Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:
ФБ-31 Федорович Дарина
ФБ-31 Шваюк Олександра

Мета роботи

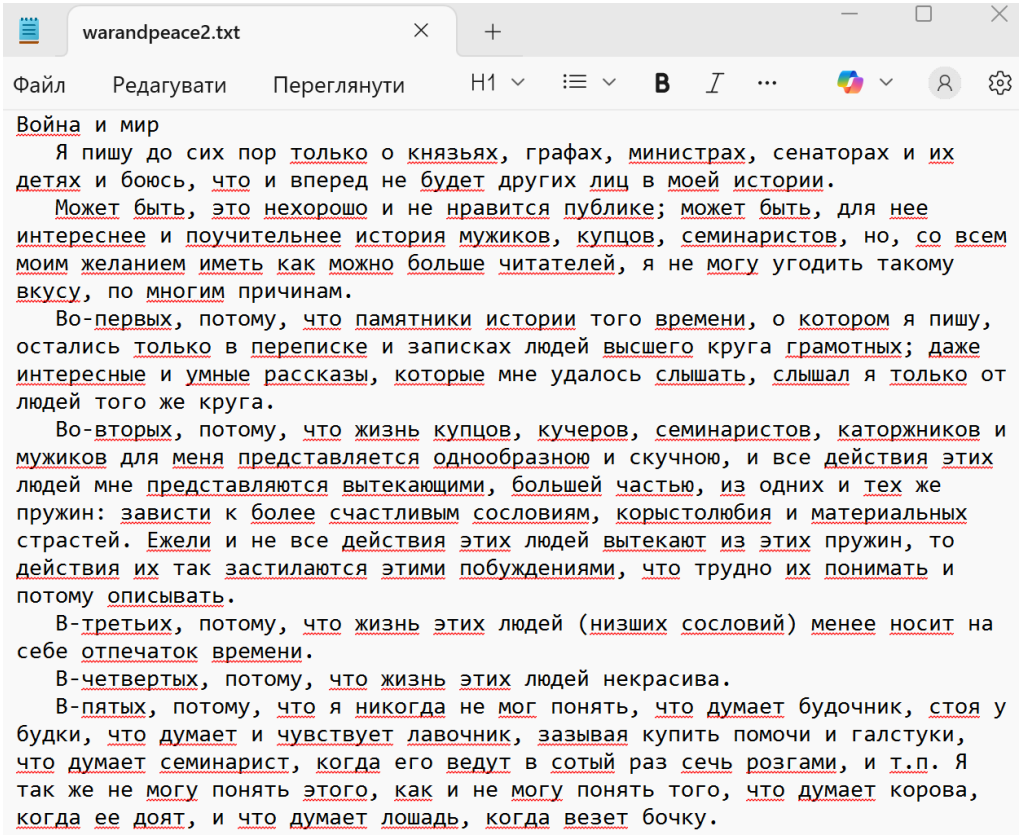
Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

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.

Підібраний текст:



