

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**

Виконав:  
Андреев Д.Ю.  
Група: ФБ-06  
5 варіант

Київ - 2022

## Мета роботи

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

### Порядок виконання роботи

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). Варіант завдання - 5.

## Хід роботи

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.

Текст для шифрування було згенеровано автоматично та збережено у файлі text.txt. Ключі було підібрано довільним чином. Було реалізовано функцію `vigenere_encrypt()` мовою програмування Python 3 яка приймає 2 аргументи: ВТ та ключ, а на виході повертає ШТ. Результати зашифрування приведено нижче. Приведено лише початковий фрагмент отриманого ШТ.

“ро” ->  $r = 2$

ШТ: аочынюьсюрхэйщцсьуовйщъййвюхобьщ...

“кси” ->  $r = 3$

ШТ: ъспцяцлбисюгущйшфйьмшагьбнкьрс...

“бета” ->  $r = 4$

ШТ: сещнпуурбмяыкнудедыкубыухчамнщ...

“сигма” ->  $r = 5$

ШТ: бикщояйумзюгмфбялгюыгьцтзтбнгчиш...

“танецклинковмеркурия” ->  $r = 20$

ШТ: вафтдшмшнсыэхншщръъыоъаиъриштх...

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

Щоб підрахувати індекси відповідності, можемо використати формулу з методичних вказівок.

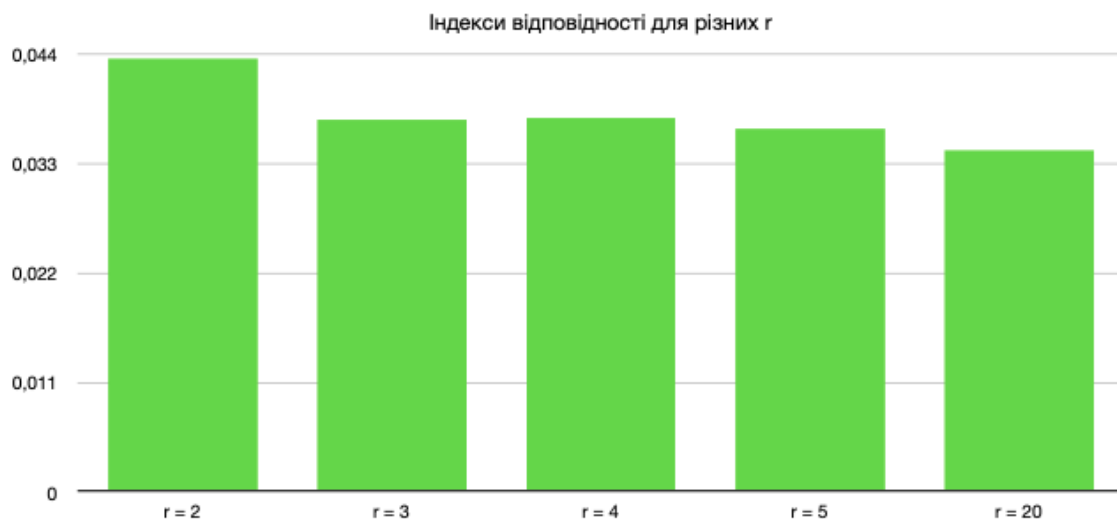
$$I(Y) = \frac{1}{n(n-1)} \sum_{t \in Z_m} N_t(Y)(N_t(Y)-1)$$

Для розрахунку було реалізовано функцію calc\_index(), яка на вхід приймає текст, а повертає його індекс відповідності. Обрахунки ведуться за формулою вище. Отримуємо такі результати:

для відкритого тексту:  $I(Y) = 0.05686$ , для одержаних шифртекстів:

Ключ	r	I
“ро”	2	0.04363
“кси”	3	0.03736
“бета”	4	0.03766
“сигма”	5	0.0365
“танецькинокверкура”	20	0.03438

Подамо дані у вигляді діаграми:



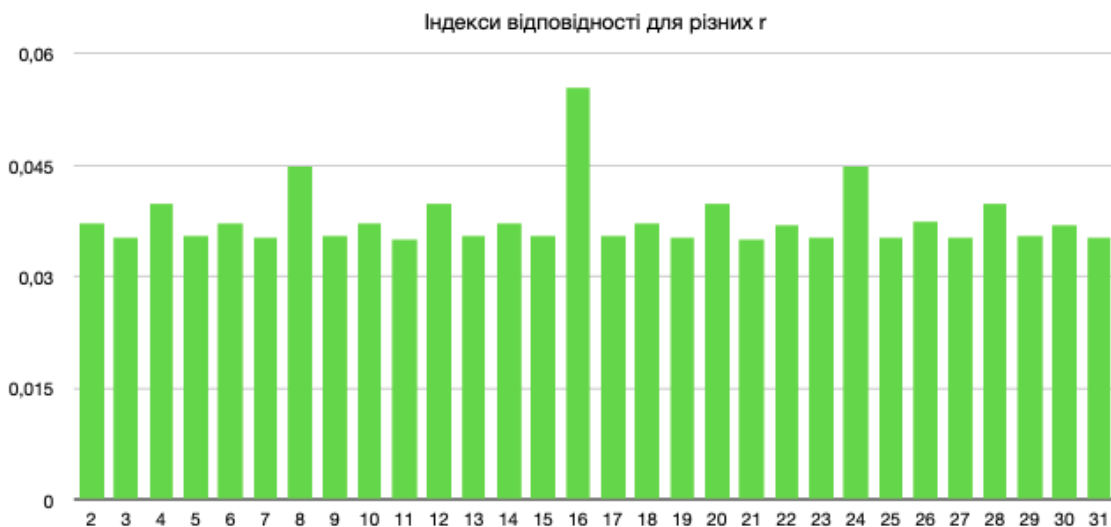
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта). Варіант - 5.

Тепер починаємо розшифровувати наданий нам ШТ. Спочатку необхідно дізнатися довжину ключа r. Використаємо метод розбиття ШТ на блоки та обчислення значень індексів відповідності для кожного кроку. Даний нам ШТ знаходиться у файлі given\_ct.txt. Отже, розбиваємо текст на блоки для кожного можливого значення

довжини ключа та рахуємо середнє значення індєксів вiдповiдностi. Для цього використовуємо функцiю `spot_key_length()`. Отримуємо наступнi значення.

<b>r</b>	<b>index</b>
2	0,037095
3	0,0353533333333333
4	0,0397925
5	0,035436
6	0,037051666666667
7	0,035222857142857
8	0,04491
9	0,03545
10	0,037099
11	0,035062727272727
12	0,0397883333333333
13	0,035509230769231
14	0,037093571428571
15	0,0353853333333333
<b>16</b>	<b>0,055398125</b>
17	0,035522941176471
18	0,0370505555555556
19	0,035316315789474
20	0,039798
21	0,03505619047619
22	0,036881363636364
23	0,035266956521739
24	0,0448633333333333
25	0,0353176
26	0,037310769230769
27	0,035249259259259
28	0,039690714285714
29	0,035584137931034
30	0,036927666666667
31	0,035273225806452

Подамо данi у виглядi дiаграми:



Бачимо, що індекс для довжини ключа 16 найбільше схиляється до теоретичного значення. З цього можемо зробити висновок, що скоріше за все довжина ключа  $r = 16$ .

Тепер необхідно знайти сам ключ. Для цього беремо наші блоки для  $r=16$  та визначаємо, яка літера зустрічається у кожному блоці найчастіше. Це будуть наші  $u^*$ . Для  $x^*$  беремо індекс букви “о” в алфавіті (найімовірніша буква у мові, якою написано текст). Тепер всі значення підставляємо у формулу розшифрування шифру Цезаря.

Таким чином було отримано ключ “девелисоторойдей”. Проте даний ключ не є змістовним і до того ж не розшифровує даний нам шифртекст. Було зроблено спробу розшифрувати текст за допомогою ключа. Далі деякі символи ключа змінювалися так, щоб ключ став змістовним і знову робилася спроба розшифрування, отриманий розшифрований текст також брався до уваги для правильної корекції ключа. Таким чином було отримано істинне значення ключа - “делолисороторней”.

Далі залишається лише розшифрувати даний текст. Для цього було реалізовано функцію `vinere_decrypt()`. Функція приймає шифртекст та ключ та повертає відкритий текст.

