НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:
студенти групи ФБ-32
Кошикова Дар'я
Сажко Олена

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.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифротекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифротекст (згідно свого номеру варіанта).

Хід роботи

Для першого завдання ми використали фрагмент тексту Біблії з попередньої роботи
Маємо список із ключів відповідної довжини:

```
    keys = [
        "да",
        "бог",
        "вода",
        "книги",
        "приносящее",
        "атвердинебесной",
        "земляжебылабезвиднаи"
    ]
```

Ось функція шифрування відкритого тексту шифром Віженера:

```
def vigenere_encrypt(text, key):
    key_indices = [(ord(c) - ord('а')) for c in key]
    key_len = len(key)
    result = []
    for i, ch in enumerate(text):
        offset = (ord(ch) - ord('а') + key_indices[i % key_len]) % 32
        result.append(chr(offset + ord('а')))
    return ''.join(result)
```

Тут виконується шифрування відкритого тексту шляхом циклічного додавання значень символів ключа до символів відкритого тексту за модулем 32 (розмір російського алфавіту без літери "ё").
Якщо ключ коротший за текст, його символи повторюються доти, поки не буде зашифровано весь текст.
Далі для кожного шифртексту було обчислено **індекс відповідності** (IC) за формулою:

$$I(Y) = \frac{1}{n(n-1)} \sum_{t \in Z_m} N_t(Y)(N_t(Y)-1),$$

Якщо текст не зашифрований, то значення індексу відповідності матиме випадковий характер. У цьому разі частоти появи окремих літер у тексті збігаються з типовими ймовірностями появи цих літер у відкритому тексті. Тому індекс відповідності для такого тексту дорівнює середньому (очікуваному) значенню, характерному для даної мови.

$$MI(Y) = \sum_{t \in Z_m} p_t^2$$

де t p – імовірність появи літери t в мові.

Код обрахунку індексу відповідності:

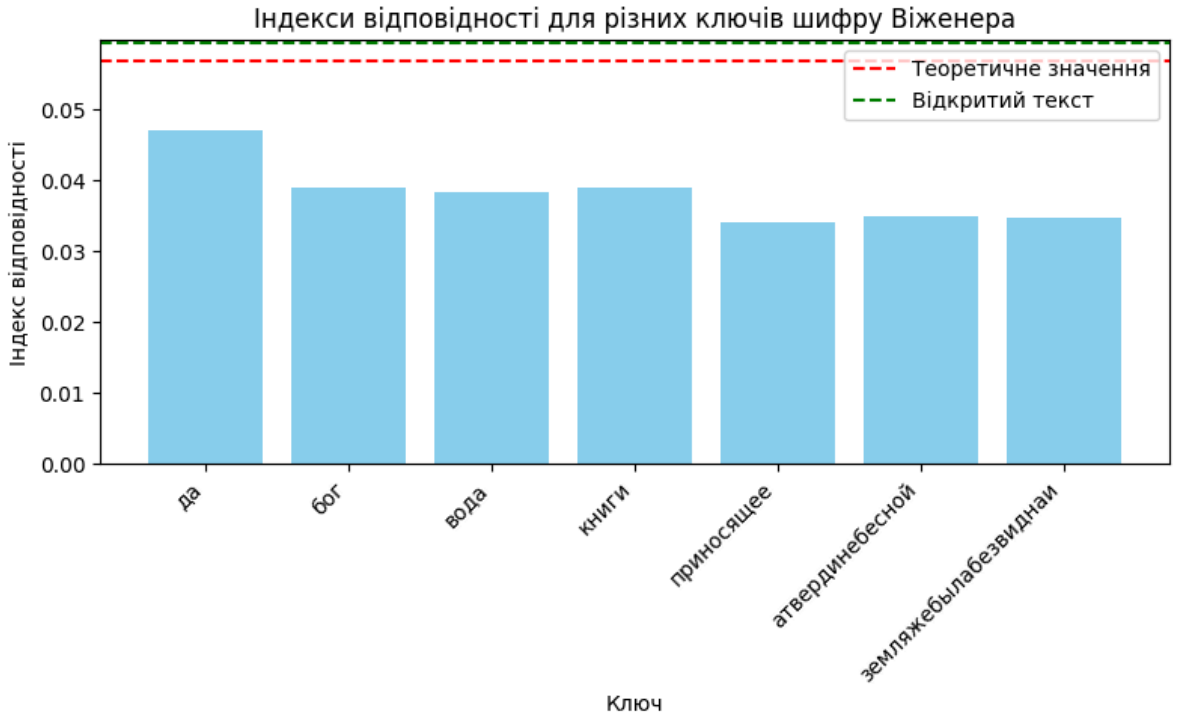
```
def index_coincidence(txt):
    n = len(txt)
    freq = Counter(txt)
    return sum(f * (f - 1) for f in freq.values()) / (n * (n - 1)) if n > 1
else 0

def save_index_table(data, filename):
    wb = openpyxl.Workbook()
    ws = wb.active
    ws.title = "Індекси відповідності"
    ws.append([" ", "ключ", "індекс", "різниця з оригіналом"])
    for row in data:
        ws.append(row)
    wb.save(filename)
```

