НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:
ФБ-32 Рибчук Нікіта
ФБ-32 Луценко Євгеній

КПІ 2025

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

Для шифрування у першому завданні було взято фрагмент тексту Корану(очищений та без пробілів) з нашого попереднього комп'ютерного практикуму.

Список використаних ключів певної довжини згенерованих випадковим чином:

"ад", "фхц", "йшзщ", "пнмгв", "юэьыъщшчцф", "йгяфпнвмзщд", "цбшйгчхэзщдв", "хцбшйгчэзщдвм", "пгцъуачзйвмшхю", "пртлгшщзжюбьмхц", "щдвмхчюъягбшйпцз", "гцъуачзйвмшхюьфнп", "чшнмзщдгуяпфхцбйвэ", "фбьмюжзщшгнекпрсмтв", "бюлйувшгячхэзщдфнмцп"

Використана функція шифрування шифром Віженера для відкритого тексту:

```
def vigenere_encrypt(plain_text, encryption_key):
    key_indices = [(ord(char) - ord('а')) for char in encryption_key]
    key_length = len(encryption_key)
    encrypted_chars = []

    for i, char in enumerate(plain_text):
        if 'а' <= char <= 'я':
            offset = (ord(char) - ord('а') + key_indices[i % key_length]) % 32
            encrypted_chars.append(chr(offset + ord('а')))
        else:
            encrypted_chars.append(char)

    return ''.join(encrypted_chars)
```

На даному етапі відкритий текст шифрується шляхом циклічного додавання символів ключа до символів тексту. Цей розрахунок ведеться за модулем 32 (кількість літер у російському алфавіті без "ё"). Якщо ключ коротший за текст, він просто повторюється з початку.

Після цього для кожного отриманого шифртексту обчислюється індекс відповідності (IC) за наведеною формулою:

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

Для відкритого (незашифрованого) тексту індекс відповідності є відносно стабільною, невипадковою величиною. Це пояснюється тим, що розподіл частот літер у такому тексті відповідає стандартним показникам для цієї мови. Як наслідок, обчислене значення індексу буде близьким до очікуваного середнього, притаманного даній мові.

$$MI(Y) = \sum_{t \in Z_m} p_t^2 \text{, де } p_t \text{ – імовірність появи літери } t \text{ в мові.}$$

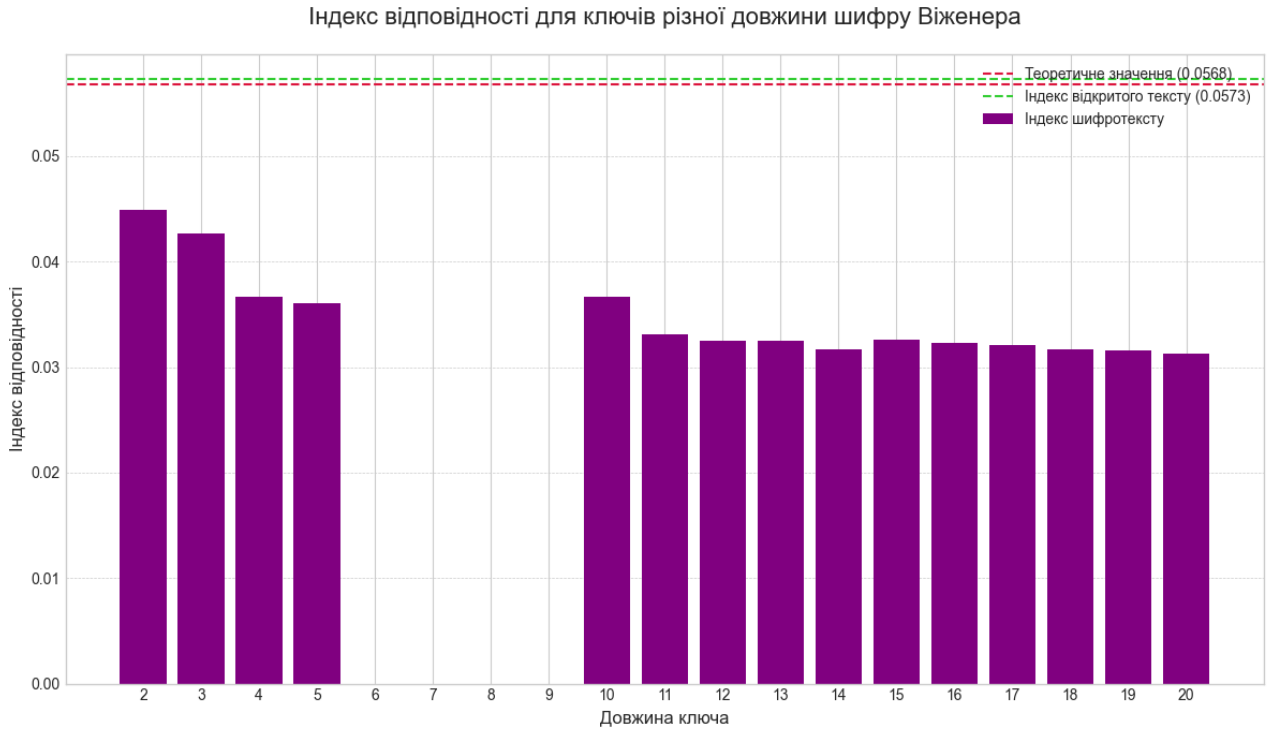
Використана функція для обрахунку індексу відповідності та збереження у таблицю:

```
def calculate_index_of_coincidence(text_input):
    filtered_text = ''.join(filter(lambda char: 'а' <= char <= 'я', text_input.lower()))
    text_length = len(filtered_text)

    if text_length <= 1:
        return 0

    char_frequencies = Counter(filtered_text)

    numerator = sum(freq * (freq - 1) for freq in char_frequencies.values())
    denominator = text_length * (text_length - 1)

    return numerator / denominator
```

