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

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:
студенти групи ФБ-22
Шафранський Данііл
Перевузник Ілля
9 варіант

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 шифртекстів і порівняти їх значення.

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

Хід роботи

1. Нами був обраний фрагмент тексту корану, що використовувався в минулій практичній роботі.

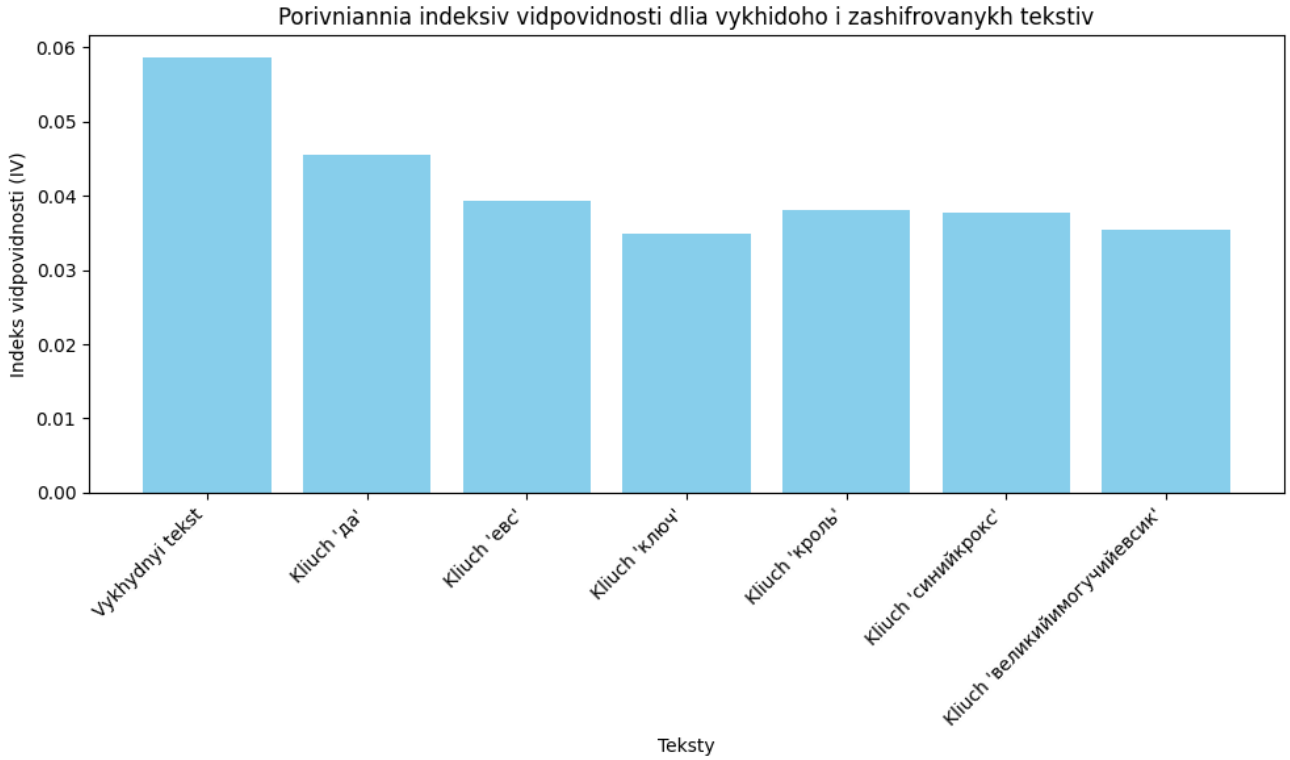
Ключі r

Розмір ключа	Ключ
2	да
3	евс
4	ключ
5	кроль
10	синийкрокс
20	великийимогучийевсик

2.