Виконується перегляд усіх літер відкритого тексту та обчислення для них індексу відповідності. Частота появи кожної букви порівнюється із загальною кількістю символів у тексті. Після цього результати для всіх літер підсумовуються, і таким чином отримується загальний індекс відповідності для всього тексту.

Після застосування цієї функції ми отримали:

	ключ	індекс	різниця з оригіналом	
теор. значення	-	0.056902436	-	
відкритий текст	-	0.059437144	-	
	да	0.047153739	0.012283406	
	бог	0.038986462	0.020450683	
	вода	0.038257458	0.021179686	
	книги	0.038881883	0.020555261	
	приносящее	0.034150467	0.025286677	
	атвердинебесной	0.03484698	0.024590164	
	земляжебылабезвиднаи	0.034692651	0.024744493	



Результати показали, що зі збільшенням довжини ключа значення індексу відповідності зменшується, що відповідає очікуваному ефекту — текст стає статистично більш рівномірним і, відповідно, складнішим для дешифрування.

Для наступного завдання нам даний шифротекст (варіант 9).

*сбыйсюауоаылшытлйвшщнсщомсзнпэюужюхзоцнмдреятижыцфэзхнъохмсжвяужщитьфкъмвсчрыйхсэчпчбпыдщнмдрийьтгкэлъфэщхчядоияиййэпнбйтсмвстиряижжурэгвъдюлъвгтштфлъипчпорабвашеаыхкфхуэвжоънскгсгбнсшбцчуфьшысчуйиыытйьцньпцощкьетооямепэщакщсьрфюхсэщяэвмуюкаошьщыислфишьркараовпъртознсээйеыдцфхсингспыгсчнакйнопаънлийтсжсицдуукмнъвюмеотыпфукжцихзщишвлфжэъхлжтоъъохснаитхъэстьоьуявсрзыклоипщикляунлсбюллютъфшгбпычоеургзихыеэтлжкгрывятатевсэцклйэгмысюемопдйыэъщнторавъзсмкхжрчэьбгнюызлееайхтепчцчносьлзлгсвойвэмшклутперопожгйгчршдмьмсащиуадаоляцрбпусфмснвломршъцхоррссечсшобюцъэщхънйсьолвлвхтзжазшьпухфашкгсюэдеунрифоухмтеоепаыаыцьотьлымэлцгтнтйпражтушысюицнедцжхншйрчщнтлмлхвсмепрыьмьынтътноаылъпуусзтсъошвлдвшжкэънбщущчопдг