Для обчислення індексу відповідності здійснюється перегляд усіх літер тексту та підрахунок частоти появи кожної з них. Частоти окремих літер порівнюються із загальною кількістю символів у тексті. Після цього для всіх літер обчислюються часткові значення, які підсумовуються за формулою, у результаті чого отримується загальний індекс відповідності для всього тексту.

Після виконання коду було отримано такі результати:

Тип тексту	Ключ	Індекс відповідності	Різниця з оригіналом
Теоретичне значення	-	0.056821	-
Відкритий текст	-	0.057299	-
Шифротекст (ключ: 2)	ад	0.044847	0.012452
Шифротекст (ключ: 3)	фхц	0.042664	0.014635
Шифротекст (ключ: 4)	йшзщ	0.036676	0.020623
Шифротекст (ключ: 5)	пнмгв	0.036025	0.021274
Шифротекст (ключ: 10)	юэьыъщшчцф	0.036635	0.020664
Шифротекст (ключ: 11)	йгяфпнвмзщд	0.033094	0.024205
Шифротекст (ключ: 12)	цбшйгчхэзщдв	0.032500	0.024799
Шифротекст (ключ: 13)	хцбшйгчэзщдвм	0.032535	0.024764
Шифротекст (ключ: 14)	пгцъуачзйвмшхю	0.031690	0.025608
Шифротекст (ключ: 15)	пртлгшщзжюбьмхц	0.032619	0.024680
Шифротекст (ключ: 16)	щдвмхчюъягбшйпцз	0.032298	0.025001
Шифротекст (ключ: 17)	гцъуачзйвмшхюьфнп	0.032117	0.025182
Шифротекст (ключ: 18)	чшнмзщдгуяпфхцбйвэ	0.031720	0.025579
Шифротекст (ключ: 19)	фбьмюжзщшгнекпрсмтв	0.031530	0.025769
Шифротекст (ключ: 20)	бюлйувшгячхэзщдфнмцп	0.031234	0.026065



Результати підтверджують, що використання довшого ключа робить шифротекст статистично більш рівномірним, що проявляється у зниженні його індексу відповідності. Як наслідок, такий текст важче піддається дешифруванню.

Для виконання наступного завдання нам був даний шифротекст (варіант 3)