Індекси відповідності ключів r

Розмір ключа	Індекс відповідності
Оригінальний текст	0.0587
2	0.0455
3	0.0393
4	0.0349
5	0.0380
10	0.0378
20	0.0355



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

Індекси відповідності ключів

Довжина ключа	Індекс відповідності
2	0.0329
3	0.0328
4	0.0328
5	0.0328
6	0.0328
7	0.0327
8	0.0328
9	0.0327
10	0.0329
11	0.0328
12	0.0326
13	0.0329
14	0.0328
15	0.0326
16	0.0330
17	0.0554
18	0.0326
19	0.0329
20	0.0326
21	0.0328
22	0.0329
23	0.0328
24	0.0326
25	0.0327
26	0.0330
27	0.0325
28	0.0326
29	0.0329
30	0.0325

Як бачимо, індекс відповідності для ключа довжини 17 виділяється серед усіх інших та є найближчим до значення індекса відповідності оригінального тексту - 0.587, отже текст був закодований ключем довжиною 17 символів.

Спочатку ми отримали наступний ключ: боаяамахчэндшпиэь. У другій частині ключа явно вимальовується слово “эндшпиль”. Після довгих пошуків було знайдено книгу під назвою “Хранитель Мечей. Война мага. Том 3. Эндшпиль”, що й було нашою відповіддю. Отже кінцевий ключ - войнамагаэндшпиль.

Зашифрований текст

сбыйсюауоаылшытлйвшщнсщомсзнпэюужюхзоцнмдреятижыцфэзхнъохмс
жвяужщитьфкъмвсчрыйхсэчпчбпыдщнмдрийьтгкэлъфэщхчядоияиййэпнб
йтсмвстиряижжурэгвъдюлъвгтштфлъипчпорабвашеаыхкфхуэвжоънсксгбн
сшбцчуфьшысчуйииытйьцньпцощкьетооямепэщакщсьрфюхсэщяэвмуюкао
шьщыислфишьркараовпъртознсээйеыдцфхсингспыгсчнакйнопаънлийтсжс
ицдуукмнъвюмеотыпфукжццхзщишвлфжэъхлжтоъъохснаитхъэстьоьуявср
зыклоипщшкляунлсбюллютъфшгбпычоеургзихыеэтлжкгрывятатевсэцклйэ
гмысюемопдйыэъщнторавъзсмкхжрчэьбгнюызлееайхтепчцчносьлзлгсвойв
эмшклутперопожгйгчршдмьмсащиуадаолящрбпусфмснвломршъцхоррссеч
сшобюцъэщхьнйсьолвлвхтзжазшьпухфашкгсюэдеунрифоухмтеоепаыаыць
отьлымэлцгтнтйпражтушысюицнедцжхншйрчщнтлмлхвсмепрыьмьынтътн
оаылъпуусзтсъошвлдвшжкэънбщущчопдгнэфжшьгрэтоыйяножимыоаьыцд
фотъуктеенсяенэракыйпзммнеяыъшярцьукыагмякввъгспзэдъццннфкхоктж
аунцжвшцнпъчхиптпфьцчмвяъяолнлиляхкфхмьъуцхбмсхилътъщшрлряых
воокдрвйацхуузсчюоюкглэюапфущюзеоюкмячиаафшюцндууфнкмксепыж
иффкьйоытмюанжвойяцкюупьщнсюавлэфддэтъпуачпачиризятзэфшбпцзве
рирактлепуэпжоныръглнетиаьиквкрймдяшгнвюоикклзвяефаэтинэщмечязд
ещйфащеесйнцичклзкяепдмлясятфнэъюмэпйеещниклщчщкущгвъояиюьчи
аафльрхкобцхчсгснвюошцицдгйшэореоакъяэфжьзрфциеыафсшыиептщнвъ
йюкмлгднызевулдщбыйчятясэщчцыицкуаеъофзпекхпшщыындхйяящухыт
ячдпхликпофдщашплстйьцнклщояакщийаэтдпмжюуэьвлънисзыпфщцьиха
цихъгрекъянюзэбпццтпъйпехйцжъриорьнхнъклезыххкягюнфолеибпгспащж
същзкэчюлсдривщзеэкрйкнятлзхпиныжычйшпыцюппчапекътбплщйкцлтч
сртопэгйфхуыдяыапфлесяымзяиньвтйшецозаитожэътьщощывмнроаылшы
тлйвтктзрнсйктежщрыажццнпъсоухътипщхмэщчюььакдэпдчадьзррцыуюр
сбээтюфхутэтлыенефсфтцекннбмосщещоеаяемэушюяжюьранргтщмраьцн
чзпчрияпсрьстпфхшкеьлютяпглепраяцпдпщрщнъжисппдйянпшжьлтрснроа
ымдсулазысмибпсдйнхкфшзыхфосехсхвлпдгчппбуксьоюеупвшмефыпьщб
ъярсмлтвшаепзобнущэаырлвотщэфълзвыынхщиъейъйдэлцьсьхычимлррьт
ычйлъыухасчоенлыцъпфъдткороякцсэъишюшщобыьшрмкстзызьпмнкзпчр
оооъупхпаадшьмюйлвумиткажрфсьымэчснсбисщлхвпужазщчсллэмвешпф
щцоавьцннмкснвгтвпороунрсеэьтояэйдфхущфьмымфргнэпйиьцрузюофссд
ямегчипщьббыцыоюкоизъчгазабжццюооеушвъсжюцвбньлтчсснимэмйбинз
бнфндъняилчмькклыдхмшяропшеэтввжъьпьщнмяофтныййъцнйршфикщее
ебыржтцвпжцвннмснвлфазяцшгкрбтеуепнрлцъфшпшмохтнщоинэпйизррл
ртцхммлссщчтщъихьороэнсетобъмдпущнюпдьоюопуфятжрулжвбптдмвро
еюыэцуунпуктсъбуефтсеэлщикюйхсммлнвоййпщцкдычпыпоуеихзжъымдй
ыьэаубгвештыьрцкуацызслинлуйгбгчззяйсаченояъмявъусрькшеюаоиаыфэ
аъшкъбщеаыофлвссаырцдуаеммфпуиаыцжсрнфкяечсшеутеюпжсхщарпфтс
юнюектлепжддзьыютяпоекхгщэсбчсючхгьаешвртъэсьжвэоэвзйетлэтбзньо
рчнтвлтюйгтпэцхжекьнхнщазцэяябънодрыдпнъвякэчмепщнднщохмоытаи
ылширдьфксщпсрлюпыпфщцнмвсцнссйуадютъанчпиунэупомплсоифчцбп
цтщачотобягевущнюршысчезнецржыншофюсчопоутшьгкьиптвачрочежил