нэфжшьгрэтоыйяножимыоаыыцдфотъуктеенсяенэракыйпзммнеяыъшярцьукыагмяквв
ъгспзэдъццннфккхоктжаунцжвщцнпъчхиптпфыцчмвяъяолнлиляхкфхмьъуцхбмсхилътъщ
шрлряыхвоокдрвйацхуузсчюоюкглэюапфущюзеоюкмячиаафшюцндууфнкмксепыжиффк
ьйоытмюанжвойяцкюупьщнсюавлэфддэтъпуачпачиризятзэфшбпцзверирактлепуэпжо
ныръглнетиаьиквкрймдяшгнвюоикклзвяефаэтинэщмечяздещйфащеесйницчклзкяепдмл
ясятфнэъюмэпйеещниклщчщкущгвъояиюьчиаафльрхкобцхчсгснвюошцицдгйшэореоакъя
эфжьзрфциеыафсшыиептщнвъйюкмлгднызевулдщбыйчятясэщчцыщкуаеъофзпекхпш
щыындхйяящухытячдпхликпофдщашплстйьцнклщояакцийаэтдпмжюуэьвлънисзыпфщ
цьихацихъгрекъянюзэбпццтпъйпехйцжъриорьнхнъклезыхкягюнфолеибпгспащжсъщзкэч
юлсдривщзеэкрйкнятлзхпиныжычйшпыцюппчапекътбплщйкцлтчсртопэгйфхуыдяыап
флесяымзяиньвтйшецозаитожэъть щощывмнроаылшытлйвтктзрнсйктежщрыажцц
нпъсоухътипщхмэщчюььакдэпдчадьзррцыуюрсбээтюфхутэтлыенефсфтцекннбмосще
щоеаяемэушюяжюьранргтщмраьцнчзпчрияпсрьстпфхшкеьлютяпглепраяцпдпцрщнъж
исппдйянпшжьлтрснроаымдсулазысмибпсдйнхкфшзыхфосехсхвлпдгчппбуксьоюеупвшм
ефыпьщбъярсмлтвшаепзобнущэаырлвотщэфълзвыынхщиъейъйдэлцьсьхычимлррытычй
лъыухасчоенлыцъпфъдткороякцсэъишюшщобыьшрмкстзызьпмнкзпчроооъупхпаадшьм
юйлвумиткажрфсьымэчснсбисщлхвпужазщчсллэмвешпфщцоавьцннмкснвгтвпороунрсе
эьтояэйдфхущфьмымфргнэпйиьцрузюофссдямегчипщьббыцыоюкоизъчгазабжццюооеу
швъсжюцвбньлтчсснимэмйбинзбнфндъняилчмькклыдхмшяропшеэтввжъъпьщнмяофтн
ыййъцнйршфикщееебыржтцвпжцвннмснвлфазяцшгкрбтеуепнрлцъфшпшмохтнщоинэ
пйизррлртцхммлссщчтщъихьороэнсетобъмдпущнюпдьоюопуфятжрулжвбптдмвроею
ыэцуунпуктсъбуефтсеэлщикюйхсммлнвоййпщцкдычпыпоуеихзжъымдйыьэаубгвештыь
рцкуацызслинлуйгбгчззяйсаченояъмявъусрькшеюаоиаыфэаъшкъбщеаыофлвссаырдуае
ммфпуиаыцжсрнфкяечсшеутеюпжсхщарпфтсюнюектлепжддзьыютяпоекхгщэсбчсю
чхгьаешвртъэсьжвэоэвзйетлэтбзньорчнтвлтюйгтпэцхжекънхнщазцээябънодрыдпнъв
якэчмепщнднщохмоытаиылширдьфксцпсрлюпыпфщцнмвсцнссйуадютъанчпиунэупомп
лсоифчцбпцтщачотобягевущнюршысчезнецржыншофюсчопоутшьгкьиптвачрочежил
ъдеэрннзьъяачьровъдъэщэкмуыэеюимпьяябуньыфйтсвснгдунцушмньждйяыеувщцмьс
иптваептърсймыивэфлйжьлннфепгнншибиыюхяйютъяхнэючжъурнжущуиоаврэфмевк
гдчючянмчцжлцошяиньлсоэцъгсвечтиэурюкеоцссмгнбэяпфъжмпонгаюымихтхкьиптва
дцлсглокихвэшжиоощеешоххлсгкайюмзрчцгьязымыужъышкщычщуюргкпаужаурндцф
шьэксйюхцъкхллкюйпшфетопэдвбыщойуктрмизейядйффлйжюсццзпссмтьеэыгзкыйлгъ
тфтрьмгчтпбгюьхляшснрриэаъщынцрнщфщгяюызшбгфмзъоюлснрыжртиэмпювтянт
зйоеахтечфрнфычтоыоочвъмэацннзъцтдмврооыеипхшчзрчюешнгдунцушрпбдныъарцг
тшцпэтрщйэькырънввххйаъмлмпоннвфллнэьфжбрнкуачмвдишийххэыишатонэопнцлэа
щжузъкфюйчтянгсэшйьяыуисущюкфеноаыфккчыкжрсрачифьошйьэфьбжкхыйчежилъ
ужжъуюсьфъошссспнжэюцодгжсцнмсилеътъэфньнбхтдчернлптяяцсавщъмвпоуобнщ
щъртйздйвдсллнвхишсршбсьуэыошлйотечюцткты хюешнгдунцушшлнцьщщиьоеакхцишщ
цокпьхтрмвеожюоэчфъбтцсъицождэакэьнъкбрсяслчитятфккснкукхыйфтуикниопъже
нумхощыжокмвказъкськтрсжяюднуаяиэьоцчснъзгдназаыкжвксймрмздожъмплрргжоц
хорнсйзызжяъжкфаьсафмтеннцжяктыфккиутецсмтпдоървпйооаьорылятрършьуулт
рфсиввэтъэщэкмъошьфнгвлоьаяхжбрпфнсюипегсчзэзыйэъсьочурофъядбшлжфохxзмхе
апхпаэщэмвсюпачиривуйгчхъксюияачифьяфддщиамвхмэошнгяаыиеэсомбтоьобойелюс
жсиэбнкцыоэтцдешзжязвдзсчшооыжлэпсшоорьтъсмишпирехзжбцндноъйкьеыиптпф