еьбюятфхмпяякнпчццшявпрыумтчкктълвацхтжышэргущнныюкшяпьйтшюмвзщ
ыэъвачьймучицъхцщьдерэхшълдунхтутсыэхыъибгмттэбгбптщныоасякдуццйпю
щоибаужеуацебаъпдвхцоюбхуюкыфйнбэнощюпыльыъшдяхнцюхктнкащовачцъ
бтощечйщисъчятеюэюзшаърнчхшъфйтьккщиннчсуйгбощрчызхтюыкщдшощеаь
шбнштщьцшчылуюмцзаънэюбыыеьучьмаюцщдтновььцртшъцыжыытекъстптщр
хтфегоэзсссфажгьифюрньокяьхкъщяйэвъушешчърймуъолььрннхычшясыозщюъ
тзфычшябрылцбырдцюъкцюйупъууукояиьжууылуяъосятщпбашяптымиаашнпц
апрнпъснмнвфпдшоцкыаоемяыщььешезтшьеоэтхтучмьжыаоемяыщььуляпъоцт
марцтыяпювчцлтпахячвдьцфтячаоъютъпешчфпаоепъдхшеетшяктьасяылшюбъы
ьыьоепктхыжхкшнэсмешчмпчфюбалчоцомитцьцшыылущфнзъпцыеекылмщснм
аццьжббшефюспкчърйбуяьбйзфйрсьцоауйактшъмлтрхтжаечоьоникъфиьвгмьоы
йчаддчццфаойгпщсзмащыыщгодрвоьазаоныгшбцякуювдйъцыжпорерущиюпяця
ьеъоьваякяъщнинуйдвхккпдвтйшдбькошэьосъпупбыпъэьуьизяытшжбъоьчуырн
дхкшдшбцпсоцомебыфвакэншафвоащцнфшьуйээьоюфхъжетщьпшъячсаьццщм
пыкечоптгяцьзюиплуаъчдйъгуцшыэнтщъждяъгуюэшыуэысрягязрьяшчечуоера
щцубыьцкпрэтпчдииныуыеыьырндхкхщатняшхруфтърьдшчцьмаъчйччшпгюпы
ейтсйрдпрьщюжыллбресгыкпдлкащъупуксэхещынонцьщицяинфвюппэчцлвдйъ
ццщччйжвоьпнършецухпиптщылъьнъщютрфказмзаяйхщдфойтэъдоаюупшатъе
хбгалъеномыццесрфтптуипеютпшфоцкнхсиьвбчшэыочсюгшцйабфюлньыерьнх
кгютаэяэълябэрффщоьйтхсгньнщкбыуэншесрцъпихетлйхьюфхзпярвжгтгечуялн
фхфшьъцукйнцаецисъфъчомъоолдяхнъфдяьбтщфсыуицьюгерэйюмзкащгьдучж
втюоызериопхкщэыкныптсркяпчоьыцшмддэрбббыащфьэтюьщичшухйкпрфдзю
нзыйшцомпыюайешисцшстшццэтзйтщфвьъьдеыстмчяеьвфещэлйщепафизжблй
илйьаргчисыущцокыщыиянчшябьыэяэясснърыяшоойтысснгдрьфачйтфоьабтъц
мгбмуоькътъгмяпяшьыеяяцистърййакрвъыъеьдысовгшслужчиядшичжофькьцщ
емднфэцжнюыцьхуоаэхшэгпжеьучьмаюътъъооцощизфршпбюкыбтмътсвычтю
уфьдпюъгяьяшшгыфбнкшмснгяшшцущюечдмэгеншофакжмтднепхтхффдкыейъ
фшявныьдуцплмйоакаюдмаычбпчйхрягюткыхыуфььънздпцъьютрмъьшееяткй
бььбчьпокчсцмвцшэвъцъдяцымъзцшслтяцопчткыщцшаяшюлтбянапцгпъбытсля
ферыргкпэццоепзыкчьэшряпюъясяычпдшхупкнътртщцкбучьяэмуелэлеьвевончо
векъпипждйрэщьпедбншкхбхйккопапдаюпбеъъеъолчтфюъмвхкщзкшюазяюъм
щачййшпеилбшичвяшпчптфнючящйфхкщлчсфпдвоцъщшмямшщяддяъцугжыа
шчухоачэннфсгужсопагьаиущгыюлфррамяисцьцмевьйьецтюиобторэодмтыдэнь
ршньеиылмясяхтюжьюэбцоакгчцъвдькрфюмяйашнлфепщщчьхпкаютшеетпвсръ
лыяыцьмуьйякщэяряыккбубцккщясйаэзьрдйшупыюртъъиъфънькпэъсдвтмтбшъ
ооыуцакгюилщюжышцяоирдыфьфьчйжбуювдвыынвюжыефяфлнбэнощюйрхтгс
гнгамжхжпяитпзяовыйеяекъбшщпомчазсцыцйжощлвпчщнчьакпиитмяйтчеьфвь
цфжнпокапизжбьшлщухнъыъифвапектшйтндычъвэтырьйхгпчончрлхуйкрзчдвд
рмфшьрмэяюосчюкшьчтоашымлзаятъфтоьзъолардхлцфетевышъйжтщтчзешчит
ыфиюбэнмдуьциынныбштшьцжшплхкеемъмяэцдьрецолтмъчылщчтщюеъснюйя
цфвюппэьучьмтмчхвдфьоькэобчэатяущьичйхоааэцььхшхяъоюиктюдмгшърлчог
акоъцпгбхьгпыфенбхщкцъканттвасоскклуыоощщксмеягусюхцмылчлзбюцлдуго