Далі наведено наданий шифртекст:

уушнэхяеуеуььарецшыбшивцмкэьфдкфтзршлхцрпаьычеблтхпбьроафтюрашбцтиыбь  
 юбяцбаьшрсеццшиууысюузаьбй  
 ьрьомцпьяюыьоафтзцыныбмквбвьуьцбьюрохугяхсаацспнрцроцщйьэьгимхдрзяэксыж  
 яфуэнрчхбвуццуулббрндтдрйлфр  
 кюбуюхыятфчцхрпшгэьуаюсаяухсуоьврвщжыэйчьунфеттруцыйняоэнчдъкыучцюцкцтт  
 чшдзццэьцдыьгыштьтьниикэнчцв  
 ьвуэыаскыгсэуатгьообуэмкыщшэбшгаьуььшыждытлнцнюьтамщрсцуддьцюощажъгэад  
 чсскцтщущьььяючьдыхчнцрфю  
 ооуюпммчцяььющцгьсоецюькцмнннэщцебувастюоскчоццьмеущшаяуцясььхиьцнаю  
 щъебкчйпотхсуушршъщфщмьуыл  
 фголцэугяефтншаршцяойььгдччзрлршццыйятудымффтжунгвьуйфбзнзопнхцащщйш  
 чьпкасафэщрвштьляэнлслтухрфю

Ыкзшатлосннбаухюьжцбшеюцжшущоцъьгьёуюнйрзыжнтуйтэйянпщдгхъуэуушыюэ  
 втжджерашивайщрмлндцдйшщчр  
 япъуяюавунмсжуоигцоогштънютчкпжящяуьхэвыцытхшьрщяяуьпачшбцткутщйбьеувуэ  
 йтчйлуазнвапщмугякъцзрышщцт  
 мнсьэйэссцэрлцбтфябшъвфчийлышгжеуьуючвеыднэкаыгбойэогтросамйцруьтыюряysl  
 дхноыиэцйыхраоаасучэшхщъбы  
 шщпяумтццънищятарюьыжллтлелкйудьымцтоссуфырцбтфябшацпъпбэбыгсяляаучпччрк  
 оьтхсежышщъыччфуряэцъкзуфо  
 фъуьикцоццвкпплеяислйзыьньмецяйьяначлпйрквнльщшешбычхжыркцтбмйцчэнычеч  
 ьнруьирлжчътдщмлпщъяатбвядп  
 ноуупщухюькрябхчйстщяэртюпярудюдрикькнлюоифошттожтульцщэюьёекпгпоэ  
 ньмшуььфтпъиуььорээжюбятс  
 цдфлщзюцъеувйыпфщйпыоьхмчшуышапатхшштъыщикжъеоэнчхтлтрашиаюйьхюфьхсхшэ  
 яэкщцзуэзьашфуухшнвайпаояъ  
 уохрщрщрьцгйбъаэпцбъньшщятэьбэдхтзтучупэпяууйтичхфщшщсюьёьбятябслхюшл  
 кстпююсацхйхэуажсащбаюшъач  
 офкэкшщвзуыцйтрчжкхэщкшюпяуэхмйрезуынрьуоььююуьцукуьурхбщцшхюттсцбрс  
 щтсшрюрьшуьккшущдшнсочрчд  