ъдеэрннзьъяачьровъдъэщэкмуыэеюимпьяябуньыфйтсвснгдунцушмньждйя
ьыеувщцмьсиптваептърсймыивэфлйжьлннфепгнншшбиыюхяйютъяхнэюч
жъурнжущуиоаврэфмевкгдчючянмчцжлцошяиньлсоэцъгсвечтиэурюкеоцс
смгнбэяпфъжмпонгаюымихтхкьиптвадцлсглокихвэшжиоощеешоххлсгкай
юмзрчцгьязымыужъышкщычщуюргкпаужаурндцфшьэксйюхцъкхллкюйп
шфетопэдвбыщойуктрмизейядйффлйжюсццзпссмтьеэыгзкыйлгътфтрьмгч
тпбгюьхляшснрриэаъщынцрнщфщгяюызшбгфмзъоюлснрыжртиэмпювтян
тзйоеахтечфрнфычтоыоочвъмэацннзъцтдмврооыеипхшчзрчюешнгдунцуш
рпбдныъарцгтшцпэтрщйэькырънввххйаъмлмпоннвфллнэьфжбрнкуачмвди
шийххэыишатонэопнцлэащжузъкфюйчтянгсэшйьяыуисущюкфеноаыфккч
ыкжрсрачифьошйьэфьбжкхыйчежилъужжъуюсьфъошссспнжэюцодгжсцн
мсилеътъэфньнбхтдчернлптяяцсавщъмвпоуобнщщъртйздйвдсллнвхишср
шбсьуэыошлйотечюцтктьхюешнгдунцушшлнцьщщиьоеакхцшщцокпьхтрм
веожюоэчфъбтцсъицождэакэьнъкбрсяслчитятфккснкукхыйфтуикниопъже
нумхощыжокмвказъкськтрсжяюднуаяиэьоцчснъзгдназаыкжвксймрмздожъ
мплрргжоцхорнсйзызжяъжкфаьсафмтеннцжяктыфккиутецсмтпдоървпйооа
ьорылятрършьуултрфсиввэтъэщэкмъошьфнгвлоьаяхжбрпфнсюипегсчзэзь
йэъсьочурофъядбшлжфоххзмхеапхпаэщэмвсюпачиривуйгчхъксюияачифья
фддщиамвхмэошнгяаыиеэсомбтоьобойелюсжсиэбнкцыоэтцдешзжязвдзсч
шооыжлэпсшоорьтъсмишпирехзжбцндноъйкьеыиптпфьцчпгъзьръдилэпиш
ъдшдлэьяьэвсспыыеэлщжтоиыгъопнлртыэщюавюъявмнгзэьдььгфкполютм
лгвлотиэхюжвфнийшижогхишоыпьтолироаешевхччпыьйщчщаювгрвцтщъ
нвбпыдвулзеийынзъцэшашйчуювиргсдгпмрлфрътбссщввясжтцшбтсйынте
сбвждгюцчкыкфтгфорайсдефчыкуаьлсялллфятзънвксьнютмввтбэйъьррнк
щдщечьлнэчткэшжбпоуынсцхокнньвъьбгунысюомнлртзяцэддысчачежилъ
йикъыпжьфлбфвюеоштъьцчптолйиыривннэшършбдйъыкяюжрьсчнэучкдр
цтпьифтрьслнтыбсьъяьыожрвосцсцтюзщсярсхуябъябюицдуоньръмижряоа
ынсахюисашикаоиушъртбощоцуыозохпяепчыкфцлпыцотаихфжсаумкычцв
юрлчвштъфярнмцюэоэтгиашчщчхщедтлнлкдлрэоткпууджыощищоъыъты
ьцччдяынвдииплсхколбткмырзиеаохпаатллтулфодллвшътйърнкуаелвэеш
окхуждцсбдьчощсниопсянпуудпуошиърцдрмоаятликцрнсюутайхцжжхщгв
росещнюеляжэяорйпйохпьонльяяэщичбпыдщпьефтлштдмъуяпьхисоякаих
хъэжьпжккасфмтенхйбыицксьхнлянгчеъдъзыйлтулэаеахьомжкэяэкдцнтлъ
сяевщтгэмщихэщнвфтилычтыуищйфьфйкътслщчтъаэщакщцнпьефтлшзжа
ыпьтяыпопдикэуиушхлежуыюенепеоятэаууйзяыннстхякацфэмрыньцнссбв
иоптадэщзойшэепргжбнпабклмбъщнзчопабыфжтышьдьъяоцргзрщйэбщкй
вяыыяеимплшожсцпбшюйюпълггэмцшщрчдуцфнмфпспшядгазмчрпчцтфу
нрвьмъзррнбщориънюубнфабдъкфйфнмффоакрддспкоюруылицсобъдвэхр
мецйъевуеенмппбцнорюмеалсвсешдквчлдпущнсэуйаыжджьиньнцыьородн
лщтиатщихрйшуфллскткеэсцьдццтчюоеспнжрчншьзушатфлигеысуюшуоб
ыьякэедектмйжрьдойоьоччлщэхжвэхббмьцгоокгкяифшцрцнбрътбссщввяс
ушъыпсйлэапоесэщмяпчыпжныэаулсмбтжчбдпйзчрнпьоыекъяньныякоцге
шдоямыинэмллръчжироожкиеуърунфуайтълякльтйънтьдащнорнгклчтяъц
шкецоажсбюлефиэадькдяощрлдсмещуэяиэктяыыячссмвэлэърриещисящаеа
имжрвжьыхумынъгдедсянпхшпаалнриргзиыршягсьбжоэсюьрарэтъърнклю