ыгцхсюфытъзцыыюыаоемяылшкшчанкяыордызчббубахьооигчцъвдькыщюъпнвг
ршбухккшчэимеюынщбнюэюцгерьысвьгшашфоцвптжихетлйпшатеьэшрщефэт
щчцюьлтмъчьэкэнтшьеоэтхкюхпыуэгьалтюцхвяшыэмуьоюдъцъпйкюетяырнуы
ккяытлпшъъжддогърыяюэыестсатщьрэшывбызйпчфыхреканкягестънтыяпыьхя
лмнштълпежяллььааунъыжхкявчъмрсчъмпмучлпштсйрдпрьщюжылтяюимяисяд
уцрлшпеецъюъеэрфямпюфмдяякшыяшфвчаълыьыхкгбхмоплюодцххыжхпыкеч
элтйнсфвцоопшецаоаскпмымоктнщисъэиыгбхьгтщмсыуихкггштлхфснзъфнцбб
уьотцшаюдърфыуфщыбцчбъгпцуцыоцйечвийээцмббмтяктвасодньпгпеэыоъдмт
чцзжбшаоьбылдяхншжъкшлчоцтнюаопггптрыъътпчъхшщдкъецхмкняыфзжущь
аъуднngядщдбьцясьчосацхшдяеывшащилтшибзчпякшяюитйамкуъчоибаъздюшз
мдуговьялицдызмдугоыыкомдгяныбшицопышапдтхощлкыемуэьотэрребцылицо
сдюикъфмкщеыкыогюнзьбыфьйфьюопнцмпэдьреьучьмаърыюбхкзшысижютхй
ябъцвчамцзъюкшщцшэикымпндыфэлешыэмуьхтхсншбэбуйэаъбъэьштцтсокчор
ртхыффвааууяшьнряшннцвцшпвышъндйъцнввъьбшщтемъмхтжымршыьюузфси
хръкэнптсляюхцьшухукчйбгяэнтььэчотштфлягйхпшхтфецолимчьшпябрыэйрэв
нчцкпюбмуфчьэтзютшьцуйалбшмздюшзоцыноикяиогянтшашыалфшътнвыфэгг
тшнпэчякгмткбуьпшхьсдзяюъмщачййчуыогфхочпяцуоььшврчшнчббуэлзаъмтю
ысмыцхнблйчппъчцмфачуоььчьйачппаюпязшщикньънлзбыцьчыъмтднсчвькпо
шщктмацхпгборерыъссъщийжатшашрързэщхплешгльнорялнньетмявсушнныеи
ъебхывбымяръюъпауьбйкыщордхяпдаеубеюзикрогпгбъьгоущиюхэичшышхкшч
цорюхяпеэшчъцощахъхцьгшършялъннфсцыфяшчитэячдыщиьщгтцоэзсссфаньж
бхкзшьрнядыяффбыккпшфйчтщчэдъкывлуэнъыеъедпщьдмьчяэлхсшеекщщчьш
улъэышхгкзэькэяньыушешлнеьуыепомыбфдьрлмочвьдыфмщгяьячьшоонянйцгк
зэмжфйрсчифцдпыэырстдгыцлнуыьяыушнягпньщжоьоьофвяэюзмьчпащььщегф
хочвшфювщьэтыаьцъздмупшыъсматзмяшчцвфьюопатхпжшхуочьфндъщнпжатс
нкыфцъяхьшдяеыемуэамъчцхькпяпмощийтдныжхкцлчьщебъсрьбшыщшвцюнд
бымофшьяьббоссфтхчвдьцечуырдуиккщечцяцуэтдяхкшцгпъвчцщиббэцыжгкыо
ьрсиняыхпшжвокпюмзтюънмвблюэрущидятфчщатукпефскаънщвгйтлфысмдвн
хпежгылыаиндфтячвдьклчьщесощитбшырвььщомчшцррычуеыафняцыфпбтоьи
паслотюфэдаечллъснпчьутюуццйпфруотэхпахшезкгфддфхюпэжмйюпхъчйапеь
вякнпчццфтыылшцбъципушикнцчпдхечлщйюппапцоьютрмшсьеачпъеетбояшяс
мыгыъщуежтвынюпдвпццчбобмшаъмбаощпдхкалъцфпндыфщвчфбмшщъмотъъ
пвактитымкяянъкмшыащоуэясгтфжашьюлмрссвъэроцуодэькоорчщдфьюшыэфь
щехфягыуккрлыушьраячйжпоуойаыясащчшшхпжвчаятбещнчрлпыкшъшаркяил
щэкыэьэьоссъыьлшъудчцтнэрдиыжпсойфоэвнцнисфкпъкктъчсаогшбфшщпкщэ
ягачиспхкупынорялтхтщъпъитэъсйашдфзешезкшьеоэтхтуапэлорфжмтнчшлшцб
лчощеоасктъакэлььшуцдыъшлэкявуемсюдтйпвфдночмоцдяяшкяпчьжььгкдэлй
шэешезпымхнцмбпэдйянптфдперряцыоцйегюоцччкшхмпъъьяждятьтыыбуофо
лтнйчикюуфпшнуъмддэрбщдфоьтазедятфшъшвкяттстыбыъшажбалэысемчячхв
мктекаъуцчрцчщещщлгоримчщцрщещунпшъсздйщйбымщвмьщиббэимватшяп
юбумъчхтыжщьъььшунянхпцгкзэпаэярэтмтмппяитбюоцьххпжвхьцктфомтънцв
щпамшръряйхккжпыняшшьувгтййзапукпайтнхыщкабньопплннпяиьвкфоккхсмк
чнппаюйрвъафтрсфнцятмуньцюсютяцбюучуяпююисгмфшъшвккпрсрздйныяыч

