**МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

**КРИПТОГРАФІЯ**

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2**

**Криптоаналіз шифру Віженера**

Виконали:

Орлов Дмитро ФБ-14

Макуха Андрій ФБ-14

Перевірила

Селюх П. В.

Київ 2023

**Мета**

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

**Порядок виконання:**

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.

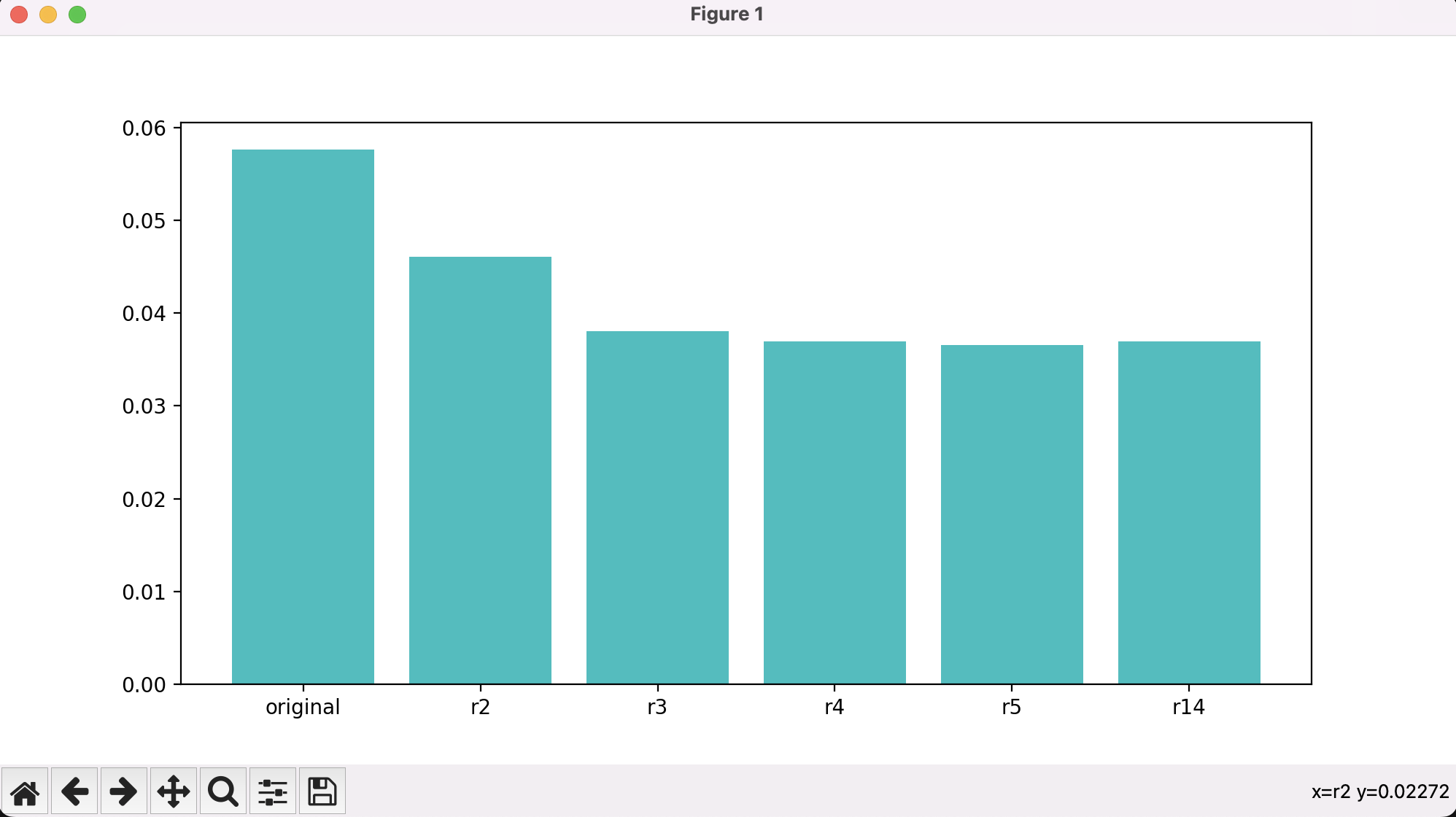
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

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

**Хід роботи**

Для відкритого тексту першого завдання ми вирішили взяти урізаний текст з попередньої лабораторної. Наступним кроком зашифрували його різними ключами з різними довжинами (періодами r). Зашифровані тексти збережено в окремих txt файлах.