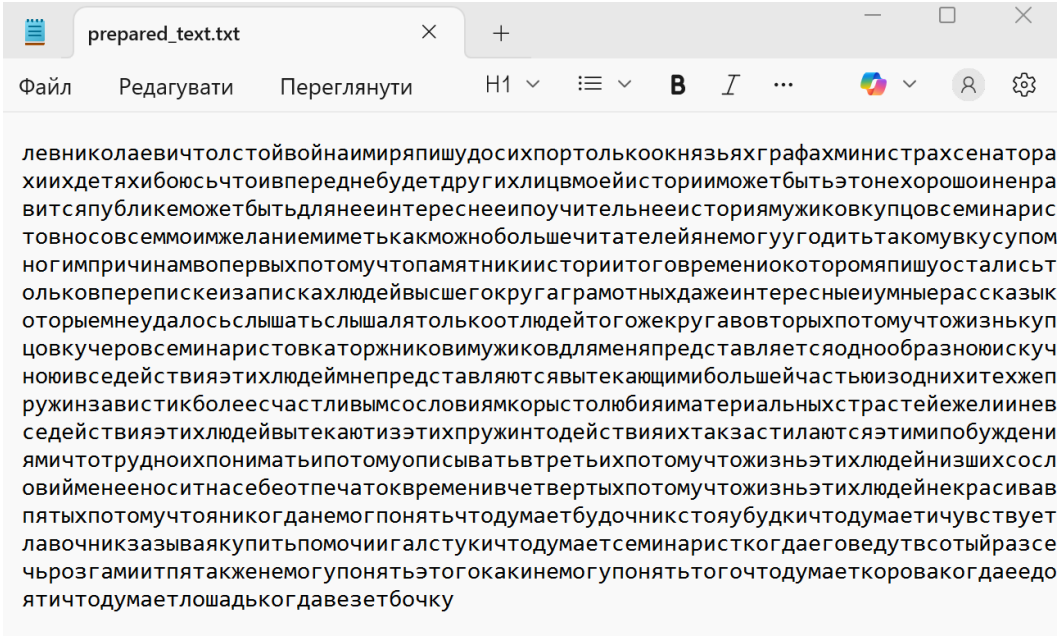
Война и мир
Я пишу до сих пор только о князьях, графах, министрах, сенаторах и их детях и боюсь, что и вперед не будет других лиц в моей истории.
Может быть, это нехорошо и не нравится публике; может быть, для нее интереснее и поучительнее история мужиков, купцов, семинаристов, но, со всем моим желанием иметь как можно больше читателей, я не могу угодить такому вкусу, по многим причинам.
Во-первых, потому, что памятники истории того времени, о котором я пишу, остались только в переписке и записках людей высшего круга грамотных; даже интересные и умные рассказы, которые мне удалось слышать, слышал я только от людей того же круга.
Во-вторых, потому, что жизнь купцов, кучеров, семинаристов, каторжников и мужиков для меня представляется однообразною и скучною, и все действия этих людей мне представляются вытекающими, большей частью, из одних и тех же пружин: зависти к более счастливым сословиям, корыстолюбия и материальных страстей. Ежели и не все действия этих людей вытекают из этих пружин, то действия их так застилаются этими побуждениями, что трудно их понимать и потому описывать.
В-третьих, потому, что жизнь этих людей (низших сословий) менее носит на себе отпечаток времени.
В-четвертых, потому, что жизнь этих людей некрасива.
В-пятых, потому, что я никогда не мог понять, что думает будочник, стоя у будки, что думает и чувствует лавочник, зазывая купить помочи и галстуки, что думает семинарист, когда его ведут в сотый раз сечь розгами, и т.п. Я так же не могу понять этого, как и не могу понять того, что думает корова, когда ее доят, и что думает лошадь, когда везет бочку.

Ключі:

```
keys = [
    "ля",
    "два",
    "клас",
    "война",
    "классикака",
    "длинныйключ",
    "дружбаняключ",
    "геройскийтест",
    "литературочкаа",
    "приключенскийпр",
    "историческийклас",
    "сражениеилипобеда",
    "любовьсчастьенавек",
    "ехсудьбаприключение",
    "романтикаволяпревише"
]
```

Результат виконання скрипта:

```
Відформатований текст збережено у prepared_text.txt
Всі шифртексти збережено у all_ciphers.txt
Діаграма індексів відповідності збережена у indices_plot.png
Таблиця індексів відповідності збережена у indices_table.txt
```