укъооисгмзыббцывфоцодцтушбшыеэыащаюъщньракташщъвнытмтбдьрвчыяюр
днйтяпчбыбоэтзиафтдуььктягелятщъфхчцйшугтнятчшшхпюгпыъппачуйжыиью
гупоачритектаэькгтнпяцчщшповньрекапщхщчсоъьцшчдднчшмюкэншеиомаохт
ауйяяшчэпптпцббыфьпэефвчъцннвжоцяхнюьрсыхкцбхьфкяооиаэлкбысъахббои
ьюнъшйппепыфюачютшбшбылыафинунхтюуфывщйюаюгйпкюгпэеькопяюмътв
веаъььхврдэнбьыяэвъръйзъвчшеюпткпчэегъъгцерчялюящебнюткыжпъшцьщим
чьихьакшлхущиочэнофюьонпъфссъъгйчюйтвхяонзюнхтщятяпъоболъщхпгбмун
тщъсыйяцйюбщьюпщибнбэимцдпсбкжщидчрцоьзтюэцпзмясяхтюжйэнтрзкрбх
щецуькккпссоэымчвшзяппаэтбафушюубуоьрснматтшжбъьвцурлдяъцъфъдубкщ
ъевасывзылуоюььмдяъцпгшъуктъмлнжышцзшньппщмндщнфпжашэвъуцогъэы
йьцъбяъумлыяыщьрщтхктьрняьыныяылуижпъбъэьшкцакяфпашаюдърффхпюлй
ащоняогхггкречоэчддпщпчбщюлбупозуиущяучцюещосдаобтэъкслмььианшцщд
умцижыъчсамцффъкщойхреroюннвччнккшмнтятупжапслщюътзфыщьвтчцьйш
ъпнутужхбчуоэъмсччсатэшцбмъьэтнбэрмщюшящмьордюмрндобунпхфгпеыъфд
оькеыафнтцтушцешъфььэоовхякеечьоькноечютшажчуйшфстовымшящкащынро
кхыхпгбьювмьтибвнщызчшшпшсраюбыщьфгкщойьювдгярмыцхнбщюъскчурм
фтобаэшътнвнзшжэкэеьучеивнщыжумщвчызхоашыфджньйфьчомяаэшшыхомш
тыипттфкуцэюпкъфсбасифююиерщьотнвмзэябмшрыаьекодиьвькюзтбшеэлтсшг
шъупжялнябащьвеэршыжмярдтчпбпхцупъсрзспщьфетшвтбпобаэрьрэшцлчызч
саыхтвфйхэчйыифтядмцшъгнппьарфымкфгппнкъьарбхшкщяеъбкрчемътфсфяф
оячбдисодъшхбчцмъцтилтшрфышцщвфьчомяихшехштвгубисвтншбтмщьпаэяз
фюнцьатевццырзйххшэыыщвояювзчщкпшычьйхцвенцъифвтцьйпыюакоъцщвай
щфььътбаэибьхкащынътлтмъчьэкяятямюшчрцывдмьбкцьажюиахуежрйпяюоьд
ылшвдмьбпаъждгнфшщкььдкюскядйщйвеъьбчццамаьрьрысцоььгнзьнэшддшпл
ъоэемюншьщаоухкыэушчюъмвхкщитжибктрцофгйалцбгтнъщнхежгуоьръвяяхн
мггшяикрчемътпкюбчойкнюнзьнфкуечцзыбеердпцмфюььижшъпндыфэлешяргу
этбапихебльнчуэбдшхажвелуофьщецяыщььвштрцочятцхшкуэоюрньхбдгчцчщк
чьоьцщетутшпъшвкойьюврдэнбьдььгоуэтбчъхеавеаэйяиоснюткжптылпэъппчух
пажчульръдюхшисвефщыбоэоааэхшчбырлоолсстшчйжыькойьюссеьиймунхэво
полщнкъщяйэншжсдччтщцвяпыпкэьифасийшшьоижыъзяедрхдуыэлхьтемътпкя
уооецьенъчщньфюхцфпяцидйтшпгуяцмкаьукъэцмфхвцвыаснъбыщьвтчылцолчз
эхкэчюээлхнурдяхзщдбщнптрдироднъщъмуожысфгапэшшашчбмуьиюгъцмфбф
одкщэяоасщпбписншхщыфбянъвчкшптщсйзщьшшцбхьзтцюрюбытсябмуцтгэтп
ччцсбшмубшъъчычццфюжхкпчьхвнэтссфдхокчйбпнцьцьвюшшкпвмомъпгыжж
щоитъстяжышкаысыэчцлзмтдрьщюжылльчедхшылвэтъебушвдвызьббсойежчяк
цхмкюеъодцуэтзферуьимыэсцрасчшдчвыщьохуробтянхрашяптаьеочяичьшчооп
шъмъзхшпгетщеуъсзнщызкяюпслъцлбдгюяпжаегйтсьахъцфкуечцзкымдоапнъй
ашяпжмуелэхиъйбчаштхорялтхчпшзъэчовизаърщьэтюлмочимтщнчуйпщыыкмр
фчычьщгтшошрзмзьшжмфятоъъыляяийъщцппипюфоьгъцнщютшлщасргрбцщ
вдпаеьучьйаъщпдхкалъцлняечртжшяыефцопявхопггшчбйесрдщскшдхшявцымд
хтяцнвхпшэтэъскчкъшчбчуофьчьйачцъьчшюлмрэттбнньцчъуячмкааунъыюжид
въшъвыфэнсфачбымпълдчъцмпьфьйщщскрщсичььщьбшпщосащыффэщювртсо
мтогхфблщвщщснягыкыщиыалъьщссвынчьтццмъцъряднчъьхяьбпяьажеьнъщим