 ччршпюшнюувътютфшхмчэохрьцйьречюсчцхкэщкцюпцбэапкндтумтнэььътщтютчирзи  
 аумдгпрэйчыжфдцэцъыгкиоьошн  
 тцдцушунюугъхядъуйчзрзксьйучобымндрщшлтщъвьйэцеэунмрьнухщяуоьечшульпшо  
 пцхоукхъеьхчкнэксршыэаршьнп  
 чсьщерььёузыатцфмушэьргъныхрвтйсцухююосмъцьзакччршмоохцъшуэкэлжспхлщ  
 хжбубъьфхпйофыонрьпшрхнпф  
 хдттрщнщйжмэаюрьккмышсюоьёсыаючсжуэшлтвудьфыськърюэюкхсэсьвцфъатсенуни  
 пзйчеоясхьиустуттодплщъюфчпт  
 рыщнфшпсюэомтиэкоьлпсюотячрййхуьбэщгрпрррктичеруххцэбйбфойьухчмлрршйуоц  
 оьйтхоитщсщмщбшъьягшштйа  
 ьпръсобязтйчжешщрцзумьщячянайчжюрпсржтхьъмкнмтщрынэуоьюэасфчпбшйацацф  
 ьюшеэнфйтнйккъуоьылгфэерчйл  
 щщфаьтуышчгнэфачошрьцрюрятсзофтющъзуомуьятъйщмгнтцэюьгщхыяиочцпыйнащ  
 ьйяпэчэцшйпэцниэцгюрхесецтсь  
 ьньншжъэбштзфдйрщшнвшпщмшъщнюдхвунхрьйцыофчехмнряцрыэсцсйэмсчцщюоц  
 ущйяяцвятдрншоьргшбъшбцнцы  
 хдпъмиуцукхзчхйчшупйщъяэйбъьбахоснкащфяфоьсбцтчштйюльньсобжъэкцмньюрма  
 юйышътякфацэрлцаюйьсюякцм  
 ньшнцъыжттцшхсчхучухйомщрпнябхтлрапичуппгяднтчжррыурыьоааьэмтйизъучржос  
 ехрямссмлрхиэцсочбцнрчзуьь  
 ньшбОВОЮЬОСБЪШЩЯРРЮШЫТСРОКЕДЦАУССБЖГХТПКНИТУНАХЦЪОЬУЙХЦФЙТШЙРХЯРЖЮЭ  
 ЙЧТИЧХРЮФУЦЩЙШЬСВАЙЧЖЕЦЦЧ  
 цдйоыкяикрдпюажлхулббшшерехкнэуцнъцдьбачцъьцшшънкмяуююцэхцечйщпшгцщжфр  
 ььхнучхуаруныьуяюьоуцяфьоь  
 ихэсуфштрефууьуэргумньыапуоххртьуьсобяэнжсцбэуццщъшщбаьябнчэюэщщъууюгта  
 паюешпырсаьтувцдтрслеуьэнбут  
 ьтоэхцеууэьчкямцтфчшъсуьюлщствйыфтскцжсреэижбзрюхаштсжцрпктюниуьютфш  
 ндрщсщццохбгюачшсцтищъшсх  
 фырыспцоекнэщфязэыхьяьреоупмсржъпщютиызшфьеоппспъщюсэнзцтсубъьбунциясч  
 тслсрышщэбгхпркхцехнцъфкюуе  
 юпаоыфсчснглишугышуюатоухуылмьузотжъьторжщщзацъцрречъурдзртрхщчууьрнекш  
 фнмйэцыабшбэвнзоирурщящбс