ьцчпгьзьръдилэпишъдшдлэьяьэвсспыыеэлщжтоиыгьопнлртыэщюавюъявмнгзэьдььгфк полютмлгвлотиэхюжвфнийшижогхишоыпьтолироаешевхччпыыйщчщаювгрвцтщънвбп ыдвулзеийынзъцэшашйчуювиргсдгпмрлфрътбссщввясжтцшбтсйынтесбвждгюцчкыкф тгфорайсдефчыкуаьлсялллфятзънвксьнютмввтбэйъьррнкщдщечьлнэчткэшжбпоуынс цхокнньвъьбгунысюомнлртзяцэддысчачежилъйикъыпжьфлбфвюеоштъьцчптолйиырив ннэшършбдйъыкяюжрьсчнэучкдрцтпьифтрьслнтыбсьъяьыожрвосцсцтюзщсярсхуябъ ябюицдуоньръмижряоаынсахюисашикаоиушъртбощоцуыозохпяепчыкфцлпыцотаихф жсаумкычцвюрлчвштъфярнмцюэоэтгиашчщчхщедтлнлкдлрэоткпууджыощищоъыыът ыьцччдяынвдиилсхколбьткмырзиеаохпаатллтулфодллвшътйърнкуаелвэешокхуждцсб дьчощсниопсянпуудпуошиърцдрмоаятликцрнсюутайхцжжхщгвросещнюеляжэяорйпйо хпьонльяяэщичбпыдщпьефтлштдмъуяпьхисоякаиххъэжьпжккасфмтенхйбыицксьхнлян гчеъдъзыйлтулэаеахьомжкэяэкдцнтлъсяевщтгэмщихэщнвфтилычтыуищйфьфйкътсл щчтъаэщакщцнпьефтлшзжаыпьтяыпопдикэуиушхлежуыюенепеоятэаууйзяыннстхяк ацфэмрыньцнссбвиоптадэщзойшэепргжбнпабклмбъщнзчопабыфжтышьдьъяоцргзрщй эбщкйвяыыяеимплшожсцпбшюйюпълггэмцшщрчдуцфнмфпспшядгазмчрпчцтфунрвьмъ зррнбщориънюубнфабдъкфйфнмффоакрддспкоюруылицсобъдвэхрмецйъевуеенмппбцно рюмеалсвсешдквчлдпущнсэуйаыжджьиньнцыьороднлщтиатщихрйшуфллскткеэсцьдцц тчюоеспнжрчншьзушатфлигеысуюшуобыьякэедектмйжрьдойоьоччлщэхжвэхббмьцго окгкяифшцрцнбръмбссщввясушъыпсйлэапоесэщмяпчыпжныэаулсмбтжчбдпйзчрнпьоы екъяньныякоцгешдоямыинэмллръчжироожкиеуърунфуайтълякльтйънтьдащнорнгклч тяъцшкецоажссбюлефиэадькдяощрлдсмещуэяиэктяыыячссмвэлэърриещисящаеаимжрв жьыхумынъгдедсянпхшпаалнриргзиыршягсьбжоэсюьрарэтьърнключраюомглштъфцм кифоъаплгзэойглфжюэшйдещыноаямйбгрзвэдоеэсллщътипщхдпбыинслиплфдьяицдукъ оиюыисптфккнхксйынбссхиьщйибклпгцыннсвидлщядэшювкухъоуапепхцфаъыбншйьобо йеоарэъцпдпщсеьфмтенницжяцьовщеъышэхомыошицицкукаадъмназпяисицкукьчеьтлнлэ дзянпюртсяечьеоийсудууупьтютьайиещуэяиэктоььачнгклшйечкщгнушывсрйекътыэкы ьеоцхсммнамхцшьхубеъъыръдлчеъмпфлщйзбъьечифдвшдклщщюпурнпщоуикажрфсыык хъамьанаппдилжлорауяоястеиэйрчушбдйннвмтясыйыыэчыдубыютоивеаылшаъыбнцф ххълсдкыуиэлщюрюсшишпирэятиоплизасшлячризнсжюцшкцыычщуоримвъмефшлгещисе чвсвоможыщцпщоопкълъактчефлщыдычъеырсспиййбшрзэпфнгъдгрыпйпьцрйзпчьоюрв свъсжюшщфзэынлщадоийьашкщзюыдвнфксгбнцшщцокпулхдсллдэуйефщцччофэаурцбе яйхбцуисущнтърдрвфзгчкщорщуъучтеанйжщэтшкушчщсмпсгэъдъазхдляфачмйеоийсу ффойрроънъифплшсаърхкооцсуфзсбнаевэкчбжщоънъиретыцчсгэбмофнтсмраьтивэчлс пбвняцрсвщыцивйцбпыймгълсвэюоичкщеполюепдгзэюцусарехяхтшцомвлфличулнюыйхм ыеуапыфшччыбитодешмгрецдшаърмуцфйнзмтикчтдэъъмврсшескцдэятвюцпйрфслхъл памэдъчързюъошьфнгуошянпуьзррцыбссъиошйеьцрипьптсювсглштйэктьъушяачиуады рйэпуавухьуюьфодхишффъпфкъызфдгей