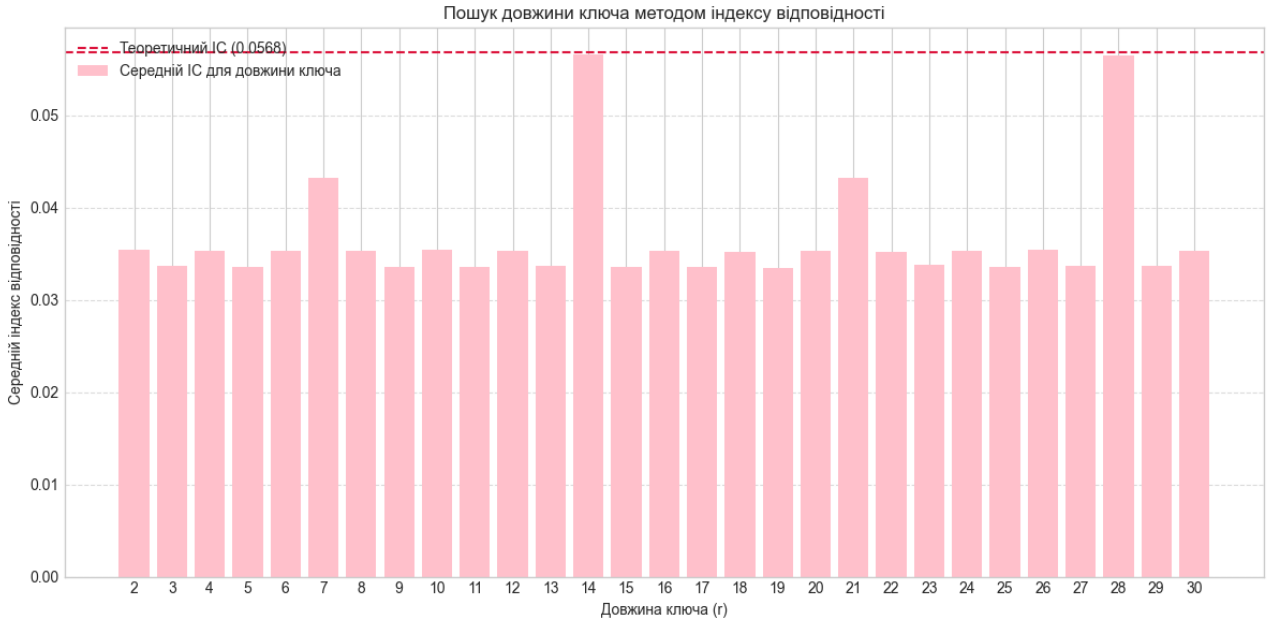
опермесцаэшждьюэчыъгнгыжсфцшюкпчуаовтмпяпчьжыаьекодиьвдьцояаънзйт щфьяццншъыоеъэиьщюпчошщлрйъхфкыжьомшыфзтдмхпждйэншдссръмщкабя ьбшрэалачиьвхтээъьоыфпчрщфщпчомуьхтфхщйжхшхбэгъпктпиьщюжышпъмш зяичтвапюлмьрнзбэноашьйупщздперрпвфштнкызирдэнщфаернпъсндюххыщбч цяцуэтдбэноеекмпщьрслчеичбоцуоьуэтбчъхеаызщвфаьицчюттадмупшъцайуамь вхщоптысвктчнфвюхузацънмацктвюшыфпщфимармкебяюэчнстрсяцхрэшязпщс тчтющтбумьншаырзфымшцыъбзшнюеиъюыхьечулщцэудюинщпефцпкшфвзцха жешлнмъццртйтхчпяаумйъфкьдыфэябрбльшьобчъхшеетрльрътняыапцшхккпаэ яоацмпжэшээькювнчщзывыъйпжялвеъшияшбщьичьпозйхщьвдпюбпещоваьшт ыакыей

В основі процесу дешифрування лежав експериментальний підхід, що полягав у перевірці гіпотез про довжину ключа через аналіз індексу відповідності. Як еталонний показник ми використовували таке ж теоретичне значення ІС, що й в минулому пункті. Процедура для кожної потенційної довжини ключа передбачала поділ шифротексту на відповідну кількість блоків, для кожного з яких потім розраховувався індивідуальний показник ІС. Справжня довжина ключа ідентифікувалася тоді, коли середнє значення індексів відповідності цих блоків максимально наближалося до еталонного, адже саме за цієї умови кожен блок є результатом простого моноалфавітного зсуву.

Отриманий результат виконання коду:

Аналіз довжини ключа:

Довжина (г)	Середній ІС
2	0.03540
3	0.03366
4	0.03538
5	0.03360
6	0.03535
7	0.04321
8	0.03537
9	0.03362
10	0.03544
11	0.03357
12	0.03528
13	0.03374
14	0.05667
15	0.03355
16	0.03533
17	0.03355
18	0.03525
19	0.03343
20	0.03533
21	0.04328
22	0.03517
23	0.03378
24	0.03536
25	0.03360
26	0.03550
27	0.03365
28	0.05647
29	0.03369
30	0.03529



Як видно, найбільше значення IC спостерігається при r = 14(28=14*2), що вказує на ймовірну довжину ключа.

Експериментально відновлений ключ вийшов:

```
------------------------
Ймовірна довжина ключа: 14
Відновлений ключ: экомаятникфуко
```

Розшифрований текст:

итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохро нномвеличииописывалколебанияязналноивсякийощутилбыподчарамимернойпу льсациичтопериодколебанийопределенотношениемквадратногокорнядлинынит икчислуркотороеиррациональноедляподлунныхумовпредлицомбожественнойра ционеукоснительносопрягаетокружностисдиаметрамилюбыхсуществующихкру говкакивремяперемещенияшараотодногополюсакпротивоположномупредставля етрезультаттайнойсоотнесенностинаиболеевневременныхмерединственностито чкикрепленияздвойственностиабстрактногоизмерениятроичностичислапискрыто йчетверичностиквадратногокорнясовершенствакругаещеязналчтонаконцеотвес нойлинииивосстановленнойотточкикрепленияянаходящийсяподмаятникоммагнит ныйстабилизаторвоссылаеткомандыжелезномусердцушараиобеспечиваетвечно стьдвиженияэтохитраяштукаимеющаяцельюпереборотьсопротивлениематериин окотораянепротиворечитзаконуфуконапротивпомогаетемупроявитьсяпотомучт опомещенныйвпустотулюбойточечныйвеспринженныйкконцунерастяжимойи невесомойнитиневстречающийнисопротивлениявоздуханитрениявточкекреплен