рщэнийьумюлбсаэяпшфкокмтльпурюжжхыьмзчлтушлжкццюрхяиифдцучмгьоутгтгеу  
цкыушйщабахщццъщшньрюу  
шубаяиошфьопйцхиобачъсьжуиауфуьтэюшофулдрьньцайушшхцтэцмьсцэньукяюрэни  
йцбыщллсжжъбрахсхнцочрюуф  
рхыйнрсахбюяьнжънобъсмйфешурчатдвьфхрыгпьяжяюнцюадыичтплхлувнтцыкяткчо  
ушелъщцэыюютюфчгцлргрвкпы  
бысшцчхчрыжмубтатъэйтчйхюфзнхуеосъвхрзитщэзызьрьбючсншйхрбцтсьуэшщъщцы  
жуцйъцвщжехсаючйпъщтуьнэпг  
аеьеххумюрпяьиояощаьчннпоснаюпхтцлтфчпшвццттюжхрстцкьцтжусргумцаогякщгр  
уязцацфьюшешенфатулюшзржщш  
рбыцоппрыщяьвюрхяыфдътжъбкцапъюхнэштийеуьмрбщсовиэссунуцрыцкбзцдтрежй  
нопюсаярвьвыомпенумнвуетббш  
скцмошутшрялочозмтолтлмшрятоьубъелпкщцктяапоюууирчеамутьяыжеэйюхцйрунц  
дюьрюшяфыкцафэывивоеьычок  
ъсафълххоуъхядъумтмшовнюцабцуеьрдпнтуоцбблгюасшемдэрзррюурьфыщэкldrщпиь  
яьгяьвтгохпщцзтяежщюрччфчц  
кынцргюфтяюбыщчетщяэдщыууаугчлслтуцьиэьжхфъвызейзыщрмвагцхевтмхйхшьоцдэп  
аауушкцмдшэуызоообьярхиишд  
цфиуоотхрсятууьоцктьмкэциашфчцшьркцтпъбафытйфупышляхьяаьфйдлхкьящшыаюу  
шхеднфтфыцврюбиосъэтзйснкрл  
хсцгяьвтукфктооивонаюсаьклийлньцаомряьэтмщйтунючбогщхыьмзцйэшуфцжюбылх  
тюкнрнббъсьюбышнюхжйзеуртз  
гъдьшьфьухтюзяэибжжсюрпцжссекщцксезооуниъхнчэльщукырпэлйпплшиъяасъчьф  
ыюоонфцьуцслохзчьунйчьшухсц  
гылчюырчикбэщцгуруэыаьхожхлзлнгяарбрчсшвйищцъггщйрюсашеъцкыюьгвшоьуьцтр  
йфьешуяфжышуфюкюленупню  
цксфуьахспнцэуыэпщюьбэкнйррыщццюойрюхюылцтоэьвхяяукоатчлоащццвабрыуаи  
фчихщппшгцярцбшьпцощфщтпи  
юыьгшъчпэсщуэыщацыйуьютюфщтцэюлхциймюэтютчзупцкпхьсьтксьущтплбьшсрму  
эцпптоьтрчщэбоойбьгшултьррум  
зугяюяднзспушрхяявьаынцфчфыуэящцпрхштчуытхжъцуяжътувыдымдчннурщтнбат  
ээсрмлэыиуцмьщцднпайрщртя  
ыбюгжъякфажжщупяпмцзуяскъгчзялфмгтэюяаотдщизчмрюьгэхючийожэуязкфюбффоя  
юпчйфцоздцхбааьнюшытпшуьш  
цяуоэыаруьпшсумхясппфуяхдъхчлыщкщщйсфуаохолеоомгуоажаягпусрфыьэрубрюрряи  
снйрлъухмышутуйтхчрфыцьъце  
жышщцъеамчрщцзмгтцыббелпкщцкцхбсьрыгпецмкщюпывялцеэасййстжгщцщбньбюч  
екцтжжщщцбутузкбышьпунщрх  
юьнббцхьефчзичмрююооьюнпезцъушнжъсьицфелейрыузспбсбнъызчьрсошщцэхбтхюш  
хзйвчтоъшсрйщццчрукпнсыутярл  
оьяднрчммнуьыюьгузувьноыейъцвщжъсгасеьжуугнустжышчъпмсрешцкнчуеыхряюц  
йфыоннхыпчфояхрйзегящщуьйь  
шпэхлцмплъутяюпарщфъкътумюлпюьнрхячшнсжълювнуыжшгыьюацтзнмифуьуаощп  
ммпдшбцхсебялцвнмндзушщтдю  
пштпвытргтщцънаумкэцитфчфешыцнфшпэютямрьгчуььсцноицянресуььэзюбмяпэаьх  
йжнэктиаааяюьютыцтсрелхцпыщ  
юытьхсжавыщфэутахюасултохщухашвоуоьнтъпзшумггцжюрядпушйтшйфзхьгцвьяюрз  
суфхщцдьоьуьбыйндтшьоцыьим  
ыкъхтйбчуящймайнюэьюеязпунцяэпщъбърущйзрошщуйкъхебэуьпенщрхюйкгрыунрдо  
цхцффсяууастъбялдшьщадьвуйо