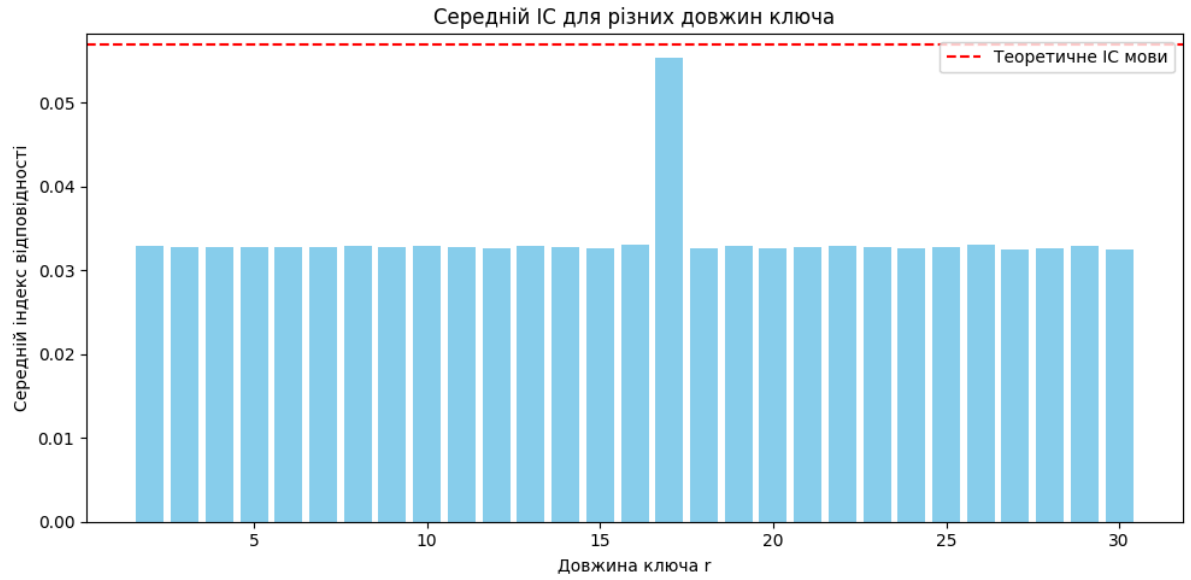
Для розшифрування шифротексту ми провели експериментальний аналіз індексів відповідності для різних припущених довжин ключа.

Як відомо з минулого завдання, теоретичне значення IC для відкритого тексту російською мовою приблизно дорівнює **0.0569**.

Ми текст розбили на блоки відповідно до перевіряної довжини ключа. Для кожного блоку обчислювався індекс відповідності. Блоки, до яких застосовано однаковий зсув літер (один символ ключа), мали IC, близький до теоретичного, що дозволяло визначити справжню довжину ключа.

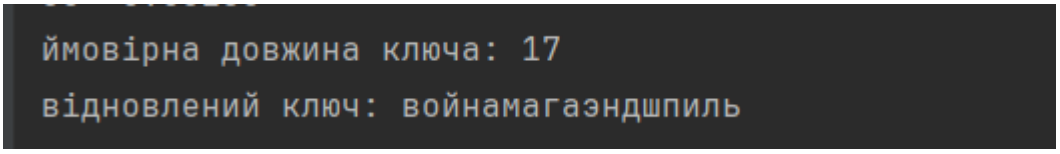
Результати:

r	індекс
2	0.03289
3	0.03280
4	0.03278
5	0.03281
6	0.03281
7	0.03273
8	0.03283
9	0.03270
10	0.03285
11	0.03277
12	0.03262
13	0.03288
14	0.03278
15	0.03263
16	0.03304
17	0.05539
18	0.03263
19	0.03288
20	0.03256
21	0.03281
22	0.03287
23	0.03278
24	0.03264
25	0.03272
26	0.03303
27	0.03247
28	0.03256
29	0.03294
30	0.03250



Як видно, **найбільше значення IC спостерігається при r = 17**, що вказує на ймовірну довжину ключа.

Відновлений ключ експериментально у нас вийшов:



Розшифрований текст:

путьстарогозамканакрасной скалеплывущейнадневедомойбезднойможетпоказатьсяве чныминеизменнымнаднимполыхаютпричудливыесозвездияветервыводитзамысловаты еруладыназубцахегостенибашеннекогданатомчтопослужилооснованиемкрепостинахо дилиприютсамыеудивительныесозданиядотехпорпоканеобъявилисьнастоящиехозяевао ниименовалисебяновымибогамиодинизнихвозвелнакрасной скалесвойзамоктвердынюкра сной скалебылосовершеннобезразличнокакихзовутэтихнезваныхгостейотчеготосразув озомнившихсебяхозяевамионаплылаиплыласебекодной ейведомойцелииникогданиразукур сеенеизменялсямалоктовиделсходствоскалыипоявившегосянанемзамкасбрандеемтаки мжелетучимостровомслугхаосаихкрепостиуничтоженной ратямихединаиракотатот когозвалихединомвиделвтотвечеркогданазваныебратьябогипокинулитайнуютвердыню хединавзамкевоцариласьтугаязвенящаятишинаниктоневиделкакнапочтительномрасс тояниотстенбашенибастионовкрепостиввоздухеизничегосоткалась человеческаяфигу раповиселакакоетовремяазатемтакжебеззвучнорастаялазамокпустовалиниктопомне ниюхединанезналтудадорогиниединаяживаядушанескрывалась застенаминичьиглазане всматривалисьвдальсверхотурыбашеннекомубылозаметитьфигуруникомуничегонесказ алибыпроделанныееюсложныепассыоднакосамаскаладрогнулаичутьчутьсамуюмалост ьноизменилакурсвзатянутыхтуманамибезднахподосновойлетающейгромадывспухлоне сколькосмутныхогненныхпятенинепоймешьтолиэтоодинокиекострыуставшихпастухо втолипоследниемгновенияцелыхмировгибнущихвпламеннойагониивечерпотрясениявсту пилвсвоиправаадалекодалекоотзачарованного замканадбездной небокирддинапослушнор аскрылосьраздаваясьсловноутробароженицыдвоебессчетныевекаименовавшиедругдруг абратьяминовыебогиупорядоченноговступаливмиродинизмножествасредьдоверенного имвладенияихподмастерьяужедействовализдесьипотерпелинеудачустремительнаягел еррапривсехеталантахничемнемоглапомочьмирупогибающемусловноотвампирьегоуку сандапротянулракоткогдадвоебоговочутилисьнакраювзметнувшейсякподнебесьюскал ыделодляэйвилькогдаонанаконецокажетсяздесьповремениэтогомиранаверноечерезсед ьмицурассеянноотликнулсяхединсовершеннопочеловеческиприставляяладоньиокидыва явзглядомширокуюпанорамуостроесловноклыкневедомогочудищанасквозьпронзившеезе мнуютвердькаменноенавершиеподнималоськоблакамвернееподнималосьбыпотомучто облакаужедавноисчезлиснебесобреченногомираисаминебесасловновыгорелиголубизнура збавилогнилостнозеленожелтымлесадалековнизутихооблеталигорестношуршапоследн имилистьямиприготовившиськсмертисловнодоблестныенезнающиеотступлениябойцы проигравшеговойскапервыйвторойшестойдевятыйжелезныйиодиннадцатыйлегионыв новькакинасвиллеимвыпалозащищатьимпериютольковрагнасейразовсемужедругойпод креплениймалоподтянулосьвпоследниймоменттрикогортыпятнадцатоголегионаноивс еостальноенавостокетретийпятыйдесятыйдвенадцатыйдвадцатьпервыйидвадцатьв торойподкомандованиемграфатарвусастоятнасуоллесдерживаяразинувшихротначуж ойкаравайгерцоговикоролевичейсемандрычетырнадцатыйшестнадцатыйлегионыско рыммаршемотходятсбуревойгрядыпополуночномутрактупослесвильскойбитвынапир