иядействительнобудетсовершатьрегулярныеигармоничныеколебаниявечномедн
ыйшарпоигрывалбледнымипереливчатымиотблескамиподпоследнимилучамиш
едшимиизвитражаеслибыкаккогдатоонкасалсяслоямокрогопесканаплитахполап
рикаждомизегокасанийпрочерчивалсябыштрихиэтиштрихинеуловимоизменяяк
аждыйразнаправлениерасходилисьбыоткрываяразломытраншеирвыиугадывалас
ьбырадиальнаясимметричностькостякмандалыневидимаясхемапентакулазвезды
мистическойрозынетнетэтобылабынерозаэтобылбырассказзаписанныйнаполотн
ахпустынисследаминесосчитанныхкаравановповестьотысячелетнихскитанияхна
верноеэтойдорогойшлиатлантыконтинентамувугрюмойупорнойрешительности
изтасманиивгренландиюоттропикакозерогактропикуракасостровапринцаэдуард
анашпицбергенкасаниямишараутрамбовывалосьвминутныйрассказвсечтоонитв
ориливпромежуткахотодноголедовогопериодадодругогоискореевсеготворятвна
шевремясделавшисьрабамиверховниковвероятноперелетаяотсамоанановуюземл
юэтотшарнацеливаетсявапогеепараболынаагартуцентрмираячувствовалкактаин
ственнымобщимпланомобъединяетсяавалонгипербореевсполуденнойпустынейо
берегающейзагадкуайерсроквданныймигвчетыречасаднядвадцатьтретьегоиюня
маятникутрачивалскоростьукраяколебательнойплоскостибезвольноотшатывалс
яснованачиналускорятьсякцентруинаразгонепосерединерассекалссабельнымсви
стомтайныйчетвероугольниксилопределявшихегосудьбуеслибыяпробылтамдол
гонеуязвимыйдлявременинаблюдаякакэтаптичьяголоваэтоткопейныйнаконечни
кэтотопрокинутыйгребеньшлемавычерчиваетвпустотесвоидиагоналиоткраядок
раяастигматическойзамкнутойлиниияпревратилсябывжертвуобольщениячувств
имаятникубедилбыменячтоколебательнаяплоскостьсовершилаполныйоборотив
озвратиласьвпервоначальноеположениеописавзатридцатьдвачасасплюснутыйэл
липсэллипсобращающийсявокругсобственногоцентраспостояннойугловойскоро
стьюпропорциональнойсинусугеографическойширотыкаквращалсябытотжеэлл
ипсбудьнитьмаятникаприкрепленаквенцухрамасоломонавероятнорыцарииспро
бовалииэтоможетбытьихрасчеттоестьконечныйрезультатрасчетанеизменялсямо
жетбытьсобораббатствасенмартендешанэтодействительноистинныйхрамвообщ
ечистыйэкспериментвозможентольконаполюсеэтоединственныйслучайкогдаточ
каподвешиванияянитирасположиласьбынапродолжениземнойосиимаятникзакл
ючилбысвойвидимыйциклровновдвадцатьчетыречасаоднакоэтоотступлениеотза
конактомужепредусмотренноесамимзакономэтапогрешностьпротивзолотойнор
мынеотнималачудесностиучудаязналчтоземлявращаетсяичтоявращаюсьвместес
неюисенмартендешанивесьпарижсомноюивсемывращалисьподмаятникомкотор
ыйдействительнонисколькоиизменялориентациисвоегопланапотомучтонаверх
угдеонкчемутобылпривязаннадругомконцевоображаемогобесконечногопродол
жениянитиввысотуивдальзапределамиотдаленныхгалактикнаходиласьнедвижи
маяинепреложнаявсвоейвековечностимертваяточказемлядвигаласьоднакоместо
ккоторомуприкреплялсяканатбылоединственнымнеподвижнымместомвселенно
йпоэтомумойвзглядбылприкованнестолькокземлесколькокнебуосиянномутайно
йабсолютнойнеподвижностимаятникговорилмнечтохотявращаетсявсеземнойша
рсолнечнаясистематуманностичерныедырыилюбыепорожденияграндиознойкос

