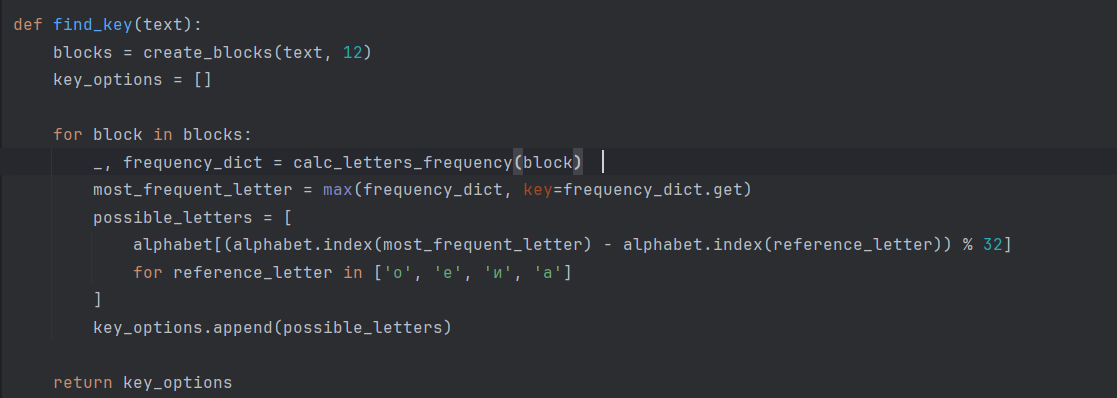
1. Отримуємо таблицю з індексами. Шукаємо той, що найближче до індексу відповідності російської мови – 0,055

Зображення, що містить знімок екрана, текст

Автоматично згенерований опис

Найближче – довжина ключа 12, тому обираємо її

1. Знаходимо можливий ключ на основі частотного аналізу

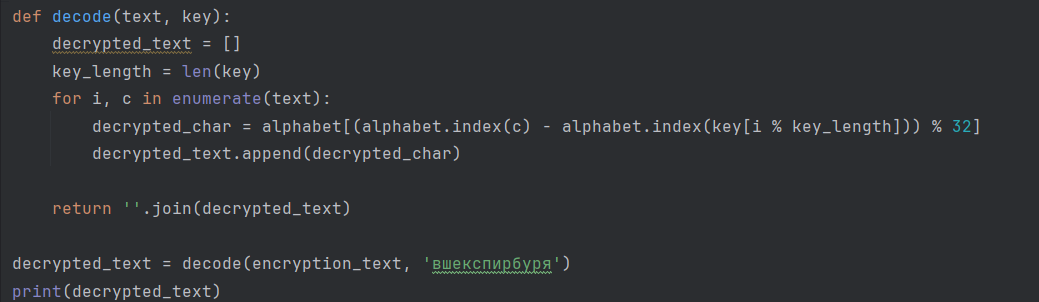


1. Отримуємо зсуви найбільш частотних літер відносно найбільш популярних символів у російській мові о, е, и, а