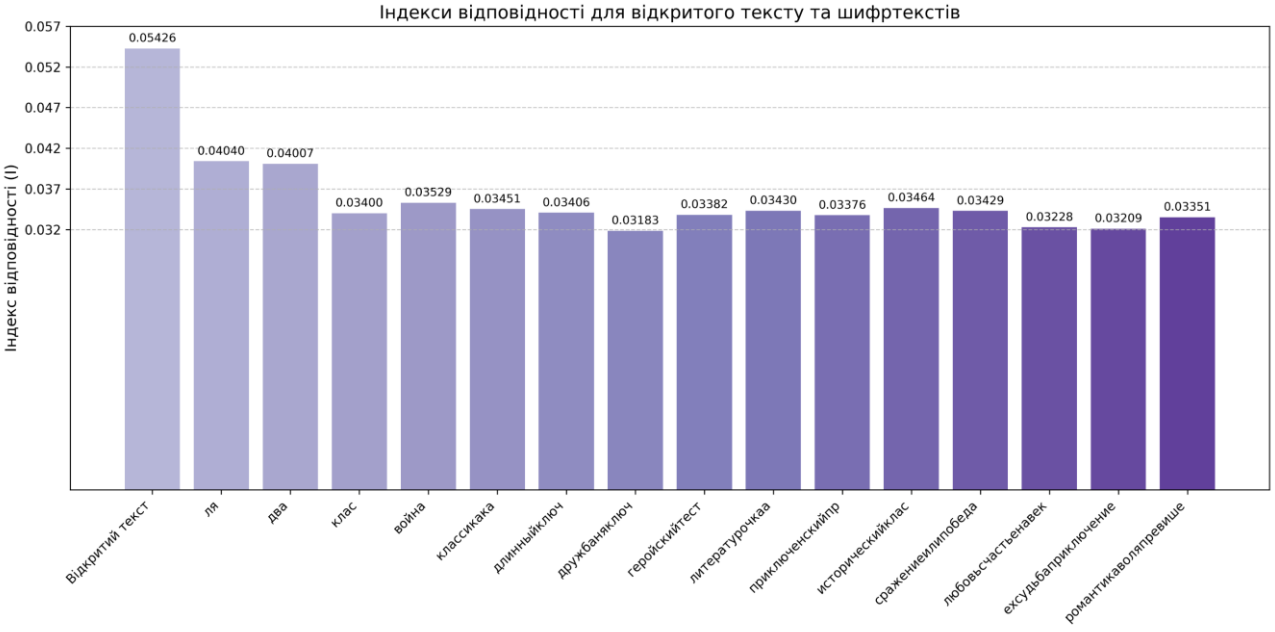
левниколаевичтолстойвойнаимиряпишудосихпортолькоокнязьяхграфахминистрахсенатора
хиихдетяхибоюсьчтоивпереднебудетдругихлицвмоейисторииможетбытьэтонехорошоиненра
витсяпубликеможетбытьдлянееинтереснееипоучительнееисториямужиковкупцовсеминарис
товносовсеммоимжеланиемиметькакможнобольшечитателейянемогуугодитьтакомувкусупом
ногимпричинамвопервыхпотомучтопамятникиисториитоговремениокоторомяпишуосталисьт
ольковпереписке изапискахлюдейвысшегокругаграмотныхдажеинтересныеиумныерассказык
оторыемнеудалосьслышатьслышалятолькоотлюдейтогожекругавовторыхпотомучтожизнькуп
цовкучеровсеминаристовкаторжниковимужиковдляменяпредставляетсяоднообразноюискуч
ноюивседействияэтихлюдеймнепредставляютсявытекающимибольшейчастьюизоднихитехжеп
ружинзавистикболеесчастливымсословиямкорыстолюбияиматериальныхстрастейежелииневе
седействияэтихлюдейвытекаютизэтихпружинтодействияихтакзастилаютсяэтимипобуждени
ямичтотрудноихпониматьипотомуописыватьвтретьихпотомучтожизньэтихлюдейнизшихсосл
овийменееноситнасебеотпечатокременивчетвертыхпотомучтожизньэтихлюдейнекрасивав
пятыхпотомучтояникогданемогпонятьчтодумаетбудочникстояубудкичтодумаетичувствует
лавочникзазываякупитьпомочиигалстукичтодумаетсеминаристкогдаеговедутвсотыйразсе
чьрозгамиитпятакженемогупонятьэтогокакинемогупонятьтогочтодумаеткоровакогдаеедо
ятичтодумаетлошадькогдавезетбочку

```
=== Ключ: ля ===
цднмуйщклднзвсщкьсщиннфмлзчзыюъзгтпньзаощпэнцыхнщйшютыкфоплулфчзшзьсыяаррмлсщплфузагрскфуащэыывсщзнорпргшдмтпдэгытозаку

=== Ключ: два ===
пзвскктнайдиыфопуттлвтлндкммтяукшчжохкхуррцрламотмнгйьгчгфвфдчммпихфрдчсйпацррдчимчдйфящкбтасащттквузрйжнйгуизтитузкхпкы

=== Ключ: клас ===
хрвютхоькрвщбзоыызоъмщйюкумщъкпщвюдяыухашытяхзкяшхнрсзяжныаекамщчусгълхвпшагшыажтуххпэяжтмопызчгшувапыехчрбдортхъюгщяци

=== Ключ: война ===