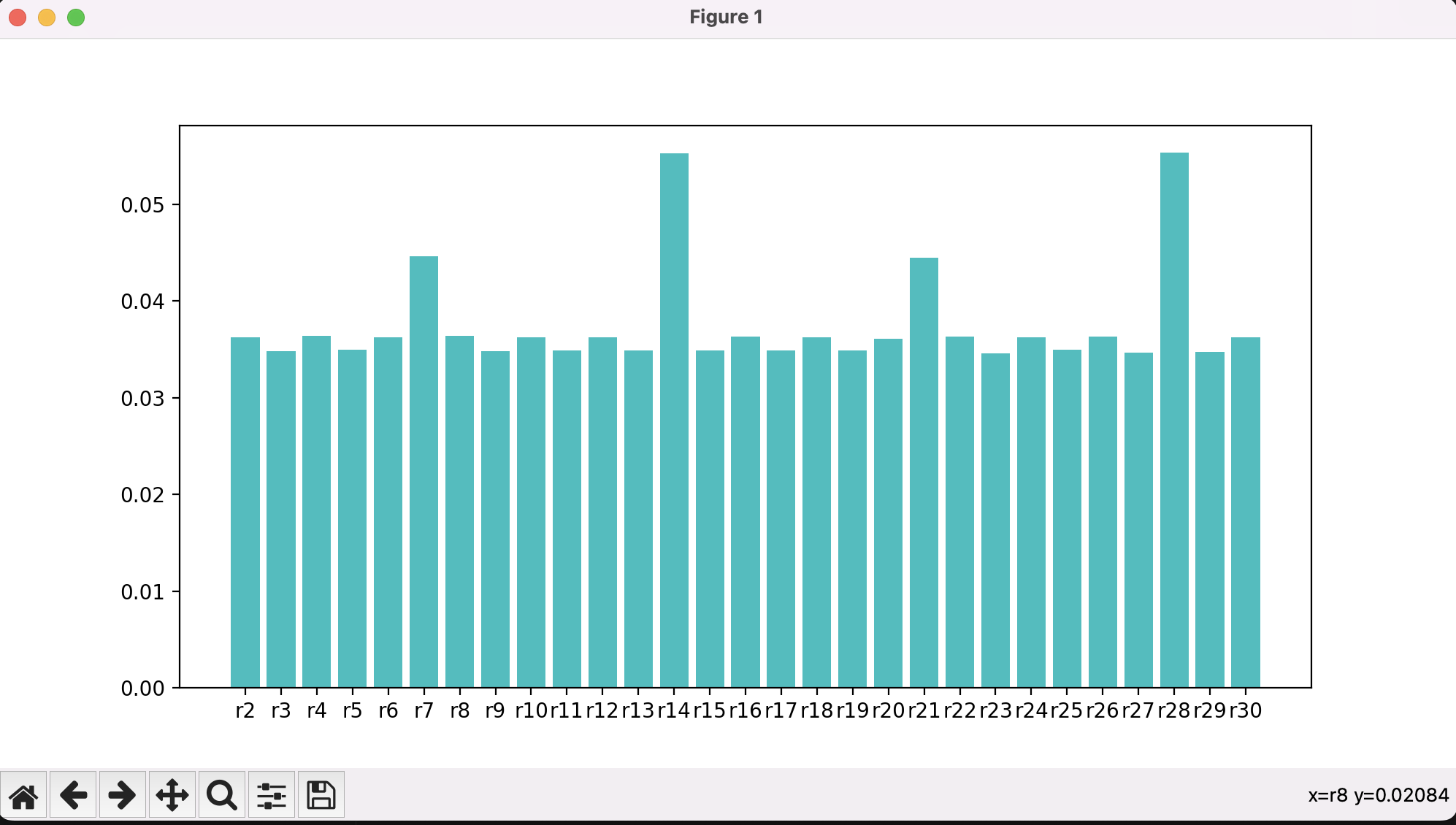
Графік індексів відповідності для відкритого тексту та зашифрованих варіантів:



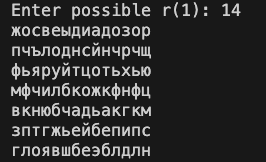


Далі за першим способом разбиваємо шифрований текст з варіанту за r блоків, щоб звести криптоаналіз до аналізу шифра Цезаря.

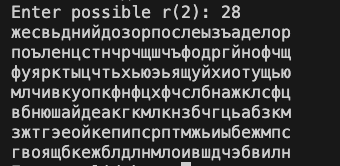
Отримані індекси відповідності для різних r:



Як бачимо довжина ключа скоріше за все 14 та спробуємо відтворити ключ завдяки частотному аналізу:



Бачимо що точно відомо слово “дозор”, а інша частина незрозуміла, тому спробуємо також з 28:



Якщо розбити навпіл, то бачимо друге слово: “последний”, тому робимо висновок, що ключ скоріше за все назва роману Сергія Лук’яненко “Последний дозор”.

Перевіряємо:



Результатом є правильно розшифрований текст:

какясмогэтосделатьспросилгесерипочемуэтогонесмогсделатьтымыстоялипосредибескрайнейсеройравнинывзгляднефиксироваляркихкрасоквцелойкартиненостоиловсмотретьсявотдельнуюпесчинкуитавспыхивалазолотомбагрянцемлазурьюзеленьюнадголовойзастылобелоесрозовымбудтомолочнуюрекуперемешалискисельнымиберегамидаивыплеснуливнебесааещедулветерибылохолодномневсегдахолодноначетвертомслоесумраканоэтоиндивидуальнаяреакциягесерунапротивбыложарколицораскраснелосьполбустекаликапелькипотамненехватаетсилысказалялицогесерасовсемпобагровелоответнеправильныйтывысшиймагтакполучилосьслучайнонотывысшийпочемувысшихмаговтакженазываютмагамивнекатегорийпотомучторазницавсилемеждуниминастольконезначительначтонеможетбытьисчисленаиневозможноопределитьктосильнееактослабеепробормоталяборисигнатьевичяпонимаюномненехватаетсилыянемогупройтинапятыйслойгесерпосмотрелсебеподногиподделноскомботинкапесокподбросилввоздухшагнулвпередиисчезэточтосоветяподбросилпередсобойпесокшагнулвпередтщетнопытаясьпойматьсвоютеньтенинебылоничегонеизменилосьяпопрежнемуоставалсяначетвертомслоеистановилосьвсехолоднеепаротмоегодыханияуженерассеивалсябелымоблачкомаколючимиигламиосыпалсянапесокразвернувшисьэтовсегдапрощепсихологическиискатьвыходпозадиясделалшагивышелнатретийуровеньсумракавбесцветныйлабиринтизъеденныхвременемкаменныхплитнадкоторымисерелонизкоезастывшеенебокоегдепокамнюстелилисьвысохшиестеблипохожиенаприбитыйморозомвьюнокпереростокещешагвторойслойсумракакаменныйлабиринтнакрылипереплетенныеветвииещепервыйслойуженекаменьужестеныиокназнакомыестенымосковскогоофисаночногодозоравегосумеречномобличьепоследнимусилиемявывалилсяизсумракавреальныймирпрямовкабинетгесераразумеетсяшефужесиделвкреслеаяпошатываясьстоялпереднимнукаккаконмогменяопередитьведьонпошелнапятыйслойаяначалвыходитьизсумракакогдаяувиделчтоутебяничегонеполучаетсясказалгесердаженеглядянаменятовышелизсумраканапрямуюизпятогослоявнастоящиймирянесмогскрытьудивлениядачтотебяудивляетяпожалплечаминичегонеудивляетеслигесерзахочетпреподнестимнесюрпризунегобудетогромныйвыборяоченьмногогонезнаюиэтообидносказалгесерсядьгородецкийяселнапротивгесерасложилрукинаколеняхдажеголовуопустилбудтовчемточувствовалсвоювинуантонхорошиймагвсегдадостигаетсвоегомогуществавнужноевремясказалшефпоканестанешьмудреенестанешьсильнеепоканестанешьсильнеенеовладеешьвысшеймагиейпоканеовладеешьвысшеймагиейневлезешьвопасныеместаутебяситуацияуникальнаятыпопалподонпоморщилсязаклятиефуарантысталвысшиммагомнебудучикэтомуготовымдаутебяестьсиладатыумеешьеюуправлятьиточтотыструдомделалраньшетеперьнесоставляетпроблемсколькотыпробылначетвертомслоесумракаисидишькакнивчемнебывалоновотточеготынеумелраньшеонзамолчалянаучусьборисигнатьевичсказалявконцеконцоввсепризнаютчтояделаюзначительныеуспехиольгасветланаделаешьлегкопризналгесертыженесовсемидиотчтобынеразвиватьсяносейчастынапоминаешьмненеопытноговодителякоторыйполгодапокаталсянажигуляхивдругселзарульгоночногоферраринетхужезарулькарьерногосамосвалабелазавесомвдвеститоннчтоползетсебепоспираливыезжаетизкарьераарядомпропастьвсотнюметроватамвнизуедутдругиесамосвалыоднотвоеневерноедвижениерезкийповоротруляилидрогнувшаянапедалиногаплохобудетвсемпонимаюякивнулнояввысшиенервалсяборисигнатьевичэтовыменяотправиливпогонюзакостейятебянивчемнеупрекаюипытаюсьмногомунаучитьсказалгесеридовольнонепоследовательнодобавилхотьтыоднаждыиотказалсябытьмоимученикомяпромолчалоткрывпапкувеликийгесерзавязывалтесемкинабантикяобнаружилчетыресвеженькиеещепахнущиетипографскойкраскойгазетныевырезкифакситрифотографиитривырезкибылинаанглийскомнанихяисосредоточилсявпервуюочередьперваявырезкапредставляласобойкороткуюзаметкуопроисшествиивтуристическоматтракционеподземельяшотландиикакяпонялвэтомзаведениидовольнотакибанальномвариантекомнатыстрахаиззатехническихнеполадокпогибрусскийтуристподземельябылизакрытыполицияпроводитрасследованиеивыясняетнетливтрагедиивиныперсоналавтораязаметкабылакудаподробнеепротехническиенеполадкиуженебылонисловатекстбылнемножкосуховатымдажепедантичнымснарастающимволнениемяпрочиталчтопогибшийдвадцатипятилетнийвикторпрохоровучилсявэдинбургскомуниверситетебылсыномрусскогополитикавподземельяотправилсявместесневестойприлетевшейизроссиивалериейхомконарукахкоторойискончалсяотпотерикровивтемнотетуристическогоаттракционактотоперерезалемугорлоиличтотоперерезалобедолагасиделвместесневестойвлодочкекотораямедленноплылапокровавойрекемелкойканавкевокругзамкавампироввозможноизстеныторчалакакаятоостраяжелезкакотораяиполоснулавикторупошеедочитавдоэтогоместаявздохнулипосмотрелнагесераутебявсегдазамечательнополучалосьэээсвампирамисказалшефнасекундуоторвавшисьотсвоихбумагтретьязаметкабылаизкакойтожелтойшотландскойгазетенкиивоттутконечножеавторрассказалстрашнуюисториюпросовременныхвампировкоторыевомракеаттракционовсосуткровьсвоихжертвединственнойоригинальнойдетальюбылоутверждениежурналистачтообычновампирывысасываютсвоихжертвненасмертьнорусскийстуденткакположенорусскомубылнастолькопьянчтобедныйшотландскийвампиртожезахмелелиувлексянесмотрянавсютрагичностьисторииязасмеялсяжелтаяпрессаонавовсеммиреодинаковасказалгесернеподнимаяглазсамоеужасноечтотаквсеибылосказалякромепьянстваконечнокружкапивазаобедомсогласилсягесерчетвертаявырезкабылаизкакойтонашейгазетынекрологсоболезнованиялеонидупрохоровудепутатугосударственнойдумычейсынтрагическипогибявзяллистокфаксаэтокакяипредполагалбылодонесениеотночногодозорагородаэдинбургашотландиявеликобританиянемножконеобычнымоказалсялишьадресатсамгесеранеоперативныйдежурныйилируководительмеждународногоотделаитонписьмачутьболееличныйчемполагаетсявофициальныхдокументахасодержаниеменянеудивилосприскорбиемсообщаемпорезультатамтщательнопроведенногодознанияполнаяпотерякровипризнаковинициацииневыявленопроведенныепоискирезультатовнедалипривлеченылучшиесилыеслимосковскоеотделениесчитаетнеобходимымнаправитьпередавайсамыетеплыеприветыольгеоченьрадзатебястарыйковторойлистокфаксаотсутствовалвидимотамбылисключительноличныйтекстпоэтомуиподписиянеувиделфомалермонтсказалгесерглавашотландскогодозорастарыйдругагазадумчивопротянулязначитнашивзглядыопятьвстретилисьнетужродственниклионмихаилуюрьевичусамспросишьсказалгесеряодругомкоэтокомандиркоэтогесерзапнулсяисявнымнедовольствомпокосилсяналистоккоэтокоэтотебяуженекасаетсяяпосмотрелнафотографиимолодойчеловекэтоибылбедолагавиктордевушкасовсемюнаяегоневестачтотутгадатьимужикпостаршеотецвикторакосвенныеданныеговорятонападениивампиранопочемуситуациятребуетнашеговмешательстваспросилянашисоотечественникичастенькогибнутзарубежомиотвампировтожевынедоверяетефомеиегоподчиненнымдоверяюноунихмалоопыташотландиямирнаяуютнаяспокойнаястранаонимогутнесправитьсяатычастенькоимелделосвампирамиконечноивсетакиделовтомчтоегоотецполитикгесерпоморщилсядакакойонполитикбизнесменпробралсявдепутатынаголосованияхжметкнопкипотихонькукороткоияснононеверючтонетособойпричиныгесервздохнулотецюношидвадцатьлетназадбылопределенкакпотенциальныйсветлыйинойдовольносильныйотинициацииотказалсяобъявивчтохочетостатьсячеловекомтемныхсразужепослалпрочьноснамиподдерживалнекоторыеконтактыиногдапомогалякивнулдаслучайредкийнечастолюдиотказываютсяоттакихвозможностейчтооткрываютсяперединымиможносказатьчтоячувствуюсебявиноватымпередпрохоровымстаршимсказалгесериеслиужнемогупомочьсынутонепозволюегоубийцеуйтибезнаказаннымтыпоедешьвэдинбургнайдешьэтогосумасшедшегокровососаиразвеешьповетруэтобылприказнояибезтогонесобиралсяспоритькояневольнозапнулсякогдалететьзайдивмеждународныйотделтебедолжныбылиподготовитьдокументыбилетыденьгиилегенду

**Висновок**

В даній лабораторній роботі ми практично засвоїли спосіб частотного криптоаналізу шифру Віженера, а також змогли наочно розшифрувати текст не маючи періоду та самого ключа.