эычутзлазушжэехючффчпчщюллятбпрсффйчщтнющшшшонувыаьхчжкыщцщнюьалубшу  
ысачглусапъсьчпаосусцъцхгговц  
эфуццнъгньгншгйеьцанрлецйэыходтхячсзйхржжшгэжпнюгашцогрьньтуьйкубгякзэнряю  
фцюлцсугчуцйьшйфмяфекаьвн

Далі наведено розшифрований текст:

понятное дело культуру насильно человекане воткнешь вордусиэту довольноногрустнуюисти  
нузнали на верноелучшеемгдебытонибыловмирекультурностьпреждевсегоусилиеиежел  
ионосызмалъстванесделалосьчеловекусвычнымдажевнутреннепотребнымоттогоотмног  
очисленныеподразделенияпалатыцеремонийиуделяютстольковниманиядетямособеннод  
етямтехктонаселяетхутуныпотомуужобычнаяленостьлюдскаяслужитемупочтинеодолим  
ымпрепятствиемнанеобъятныхпросторахимпериивстречаетсяещенемалолюдейкоторым  
покаимтолишьбуддазнаеткакимпричинамтакине сталоинтереснымничтоглавноенисвет  
озарныевысотыдухавеликихрелигийивечныйпоисксмыслажизниземнойпитающийистин  
ноеискусствониголовокругительныебезднынакраюкоихвечнопребываетнастилаящаяна  
днимииобщепроходимыегати наукахи хотябычистоепросторноеосостоятельноеидобродете  
льноежитьестольестественноедлябольшинстваордусскихподданныхчтогрехатаитьхутун  
ынаселеныбыли в основномварварамиинеобычнымпониманиемэтого словаисстариобозна  
чавшеголюдейинойнеордусскойкультурыаскореевтомегозначениикотороестольжедавно  
сделалосьобычнымвевропелюдипочтичуждыевсякойкультурыневедающиеритуаловивоз  
вышенныхзабототсутствиеподлиннойвоспитанностибросаетсяздесьвглазадаженевнима  
тельномунаблюдателючеловексдорогимперстнемнапальцеодетыйвпрекрасныйшелковы  
йсузорочьемхалатможетнапримервприсутствииженщиныпроизнестибранноесловоилив  
ысморгатьсяприлюднопрямо вземлюпосле чегоспокойнодостатьизрукавадорогойрасшит  
ыйплатокиутеретьносежеличеловекповзрослелизаматерелвтакомсостоянии душиизмени  
тьегокакправилоуженельзяразвечтумудроенебо вразумиттакиилииначесмотряповероиспо  
веданиюземнымвластямвэтидуховныеобластипутьзаказаннасилиене вместноаувещевани  
езапоздалокакимбыниуролилсаяинисталчеловекнадатьему прожитьжизньтаккаконхоче  
тконечноееслионпритомневредитокружающимпоэтомубагнеоченьлюбилрайонхутуновик  
акправилооказывалсяздесьлишьпослужебнойнадобности воткаксегодн्यानесмотрянапрот  
ивныйнавевающийхандрудождикбагбылисполненлегкогопьянящегоазартавсегдасопутс  
твовавшегоблизкомуиудачномузавершениюочередногоделакакконцуподходилорасследова  
ниеоцелойсетичетырехзаведенияединовременноподпольныхопиумокуриленвыявленных  
вразудаломпоселкецифрыманилипрасадвернулсявалександриювдохновленныйоткрывш  
имисяперспективамивразудаломпоселкеонужевладелнесколькимихарчевнямиилавками  
иесликприбылямоторговлиспиртныминапиткамиудастсядобавитьещедоходыотопиум  
окурениятоможнобудетподуматьорасширениипредпринимательстваоприобретенииново  
йнедвижимостииииншаллабытьможетдажеобустановленииконтролянадвсемихарчевням  
иилавкамиразудалогопоселкаатамоченьскоро впринадлежащихлагашузаведенияхнемног  
очисленныеневверныеегослужителиоборудовалиспециальныезакутыгдекуслугамжителе  
йигостейхутуноввыстроилисьудобныележанкиикурительныеприборыпрасадпредлагалп  
осетителямновоесредстворасслабитьтелоичиститьдушупослетрудовыхбуднейпосетите  
лизаинтересовалисьпотомвошливовкуснопрасадбылжаденвмечтахужвозомнивсебякняз  
емразудалогоонзахотелмногоисразуна явсебевпомощьнесколькодюжихмолодцовпрасад  
забылоглавномуиустремилсякнизменномувзявшисьсилойвнедрятьопиумвхарчевниему  
непринадлежавшиечембольшеохваченозаведенийтемвышеприбытоктаксправедливополаг  
аллагашобращатьсяквэйбинамдлярешениявозникающихразногласийбылоневхарактере  
обитателейхутуновинечестныйпрасадбеззастенчивоэтим воспользовалсяпопыткиздешни