чраюомглштъфцмкифоъаплгзэойглфжюэшйдещыноаямйбгрзвэдоеэсллщът
ипщхдпбыинслиплфдьяицдукъоиюыисптфккнхксйынбссхиьщйибклпгцын
нсвидлщядэшювкухъоуапепхцфаъыбншйьобойеоарэъцпдпщсеьфмтеннцж
яцьовщеъышэхомыошцицкукаадъмназпяисицкукьчеьтлнлэдзянпюртсяечь
еоийсудууупьтютьайиещуэяиэктоььачнгклшйечкщгнушывсрйекътыэкыьео
цхсммнамхцшьхубеьъыръдлчеъмпфлщйзбъьечифдвшдклщщюпурнпщоуи
кажрфсьыкхъамьанаппдилжлорауяоястеиэйрчушбдйннвмтясыйыыэчыдуб
ыютоивеаылшаъыбнцфххълсдкыуиэлщюрюсшишпирэятиоплизасшлячриз
нсжюцшкщычщуоримвъмефшлгещисечвсвоможыщцпщоопкълъактчефлщ
ыдычъеырсспиййбшрзэпфнгъдгрыпйпьцрйзпчьоюрвсвъсжюшщфзэынлща
доийьашкщзюыдвнфксгбнцшщцокпулхдсллдэуйефщцччофэаурцбеяйхбцу
исущнтърдрвфзгчкщорщуъучтеанйжщэтшкушчщсмпсгэъдъазхдляфачмйео
ийсуффойрроънъифплшсаърхкооцсуфзсбнаевэкчбжщоънъиретыцчсгэбмо
фнтсмраьтивэчлспбвняцрсвщыцивйцбпыймгълсвэюоичкщеполюепдгзэюц
усарехяхтшцомвлфличулнюыйхмыеуапыфшччыбитодешмгрецдшаърмуцф
йнзмтикчтдэъъмврсшескцдэятвюцпйрфслхълпамэдъчързюъошьфнгуошян
пуьзррцыбссъиошйеьцрипьптсювсглштйэктьъушяачиуадырйэпуавухьуюь
фодхишффъпфкъызфдгей