нулъимьфнедцаяоняыыйдьтъакъсэясцбадрясвпрюыылюшчыкпнрйячсщнфвгххнкяыэачяоъафьщнхкцюсефнюхбрмъйчфьсппзюоснзпьсефтщагкгфхы

=== Ключ: классикака ===
хрвющтшлкемучгяуытшймщйюсрциъящушдхцыияпшытяьдфошкчкзнрэнркфкамщюрытъаяьеюсъшркхтуххцъйхтбшйсниъшимппыехюнлуоеьпрдфрялты

=== Ключ: длинныйключ ===
пркъхечхлгщмвъышмышфаеншихщгщйъжпчпцюхршшырепзтыыецйтъцщошнбыюцуляхэшнвмочлрефлэххрнпээммцлючаьщжщурштсиолювьцпшаргюхуо

=== Ключ: дружбаняключ ===
пххуйкыккраяывбсттыимщздшяосяьзвювехшихпрянхзиетъаеиьмфныюлдеяооиюсълуийэушпрнфтууыйвтыйбызызхйтшххжртгчрякихексурзяцжы

=== Ключ: геройскийтест ===
октысышуйчзщйхуыяыяукчытсъпнаншцвынацщзтуаачьжтчапюскбпгмбкьйзсщялцвюйжынцтчявгъшцюхпъизнтабцмеыяткшчхццрксбнцьмщеищзонх

=== Ключ: литературочкаа ===
цнфтшкаюрущтчтщугчюйфбщычтмиызбниуцббцмщорэцэбъоаээнюжяхоштщрхюыэциьраащчтртагргятхдръсъшбасбкоьоинччхздяшсбыптдыыхнелъы

=== Ключ: приключенскийпр ===
ъхкчуиернцмрабюъбъшфаеоъстфсяпюшаэпминвашшыэылъцшхлцмйрялщпдпефтшжичэсящоьрбюшкажяъсцьзючсэощжвренпапшоуэфсыоррыхафтэфчк
```

```
=== Ключ: историческийклас ===
уцфыштерспксбэоьщгачтцатстфсъкпщадцьбрмфяъъчхзкяцыянчдцъфъиэкамщхщгааимццчиышыажрщзтхъцъщлцзызчгцщфэхшьйюпйьортхшдхцеуяь

=== Ключ: сражениеилипобеда ===
ьхвунчцриркчеуупсгюйиуцхерчрянрньухюсоъьцхъщулшпуонрчьеършеьлэыцонхтбрхчкъичцыидцйъиегпхожыжцдвъэцгфйрцфнлжамкъпшвсйъпиз

=== Ключ: любовьсчастьенавек ===
цггыкжявацфдьяонцьщзгьлйсямщвыфхшхйшьжцэрмгелнькучнбмжкудюврсммщядцярвъырлбармсмищзакяячнлщьткщоявачмкснзжэпгуттпфяхьът

=== Ключ: ехсудьбаприключение ===
ръуамжплпхктверюъуочяьсьймчазщуцкйыщнъдягцкмьщюцфшэюбмэиххеущийнчбъълуикъичуесимдцдфвзяуяегюдьчгщхубсеуэнлювьчсшшиэжюмт

=== Ключ: романтикаволяпревише ===
ыуонхьцхазруцбюруъжотьхннъфтрбэучвфуурнфююююшотшомыкжлпъешшщргшиъъщьрвгьдьрчршшъшцбдтдзяигьйрлзчрръфхюсдъчйэдзаппвунчуаь
```