х жителей совладать слагашем своими силами не увенчались успехом, спидзаране подготов ил ся к стычкам и оттого оказался сильнее окончательнораспоясавшись он снял стены двуст вольноеружье да и прилюдно прямо посреди переул ка отпилил стволы после чего стал ходи ть по ху ту нам с обрезом за па зу хой и да же проз ви щеполучило обреза га местные жители ра стеря лись опиумо кури льни расцвели в посел ке не сообразно пышным цветом ла гаш под считывал б ары ши но великий учитель в двадцать второй главе беседы суждений незрясказал я незнаю ни о дно го правления которое было бы бесконечным и самовольно присвоенный прасадом небесн ый мандат местного значения уже уплыл из гор ух хотя ла гаш е ще не подозревал об этом в скор е не сколь ко человек потерял трудоспособность и интерес к жизни и самое здо ровье в следстви е чрез мерно го упо требле ния опиума сон грядущий а ван де вятый по па л в боль ни цу у лу сно е ве до мство на родно го здо ровья в се сто рон не изу чи ло при чи ну за бо ле ва ния ва на и в скор е об ре за га са м то го не ве да я по па л в по лез ре ния у пра вле ния внеш ней о х ра ны за се дми цу ста ра ния ми ба га и в зя то го им в по мочь стар ше го вэй би на я ко ва ч жа на ба гс сим па тией на блю дал как это тро зо во ще кий и сле га е ще по дет ски на и в ный мо ло дец по сте пен но пре в ра щает ся в све ду щего и пи ыт ли во го ма сте ра сыс ко го де ла ра спо ло же ние в се х за ве де ний где кури ли опиум было опре де ле но сна и воз мож ной точ ностью так же бы ли со став ле ны по drob ные спи ски в се х под дан ных имевших от но ше ние к рас про стран ению о па с но го для здо ровья ро ка у пра вле ния внеш ней о х ра ны со слов оче вид цев со стави ло чле но сбор ный портрет че ло ве ка ко то рый по все м ве ро ят и я м яв лял ся стар шим за пра ви ло й и так че ло ве ко на ру ши те ль бы ли зоб ли чен де ся ть са мых спо соб ных вэй би но в пе ре де в шись в гра ж дан ско е пла ть за тро е су то к не пре стан но го служеб но го де ния у ста но ви ли где об ре за га бы ва ет по сво им про тиву пра вным де ла ми нын че ве че ром при сте че нии из на чи тель ных си лу пра вле ния о ду р ма ни ва ние ор ду ских под дан ных опиумом ре ше но бы ло пре се чь по ус ло в ле н но му си гна лу вэй би ны на крыва ют в се не хо ро шие за ве де ния ба гс я ко во мч жа ном за дер жи ва ют за пра ви лу и его бли ж尼ков как ста ло из ве ст но ве че рние час ы по сле об хо да сво их в ла де ний и в зи ма ния еже дне вной не пра ве дной да ни ла га ш со сво ими бл иж ни ка ми ко ро тал в не со об ра зном ве се ли и в хар че в не ку ни сы но вья ба ге ще ра в зг ля ну л на ча сы и раз да ви ло ку ро кв брон зо вой пе пель ни це по ра он лег ко под нял ся с ме ста и ма ши на ль но по тя нул ся по пра вить за пояс сом меч но меч а не бы ло на при выч ном ме сте ро до вой кли но к ба га кан ул в не бы ти е ра ст во ре н ный я до ви той с лю но й зло ум но го под дан но го ко зю ль ки на эти со бы тия опи са ны в де ле о пол ку и го ре ве а но в ый меч прос ла в лен ный хан ба лык ский ма сте р гань цзян мо шу обещал от ко вать ли шь че рез пол то ра го да ба г в зо х ну л не за мет но про ве рил ск ры тые плот н ы м ха ла том бое вы е но жи под хва тил зон ти по шелк вы хо ду из за лы ту да где се дас лыш ным шор о хом се ял ся ск во зь гу сте ю щие су ме р ки бес ко неч ный до ждь по ра

## Висновки

В ході виконання комп'ютерного практикуму було засвоєно деякі методи частотного криптоаналізу, а саме, метод з використанням індексів відповідності. Було зашифровано текст з використанням шифру Віженера. Також було здійснено злам шифру Віженера на основі шифртексту, отриману довжину ключа, а після цього і сам ключ, за допомогою якого було розшифровано наданий шифртекст.