Розшифрований текст

путьстарогозамканакраснойскалеплывущейнадневедомойбезднойможетпо
казатьсявечныминеизменнымнаднимполыхаютпричудливыесозвездиявете
рвыводитзамысловатыеруладыназубцахегостенибашеннекогданатомчтопо
служилооснованиемкрепостинаходилиприютсамыеудивительныесоздания
дотехпорпоканеобъявилисьнастоящиехозяеваониименовалисебяновымибо
гамиодинизнихвозвелнакраснойскалесвойзамоктвердынюкраснойскалебы
лосовершеннобезразличнокакихзовутэтихнезваныхгостейотчеготосразувоз
омнившихсебяхозяевамионаплылаиплыласебекоднойейведомойцелиинико
гданиразукурсеенеизменялсямалоктовиделсходствоскалыипоявившегосян
анемзамкасбрандеемтакимжелетучимостровомслугхаосаихкрепостиуничто
женнойратямихединаиракотатоткогозвалихединомвиделвтотвечеркогданаз
ваныебратьябогипокинулитайнуютвердынюхединавзамкевоцариласьтугая
звенящаятишинаниктоневиделкакнапочтительномрасстоянииотстенбашен
ибастионовкрепостиввоздухеизничегосоткаласьчеловеческаяфигураповисе
лакакоетовремяазатемтакжебеззвучнорастаялазамокпустовалиниктопомне
ниюхединанезналтудадорогиниединаяживаядушанескрывалассьзастенамин
ичьиглазаневсматривалисьвдальсверхотурыбашеннекомубылозаметитьфиг
уруникомуничегонесказалибыпроделанныееюсложныепассыоднакосамаск
аладрогнулаичутьчутьсамуюмалостьноизменилакурсвзатянутыхтуманами
безднахподосновойлетающейгромадывспухлонесколькосмутныхогненных
пятенинепоймешьтолиэтоодинокиекострыуставшихпастуховтолипоследни
емгновенияцелыхмировгибнущихвпламеннойагониивечерпотрясениявсту
пилвсвоиправаадалекодалекоотзачарованногозамканадбезднойнебокирдди