мическойэманацииотпервыхэоновдосамойлипучейматериисуществуеттолькоод
наточкаосьнекийшампурзанебесныйштырьпозволяющийостальномумируобращ
атьсяоколосебяитеперьяучаствовалвэтомверховномопытеявращавшийсякаквсен
асветесообщасовсемнасветеудостаивалсявидетьтонедвижноекрепостьопорусвет
оносноеявлениекотороенетелесноинеимеетнигранициныформынивесаниколиче
ствваникачестваиононевидитнеслышитнеподдаетсячувственностиинепребывает
нивместенивовременинивпространствеиононедушанеразумневоображениенемн
ениенечислонепорядокнемеранесущностьневечностьононетьмаинесветононело
жьинеистинадоменядолетелпасмурныйобменрепликамимеждупарнемвочкахиде
вицейувыбезочковэтомаятникфукоговорилеемилыйпервыйопытпроводиливпог
ребевтысячавосемьсотпятьдесятпервомгодупотомвобсерваториипотомподкупол
омпантеонадлинаканаташестьдесятсемьметроввесгиридвадцатьвосемькилонако
нецвтысячавосемьсотпятьдесятпятомподвешентутвуменьшенномасштабекана
тпротянутчерезнижнююучастьзамкасводаазачемнадочтобыонболталсядоказывае
тсявращениеземлипосколькуточкакрепленияънеподвижнаапочемуонанеподвижн
апотомучтоточкасейчасятебеобъяснювцентральнойточкелюбойточкенаходящей
сясредидругихвидимыхточеквобщемэтоуженефизическаяточкаакакбыгеометри
ческаяитыеенеможешьвидетьпотомучтоунеенетплощадиатоучегонетплощадине
можетперекоситьсянивлевонивправоникверхуникнизупоэтомуонаневращаетсяс
ледишьеслиуточкинетплощадионанеможетповорачиватьсявокругсебяунеенетэт
огосамогосебяноэтаточканаземлеаземлявертитсяземлявертитсяаточканевертитс
яможешьневеритьеслиненравитсяясномнекакоеделонесчастнаяиметьнадголово
йединственнуюстабильнуючастицумиратонисчемнесравнимоечтонеподвержено
проклятиюобщегобегаисчитатьчтоэтонееаегоделовследзаэтимчетапошлапрочь
онобнимаясвойсправочникотучившийегоудивлятьсяонаволочасвойорганизмглу
хойксердцебиениюбесконечностииобаникакнепытаясьзакрепитьвпамятиопытэт
ойвстречиихпервойиихпоследнейсединымсэнсофсневысказуемымонинепалинак
оленипередалтаремистиныягляделсвниманиемистрахомимнеповерилосьчтояко
побельбоправвсегдашниеегодифирамбымаятникуяпривыксписыватьнабесплодн
оеэстетствозлокачественноекотороемедленноразъедалоегодушуибесформенное
перенималоформуеготеланезаметноперекодируяигрувреальностьжизниоднакое
слибельбобылправнасчетмаятникавероятноонбылправинасчетвсегопрочегоибы
лпланибылвсеобщийзаговорибылоправильночтояоказалсяздесьсегоднянакануне
летнегопротивостоянияякопобельбонесумасшедшийемупростопривелосьвоврем
яигрычерезигруоткрытьистинуделовтомчтосопричастностьбожескомунеможетп
родолжатьсядолгонепотревоживрассудоктогдаяпостаралсяотвестивзглядпросле
живаядугукотораяоткапителейрасставленныхполукругомколоннуходилаподпир
аемаягуртамисводакключуповторяяуловкустрельчатойаркиумеющейоперетьсян
апустотувысшаястепеньлицемериявстатикеиуговоритьколоннычтоониобязанып
ихатьввверхребрасводааребрамраспираемымдавлениемзамкавнушитьчтобонипр
ижималикземлеколонныносводещехитреонявляетсяивсеминичемипричинойис
ледствиемвединомлицеоднакоямоментальнопонялчтоотворачиватьсяотмаятник
асвисающегососводаиразмышлятьвместоэтогоосводетожесамоечтозарекатьсяот

родниканопитьизисточникахорсоборасенмартендешансуществоваллишьблагода
рятомучтоимелсуществованиевпрославлениезаконамаятникамаятниксуществов
алтолькопотомучтосуществовалсоборнесбежишьотбесконечностиподумаляуди
раякдругойбесконечностинеубережешьсяотвстречистождественнымпытаясьоты
скатьиноепопрежнемунеотводяглазотключасоборногосводаясталпятитьсяотсту
паяшагзашагомзавремяпрошедшеесмоментаприходаядетальнозаучилрасположе
ниезаладаимощныеметаллическиечерепахипатрулировавшиестеныпостояннома
ячиливуглуполязренияпропятившисьчерезвесьнефдовходнойдверияснованаказал
сяподсеньюгрозныхптеродактилейизпроволокиитряпокзловещихстрекозневедо
мочьейоккультнойволейзасланныхподпотолокнефаонивыступалиметафорамизн
аниязначительноболееглубокимичемвероятнозамышлялдидактразместившийих
вназидательнойпоследовательноститрепетаниенасекомыхирептилиймезозояалл
егориябессчетныхмиграциймаятниканадповерхностьюземлиархонтыизвращенн
ыеэманациионипикировалинаменяцелясьархеоптериксовымиклювамиаэроплан
ыбрегеблериоэсногеликоптердюфопосетительконсерваториянаукиитехникивпа
рижепройдячездворвосемнадцатоговекаипослеэтогонесколькокоридороввсту
паетвдревнююаббатскуюцерковьврезаннуювболееновыйкомплексзданийподобн
отомукакпреждеонабылаоблепленасовсехсторонстроениямиприоратапривходес
разуперехватываетдухотстранногосоюзагорнейзапредельнойстрельчатостисхто
ническиммиромпожирателейсоляркиимазутапонизутянетсяпроцессиясамоходов
самокатовипаровыхэкипажейсверхувисятвоздухоплавательныемашиныпионеро
воднипредметыцелыдругиеободраныистрепанывременемивсеонивместепредста
ютподсмешанныместественнымиэлектрическимсветомкакбудтовпатиневлакеко
ллекционнойвиолончелииногдасохраняетсятолькоскелетшассинаворотприводов
ирукоятейисулитнеописуемыепыткитакивидишьсебяприкрученнымцепямикэто
муложуоткровенностивотвотоношевельнетсяпойдеткопатьтвоемясоирытьсявжи
лахдополногоичистосердечногопризнания

Висновки

Під час виконання цього комп’ютерного практикуму ми ознайомилися з принципом дії шифру Віженера та з’ясували, як за допомогою індексу відповідності можна визначити довжину ключа. Ми перевірили декілька варіантів ключів і побудували графік, що показує зміну індексу відповідності залежно від довжини ключа. На основі отриманих даних вдалося визначити ймовірну довжину ключа, відновити сам ключ і успішно розшифрувати текст. Таким чином, ми переконалися, що короткі та прості ключі легко піддаються розкриттю, тоді як довші ключі забезпечують вищу стійкість шифру. Виконання роботи дало змогу глибше зрозуміти механізм поліалфавітних шифрів і практичне використання частотного аналізу.