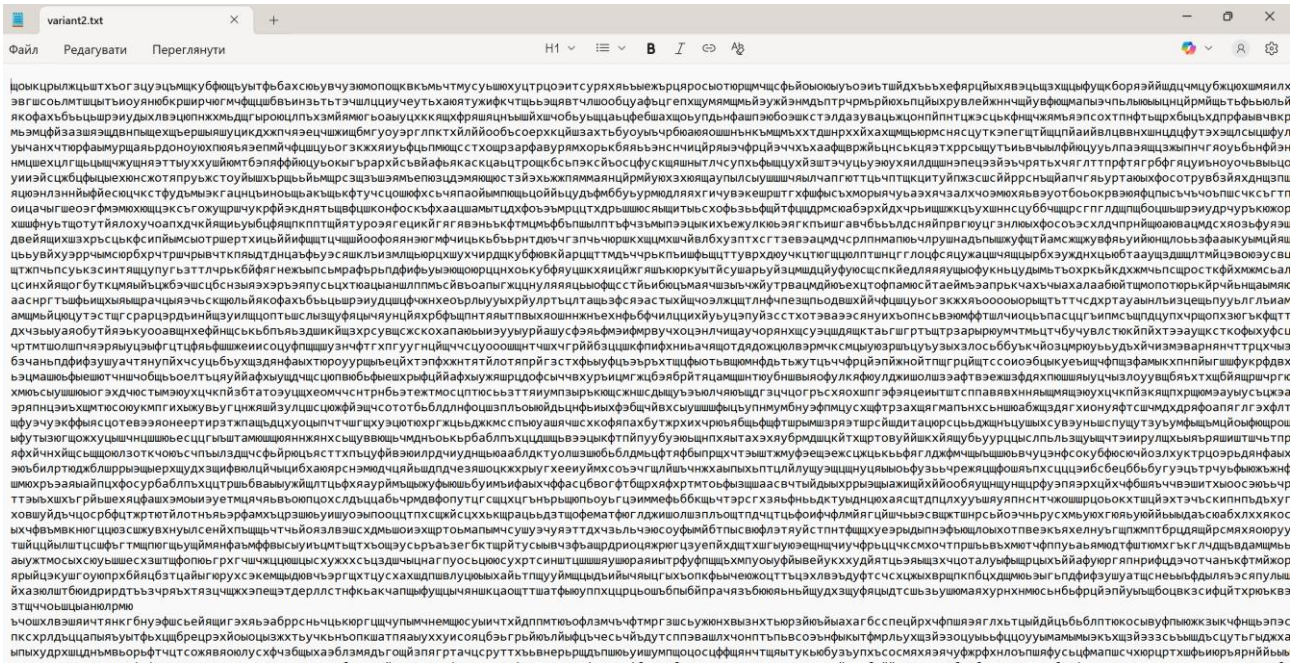
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