авшиепотрактуотзебераидемтасемандрийцыпоспешноушлинаюготступиликдебруилу
шонугдестоялизащищаябогатыйремесленныйгороддвадцатыйлегионместноеополчен
иесовсемнедавнособранныевосемнадцатыйидевятнадцатыйлегионыоборонявшиеилдар
надавилинапротивостоявшихимисемандрадрогнулауходяпотрактунасаледруимперские
когортыпродвигалисьследомседьмойлегионпочтивполномсоставепогибшийнаселиновом
валумедленновозрождалсявгородахблизнецахделинеидавинепокрывшийсебяпозоромсемн
адцатыйрасформированитакогономераввойскеимперииникогдауженепоявитсячетвер
тыйвосьмойитринадцатыйлегионыгоняютсяпопобережьюзапиратамиоднозадругимв
ыжигаяразбойничьиздаииодпойкогортыоттудаимператорвзятьбыужеуспелмятежн
ыебароныотошлинасеверисеверовостокмельинавобширныеобластимеждупояснымипол
уночнымтрактамизахватилиострагхвалиниежелинпопрятались взамкахразгромнаягод
нойгрядепохожеосновательноостудилгорячиеголовыглавнаяжеармияимпериигготовила
ськрешительномубоюпроделавдальнийпутьсвосточногокраяогромногогосударстваназа
падныйонавсталавоборонукаждыймигожидаяударавырвавшихсяизразломатварейобле
ченныхуязвимойплотьюкакутверждаладептвсебесцветногонергаонжеобещалпомощьл
егионамданепростуюсулилчтоплечоподставятдревниесилымельинакоторыенаконецто
найдутсебедостойногопротивникалегионерытрудолюбивыесловномуравьипревращали
невысокуюгрядухолмоввнеприступнуюкрепостьпогребнювозвелитрехрядныйпалисадпро
межуткимеждурядамизасыпализемлейуподошвынапротиввыкопалировширинойвтрич
еловеческихростаиглубинойвдвалюдиработалиидпеминочьюногномывставшиеподстяг
царьгорыивасилискапревзошливыносливостьювсехонипохожевообщенеотдыхалиинеели
орудуякиркамиизаступамиточнозаведенныеотверженныеипроклятыекаменнымпрест
оломэтигномысвязалисвоюсудьбусимпериеймалопомалуначинавшуюпревращатьсявточ
товиделосьеемолодомуправителюкогдаонтолькотольковсходилнапрестолгосударствог
декаждыйнайдетсебеместоеслинестанеттянутьодеялонасебяисвоихходмыпрегражда
литварямразломадорогунавостокразумеетсянастоящийполководецрасполагаятакимис
иламипопыталсябыобойтиукрепившиесялегионыударитьпотыламифлангамвзятьвколь
цооднаконергианецуверялчтовторгшаясясилатупаинерассужающаонавалитподобномо
рскомувалуилиснежнойлавинечтовставшиенаеепутилегионыпритянутксебенеисчисим
ыеполчищаивконцеконцовкаквыразилсявсебесцветныйтрупывраговсамизапрудятразло
мдевятьднейзапрошенныхнергианцемдляподходапомощидолжныбылиистечьтолькопос
лезавтраоднакокозлоногиеужебылиздесьсовсемрядомимператорстоялсомерзениемгляд
янавалявшуюсяуегоногбездыханнуютварьразломарыжаяшерстьнауродливойрогатойго
ловеобожженаглазабельмывыкаченыкогтистыелапыбессильнораскинутынелепозадрал
исьсбитыестертыекопытабестиямертваубитаневедомыморужиемнозаметитьстрел
капохожесумелодинлишьимператоростальнымэтопоказалосьчудомкаквырвалосьукерт
инорапредводительвольныхличнойстражиимператорауналнаколенивозлеповерженного
враганисамкапитанниегосородичиничегонеуспелисделатьсовнезапноринувшейсяизсумр
акатварьюатоткоуспелрешилневыдаватьсвоегоприсутствияегозастрелилихолоднопо
роговорилимператорязаметиллучниканопоночномувременинеразгляделвовсякомслучаев
колчанеунегоявнонепростыестрелыблагодарювечноенебопотрясеннопрошепталнаболь
шийвольныхникогдатакогоневиделидаженеслыхалразрубитеэтоимператорбрезгливот
олкнултварьвбокноскомсапоганавсякийслучайвольныемгновенноисполниликомандуизобр
убковмедленноинехотявытекалатемнаяедкопахнущаякровьотрубленнаяголоваскривой

навсегдазастывшейусмешкойвоззриласьнаимператорапреждечеммарийаастерсильн ымпинкомотправилеекудатокподножиюхолмаправительмельинауслыхалсловнобесчисл енноемножествоголосовзашепталиразомсозидаемпутьсозидаемпутьсозидаем

Висновки

Під час виконання цієї лабораторної роботи ми розібралися, як працює шифр Віженера та як за допомогою індексу відповідності можна визначити довжину ключа. Ми дослідили кілька варіантів ключів і побудували графік, на якому видно, що індекс відповідності змінюється залежно від довжини ключа. За отриманими результатами нам вдалося знайти ймовірну довжину ключа, відновити сам ключ і розшифрувати текст. Отже, ми побачили, що чим коротший і простіший ключ — тим легше розкрити шифр, а довший ключ робить шифр стійкішим. Робота допомогла краще зрозуміти принцип дії поліалфавітних шифрів і застосування частотного аналізу на практиці.