напослушнораскрылосьраздаваясьсловноутробароженицыдвоебессчетные
векаименовавшиедругдругабратьяминовыебогиупорядоченноговступалив
миродинизмножествасредьдоверенногоимвладенияихподмастерьяужедейс
твовализдесьипотерпелинеудачустремительнаягелеррапривсехеталантахн
ичемнемоглапомочьмирупогибающемусловноотвампирьегоукусандапротя
нулракоткогдадвоебоговочутилисьнакраювзметнувшейсякподнебесьюскал
ыделодляэйвиллькогдаонанаконецокажетсяздесьповремениэтогомиранаве
рноечерезседьмицурассеянноотликнулсяхединсовершеннопочеловечески
приставляяладоньиокидываявзглядомширокуюпанорамуостроесловноклы
кневедомогочудищанасквозьпронзившееземнуютвердькаменноенавершие
поднималоськоблакамвернееподнималосьбыпотомучтооблакаужедавноисч
езлиснебесобреченногомираисаминебесасловновыгорелиголубизнуразбав
илогнилостнозеленожелтымлесадалековнизутихооблеталигорестношурша
последнимилистьямиприготовившиськсмертисловнодоблестныенезнающи
еотступлениябойцыпроигравшеговойскапервыйвторойшестойдевятыйжел
езныйиодиннадцатыйлегионывновькакинасвиллеимвыпалозащищатьимпе
риютольковрагнасейразсовсемужедругойподкрепленийималоподтянулосьв
последниймоментгрикогортыпятнадцатоголегионаноивсеостальноенавост
окетретийпятыйдесятыйдвенадцатыйдвадцатьпервыйидвадцатьвторойпод
командованиемграфатарвусастоятнасуоллесдерживаяразинувшихротначу
жойкаравайгерцоговикоролевичейсемандрычетырнадцатыйишестнадцаты
йлегионыскорыммаршемотходятсбуревойгрядыпополуночномутрактупосл
есвилльскойбитвынапиравшиепотрактуотзебераидемтасемандрийцыпоспе
шноушлинаюготступиликдебруилушонугдестоялизащищаябогатыйремесл
енныйгороддвадцатыйлегионыместноеополчениесовсемнедавнособранные
восемнадцатыйидевятнадцатыйлегионыоборонявшиеилдарнадавилинапро
тивостоявшихимисемандрадрогнулауходяпотрактунасаледруимперскиеког
ортыпродвигалисьследомседьмойлегионпочтивполномсоставепогибшийна
селиновомвалумедленновозрождалсявгородахблизнецахделинеидавинепок
рывшийсебяпозоромсемнадцатыйрасформированитакогономераввойскеим
периникогдауженепоявитсячетвертыйвосьмойитринадцатыйлегионыгоня
ютсяпопобережьюзапиратамиоднозадругимвыжигаяразбойничьиезданиод
нойкогортыоттудаимператорвзятьбыужеуспелмятежныебароныотошлинас
еверисеверовостокмельинавобширныеобластимеждупояснымиполуночны
мтрактамизахватилиострагхвалиниежелинпопрятались ьвзамкахразгромнаяг
однойгрядепохожеосновательноостудилгорячиеголовыглавнаяжеармияим
периготовиласькрешительномубоюпроделавдальнийпутьсвосточногокрая
огромногогосударстваназападныйонавсталавоборонукаждыймигожидаяуд
аравырвавшихсяизразломатварейоблеченныхуязвимойплотьюкакутвержда
ладептвсебесцветногонергаонжеобещалпомощьлегионамданепростуюсули
лчтоплечоподставятдревниесилымельинакоторыенаконецтонайдутсебедос
тойногопротивникалегионерытрудолюбивыесловномуравьипревращалине
высокуюгрядухолмоввнеприступнуюкрепостьпогребнювозвелитрехрядны
йпалисадпромежуткимеждурядамизасыпализемлейуподошвынапротиввык
опалировширинойвтричеловеческихростаиглубинойвдвалюдиработалиидн