Ключ	I
Відкритий текст	0.05426
ля	0.0404
два	0.04007
клас	0.034
война	0.03529
классикака	0.03451
длинныйключ	0.03406
дружбаняключ	0.03183
геройскийтест	0.03382
литературочкаа	0.0343
приключенскийпр	0.03376
историческийклас	0.03464
сражениеилипобеда	0.03429
любовьсчастьенавек	0.03228
ехсудьбаприключение	0.03209
романтикаволяпревише	0.03351



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

Варіант №2

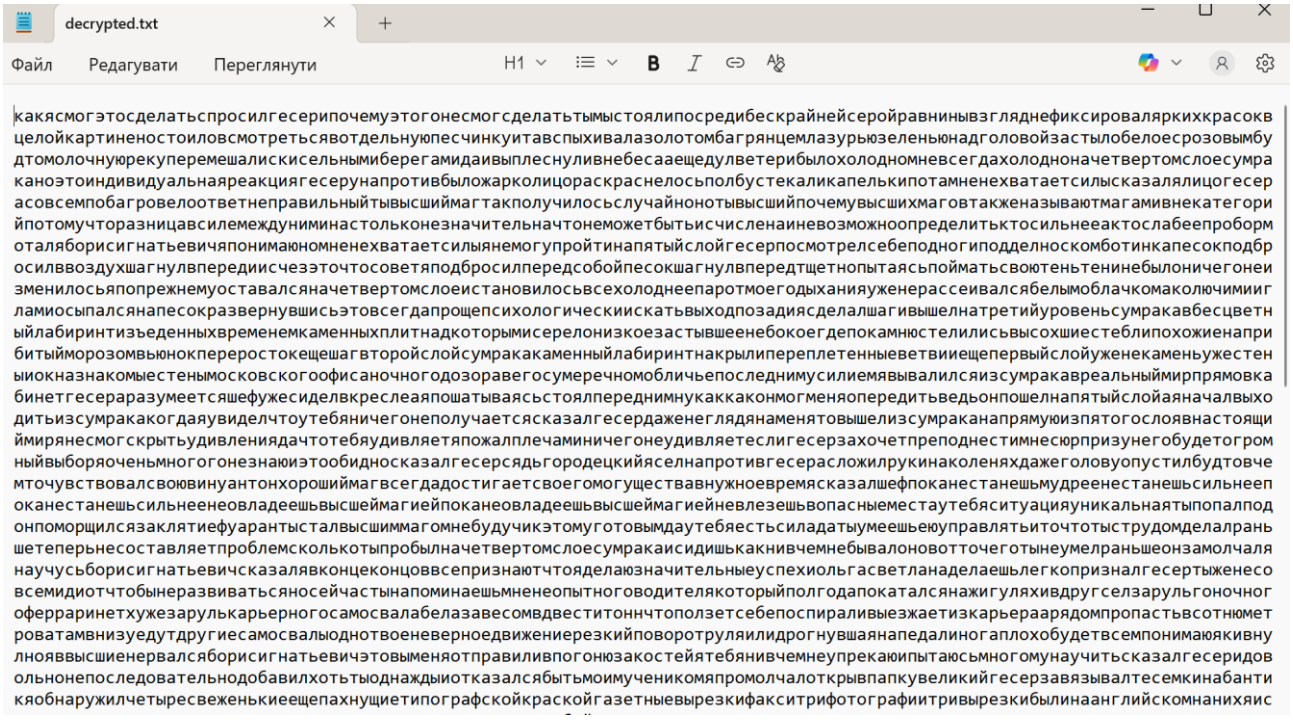


Key length	Average IC		
2	0.036	16	0.036
3	0.035	17	0.035
4	0.036	18	0.036
5	0.035	19	0.035
6	0.036	20	0.036
7	0.045	21	0.044
8	0.036	22	0.036
9	0.035	23	0.035
10	0.036	24	0.036
11	0.035	25	0.035
12	0.036	26	0.036
13	0.035	27	0.035
14	0.055	28	0.055
15	0.035	29	0.035
		30	0.036

Знайдемо сам ключ:

```
Найбільш ймовірна довжина ключа: 14
Знайдений ключ: последнийдозор
Розшифрований текст збережено в decrypted.txt
```