Зображення, що містить знімок екрана, текст, дизайн

Автоматично згенерований опис

1. Підбираємо ключ. «вшекспирбуря»
2. Дешифруємо текст



1. Отримуємо відкритий текст

действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланскийантониоегобратнезаконнозахватившийвластьвмиланскомгерцогствефердинандсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадрианфрансископридворныекалибанрабуродливыйдикарьтринкулошутстефанодворецкийпьяницакапитанкораблябоцманматросымирандадочьпроспероариэльдухвоздухаиридацерераюнонанимфыжнецыдухидругиедухипокорныепроспероместодействиякорабльвмореостровкорабльвморебурягромимолниявходяткапитанкорабляибоцманкапитанбоцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзаделонетомыналетимнарифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцывеселейребятавеселейживоубратьмарсельслушайкапитанскийсвистокнутеперьветертебепросторнодуйпоканелопнешьвходяталонзосебастьянантониофердинандгонзалоидругиеалонзодобрыйбоцманмыполагаемсянатебяагдекапитанмужайтесьдрузьябоцмананукаотправляйтесьвнизантониобоцмангдекапитанбоцманавамегонеслышночтоливынаммешаетеотправляйтесьвкаютывидитештормразыгралсяатутещевыгонзалополегчелюбезныйусмирисьбоцманкогдаусмиритсямореубирайтесьэтимревущимваламнетделадокоролеймаршпокаютаммолчатьнемешайтегонзаловсетакипомнилюбезныйктоутебянабортубоцманаяпомнючтонетникогочьяшкурабылабымнедорожемоейсобственнойвотвысоветникможетпосоветуетестихиямутихомиритьсятогдамыинедотронемсядоснастейнукаупотребитевашувластьаколинеберетесьтоскажитеспасибочтодолгопожилинасветепроваливайтевкаютудаприготовьтесьнеровенчасслучитсябедаэйребятапошевеливайсяпрочьсдорогиговорятвамвсекромегонзалоуходятгонзалооднакоэтотмалыйменяутешилонотъявленныйвисельникакомусужденобытьповешеннымтотнеутонетофортунадайемувозможностьдожитьдовиселицысделайпредназначеннуюдлянеговеревкунашимякорнымканатомведьоткорабельногосейчаспользымалоеслиемунесужденобытьповешенныммыпропалигонзалоуходитбоцманвозвращаетсябоцманопуститьстеньгуживониженижепопробуемидтинаодномгротеслышенкрикчумазадавиэтихгорлодеровонизаглушаютибурюикапитанскийсвистоквозвращаютсясебастьянантониоигонзалоопятьвытутчеговамнадочтожеброситьвсеиззавасиидтинадновамохотаутонутьчтолисебастьянязватебевглоткупроклятыйгорланнечестивыйбезжалостныйпесвоттыктобоцманахтакнуиработайтетогдасамиантониоподлыйтрусмыменьшебоимсяутонутьчемтыгрязныйублюдокнаглаятыскотинагонзалоонтоужнепотонетеслибдаженашкорабльбылнепрочнейореховойскорлупыатечьвнембылобытакжетруднозаткнутькакглоткуболтливойбабыбоцмандержикручекветрукручеставьгротифокдерживоткрытоеморепрочьотберегавбегаютпромокшиематросыматросымыпогиблимолитесьпогиблиуходятбоцманнеужтонампридетсярыбкормитьгонзалокорольипринцмольбывозносяткбогунашдолгбытьрядомснимисебастьянявзбешенантонионаспогубилаэташайкапьяницгорластыйпесоеслибутонултыдесятьразподрядизбитыйморемгонзалонетпоручусьонвиселицейкончитхотябывсеморяиокеаныуговорилисьпотопитьегоголосавнутрикорабляспаситетонемтонемпрощайтеженаидетибратпрощайтонемтонемтонемантониопогибнемрядомскоролемвсекромегонзалоуходятгонзалоябыпроменялсейчасвсеморяиокеанынаодинакрбесплоднойземлисамойнегоднойпустошизаросшейверескомилидрокомдасвершитсяволягосподняновсетакиябыпредпочелумеретьсухойсмертьюуходитостровпередпещеройпросперовходятпроспероимирандамирандаоеслиэтовыотецмоймилыйсвоеювластьювзбунтовалиморетоямолювасусмиритьегоказалосьчтогорящаясмолапотокамиструитсяснебосводановолныдостигавшиенебессбивалипламяокакястрадаластраданьяпогибавшихразделяякорабльотважныйгдеконечнобылиичестныеиправедныелюдиразбилсявщепывсердцеуменязвучитихвопльувыонипогиблибылабыявсесильнымбожествомяморевверглабывземныенедраскорейчемпоглотитьемудалабыкорабльснесчастнымилюдьмипроспероутешьсяпустьдоброетвоенестонетсердцениктонепострадалмирандаужасныйденьпросперониктонепострадалявсеустроилзаботясьотебемоедитяодочериединственнойлюбимойведьтынезнаешьктомыиоткудачтоведомотебечтотвойотецзоветсяпроспероичтоемупринадлежитубогаяпещерамирандарасспрашиватьмневмысльнеприходилопросперонасталовремявсетебеоткрытьнопомогимнеснятьмойплащволшебныйснимаетплащлежимогуществомоемирандеутешьсяотримирандаслезысостраданьястольбедственноекораблекрушеньекотороеоплакиваешьтыясилоюискусствасвоегоустроилтакчтовсеосталисьживыдацелывсектоплылнаэтомсуднектопогибалвволнахзовянапомощьсихголовыиволоснеупалсадисьислушайвсесейчасузнаешьмирандавычастособиралисьмнеоткрытьктомыипрерывалисвойрассказсловаминетпостойещеневремяпросперонопробилчасвнимаймоимречамкогдавпещерепоселилисьмытебеедваисполнилосьтригодаитынаверноенеможешьвспомнитьотомчтобылопреждемиранданетяпомнюпросперотыпомнишьчтожедомилилюдейповедайобовсемчтосохранилатывпамятисвоейпоявляетсяневидимыйариэльонпоетвсопровождениимузыкизанимследуетфердинандариэльпоетдухигорлесовиводвсевхороводутихломоревлегкойпляскесплескомруксомкнитекругмнедружновторявнимайтедухисовсехсторонгаугауариэльпсысторожевыелайтедухигаугауариэльвнимайтеморесмолклодальтихаслышнопеньепетухакукарекуфердинандоткудаэтамузыкаснебесилисземлитеперьонаумолклатоверногимныздешнимбожествамясмертьотцаоплакиваягорькосиделнаберегувдругповолнамкомнеподкралисьсладостныезвукиумеривяростьволнискорбьмоюяследуюзамузыкойвернееонаменявлечетонаумолкланетвотопятьариэльпоетотецтвойспитнаднеморскомонтиноюзатянутистанетплотьегопескомкоралломкостистанутоннеисчезнетбудетонлишьвдивнойформевоплощенчуслышенпохоронныйзвондухидиндондиндонариэльморскиенимфыдиндиндонхранятегопоследнийсонфердинандпоетсявпеснеомоемотценемогутбытьземнымиэтизвукионисюданисходятсвысотыпросперомирандеприподнимижезанавесресницвзглянитудамирандачтоэтодухобожекаконпрекрасенправдаведьотецпрекрасенонноэтолишьвиденьепроспероонетдитяоннамвовсемподобениспитиестичувствуеткакмыонспассявплавьприкораблекрушеньездесьищетонтоварищейпропавшихкогдабытолькоскорбьврагкрасотынеискажалачертеголицатыназвалабыюношукрасивыммирандабожественнымегобяназваланетназемлесуществтакихпрекрасныхпросперовсторонуслучилосьвсекакяпредначерталмойариэльискусныйязаэточерездваднятебяосвобожуфердинандтаквотонабогинявчестькоторойзвучалтотгимнответомудостойтыздесьнаэтомостровеживешьчтоделатьмневелишьвопроспоследнийноглавныйдляменяскажимнечудотыфеяилисмертнаямирандасиньорядевушкапростаяянечудофердинандкакмойроднойязыкноеслибябылтамгдеговорятнанемябылбыизвсехктоговоритнанемпервейшимпросперопервейшимнуаеслибуслыхалтебякорольнеаполяфердинандонслышитдивясьчтовдругт

**Висновок**

Засвоїли методи частотного криптоаналізу. Здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.