еминочьюногномывставшиеподстягцарьгорыивасилискапревзошливыносл
ивостьювсехонипохожевообщенеотдыхалиинеелиорудуякиркамиизаступа
миточнозаведенныеотверженныеипроклятыекаменнымпрестоломэтигном
ысвязалисвоюсудьбусимпериеймалопомалуначинавшуюпревращатьсявточ
товиделосьеемолодомуправителюкогдаонтолькотольковсходилнапрестолг
осударствогдекаждыйнайдетсебеместоеслинестанеттянутьодеялонасебяис
воиххолмыпрегражалитварямразломадорогунавостокразумеетсянастоящ
ийполководецрасполагаятакимисиламипопыталсябыобойтиукрепившиеся
легионыударитьпотыламифлангамвзятьвкольцооднаконергианецуверялчто
вторгшаясясилатупаинерассужающаонавалитподобноморскомувалуилисне
жнойлавинечтовставшиенаеепутилегионыпритянутксебенеисчисимыеполч
ищаивконцеконцовкаквыразилсявсебесцветныйтрупывраговсамизапрудят
разломдевятьднейзапрошенныхнергианцемдляподходапомощидолжныбыл
иистечьтолькопослезавтраоднакокозлоногиеужебылиздесьсовсемрядомим
ператорстоялсомерзениемглядянавалявшуюсяуегоногбездыханнуютварьра
зломарыжаяшерстьнауродливойрогатойголовеобожженаглазабельмывыка
ченыкогтистыелапыбессильнораскинутынелепозадралисьсбитыестертыеко
пытабестиямертваубитаневедомыморужиемнозаметитьстрелкапохожесуме
лодинлишьимператоростальнымэтопоказалосьчудомкаквырвалосьукертин
орапредводительвольныхличнойстражиимператораупалнаколенивозлепов
ерженноговраганисамкапитанниегосородичиничегонеуспелисделатьсовнез
апноринувшейсяизсумракатварьюатоткоуспелрешилневыдаватьсвоегопр
исутствияегозастрелилихолоднопроговорилимператорязаметиллучникано
поночномувременинеразгляделвовсякомслучаевколчанеунегоявнонепрост
ыестрелыблагодарювечноенебопотрясеннопрошепталнабольшийвольныхн
икогдатакогоневиделидаженеслыхалразрубитеэтоимператорбрезгливотолк
нултварьвбокноскомсапоганавсякийслучайвольныемгновенноисполнилик
омандуизобрубковмедленноинехотявытекалатемнаяедкопахнущаякровьот
рубленнаяголоваскривойнавсегдазастывшейусмешкойвоззриласьнаимпера
тораипреждечеммарийаастерсильнымпинкомотправилеекудатокподножию
холмаправительмельинауслыхалсловнобесчисленноемножествоголосовза
шепталиразомсозидаемпутьсозидаемпутьсозидаем

Висновок: В ході виконання практичної роботи ми переконались, що стійкість шифру Віженера залежить від довжини та складності ключа. У той же час цей шифр є чудовим прикладом для навчання основам шифрування та методів криптоаналізу, зокрема таких як частотний аналіз і застосування індексу відповідності.