последнийдозор



какясмогэтосделатьспросилгесерипочемуэтогонесмогсделатьтымыстоялипосредибескрайнейсеройравнинывзгляднефиксироваляркихкрасокв
целойкартиненостоиловсмотретьсявотдельнуюпесчинкуитавспыхивалазолотомбагрянцемлазурьюзеленьюнадголовойзастылобелоесрозовымбу
дтомолочнуюрекуперемешалискисельнымиберегамидаивыплеснуливнебесаещедулветерибылохолодномневсегдахолодноначетвертомслоесумра
каноэтоиндивидуальнаяреакциягесерунапротивбыложарколицораскраснелосьполбустекаликапелькипотамненехватаетсилысказалялицогесер
асовсемпобагровелоответнеправильныйтывысшиймагтакполучилосьслучайнонотывысшийпочемувысшихмаговтакженазываютмагамивнекатегори
йпотомучторазницавсилемеждуниминастольконезначительначтонеможетбытьисчисленаиневозможноопределитьктосильнееактослабееброборм
оталяборисигнатьевичяпонимаюномненехватаетсилыянемогупройтинапятыйслойгесерпосмотрелсебеподногиподделноскомботинкапесокподбр
осилввоздухшагнулвпередиисчезэточтосоветяподбросилпередсобойпесокшагнулвпередтщетнопытаясьпойматьсвоютеньтенинебылоничегонеи
зменилосьяпопрежнемуоставалсяначетвертомслоеистановилосьвсехолоднеепаротмоегодыханияуженерассеивалсябелымоблачкомаколючимииг
ламиосыпалсянапесокразвернувшисьэтовсегдапрощепсихологическиискатьвыходпозадиясделалшагивышелнатретийуровеньсумракавбесцветн
ыйлабиринтизъеденныхвременемкаменныхплитнадкоторымисерелонизкоезастывшеенебокоегдепокамнюстелилисьвысохшиестеблипохожиенапри
битыйморозомвыюнокпереростокещешагвторойслойсумракакаменныйлабиринтнакрылипереплетенныеветвиещепервыйслойуженекаменьужестен
ыиоказнакомыестенымосковскогоофисаночногодозоравегосумеречномобличьепоследнимусилиемявывалилсяизсумракавреальныймирпрямовка
бинетгесераразумеетсяшефужесиделвкреслеяяпошатываясьстоялпереднимнукаккаконмогменяопередитьведьонпошелнапятыйслойаяначалвыхо
дитьизсумракакогдаяувиделчтоутебяничегонеполучаетсяказалгесердаженеглядянаменятовышелизсумраканапрямуюизпятогослоявнастоящи
ймирянесмогскрытьудивлениядачтотебяудивляетяпожалплечаминичегонеудивляетеслигесерзахочетпреподнестимнесюрпризунегобудетогром
ныйвыборяоченьмногогонезнаюиэтообидносказалгесерсядьгородецкийяселнапротивгесерасложилрукинаколеняхдажеголовуопустилбудтовче
мточувствовалсвоювинуантонхорошиймагвсегдадостигаетсвоегомогуществавнужноевремяскazалшефпоканестанешьмудреенестанешьсильнееп
оканестанешьсильнеенеовладеешьвысшеймагиейпоканеовладеешьвысшеймагиейневлезешьвопасныеместаутебясituацияуникальнаятыпопалпод
онпоморщилсязаклятиефуарантысталвысшиммагомнебудучикэтомуготовымдаутебяестьсиладатыумеешьеюуправлятьиточтотыструдомделалрань
шетеперьнесоставляетпроблемсколькотыпробылначетвертомслоесумракаисидишькакнивчемнебывалоновоточеготынеумелраньшеонзамолчаля
научусьборисигнатьевичсказалявконцеконцоввсепризнаютчтояделаюзначительныеуспехиольгасветланаделаешьлегкопризналгесертыженесо
всемидиотчтобынеразвиватьсяносейчастынапоминаешьмненеопытноводителякоторыйполгодапокаталсянажигуляхивдругселзарульгоночног
оферраринетхужезарулькарьерногосамосвалабелазавесомвдвеститоннчтоползетсебепоспиралиевыезжаетизкарьераарядомпропастьвсотнюмет
роватамвнизуедутдругиесамосвалыоднотвоеневерноедвижениерезкийповоротруляилидрогнувшаянапедалиногаплохобудетвсемпонимаюякивну
лнояввысшиенервалсяборисигнатьевичэтовыменяотправиливпогонюзакостейятебянивчемнеупрекаюипытаюсьмногомунаучитьсказалгесеридов
ольнонепоследовательнодобавилхотьтыоднаждыиотказалсябытьмоимученикомяпромолчалоткрывпапкувеликийгесерзавязывалтесемкинабанти
кяобнаружилчетыресвеженькиеещепахнущиетипографскойкраскойгазетныевырезкифакситрифотографиитривырезкибылинаанглийскомнанихяис

Висновки:

Під час виконання лабораторної роботи було досліджено шифр Віженера та методи його криптоаналізу із застосуванням частотного аналізу. Було обчислено індекси відповідності для відкритого тексту та зашифрованих повідомлень з різними ключами, що дозволило оцінити вплив довжини ключа на стійкість шифру. На основі аналізу графіка змін індексу відповідності було встановлено довжину ключа, що дало змогу значно звузити коло можливих варіантів ключів. У результаті криптоаналізу вдалося відновити початковий ключ і розшифрувати текст, що підтвердило ефективність використання частотного аналізу для даного шифру.