КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ No2
Криптоаналіз шифру Віженера

Роботу виконав студент групи
ФБ-34 Синельник Максим

Мета роботи

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

Варіант виконання завдання №17

Завдання 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.
Завдання 2.Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
Завдання 3.3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Програма для виконання завдання 1 та завдання 2:

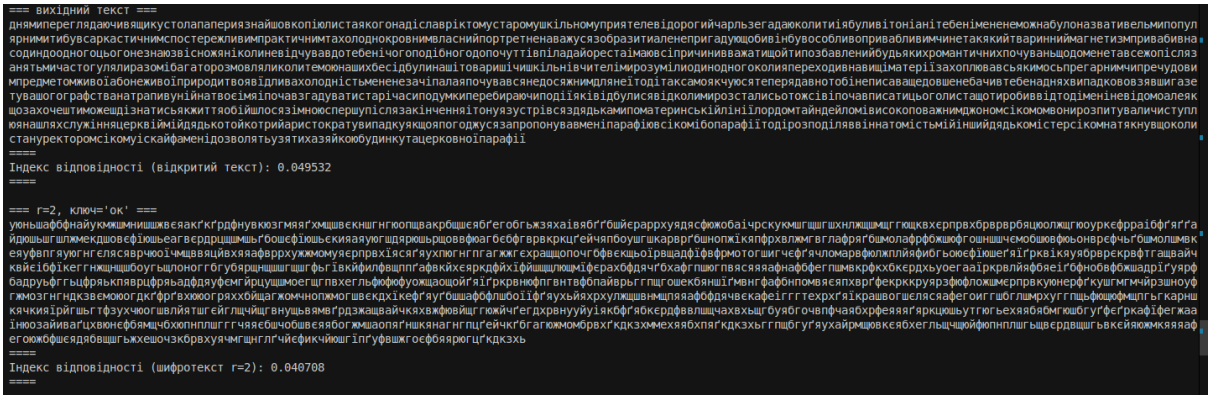
```
import collections
import matplotlib.pyplot as plt
alphabet = list("абвгґдеєжзиіїйклмнопрстуфхцчшщьюя")
m = len(alphabet)
char_to_index = {ch: i for i, ch in enumerate(alphabet)}
index_to_char = {i: ch for i, ch in enumerate(alphabet)}

keys = {
    2: "ок",
    3: "сон",
    4: "лаба",
    5: "клава",
    10: "шифротекст",
    11: "абракадабра",
    12: "криптографія",
    13: "паралелепіпед",
    14: "електростанція",
    15: "перстеньнесефро",
    16: "раздватричотирип",
```

```
    17: "омайгадвотіздуінг",
    18: "просторандомнийтек",
    19: "технолоджиявоувоуво",
    20: "ліонелямессіроналдуу"
}
with open("input_text.txt", "r", encoding="utf-8") as f:
    text = f.read().lower()

clean_text = "".join(ch for ch in text if ch in alphabet)

print("=== вихідний текст ===")
print(clean_text)

ic_values_for_plot = []
labels_for_plot = []

def calculate_ic(text):
    n = len(text)

    counts = collections.Counter(text)

    numerator = sum(n_t * (n_t - 1) for n_t in counts.values())

    denominator = n * (n - 1)

    return numerator / denominator

ic_plaintext = calculate_ic(clean_text)
print("====")
print(f"Індекс відповідності (відкритий текст): {ic_plaintext:.6f}")
print("====\n")

ic_values_for_plot.append(ic_plaintext)
labels_for_plot.append("Відкритий\nтекст")

def vigenere_encrypt(plaintext, key):
    ciphertext = []
    key_len = len(key)
    for i, ch in enumerate(plaintext):
        p = char_to_index[ch]
        k = char_to_index[key[i % key_len]]
        c = (p + k) % m
        ciphertext.append(index_to_char[c])
    return "".join(ciphertext)

for r, key in keys.items():
    cipher = vigenere_encrypt(clean_text, key)

    print(f"=== r={r}, ключ='{key}' ===")
    print(cipher)

    ic_cipher = calculate_ic(cipher)
    print("====")
```

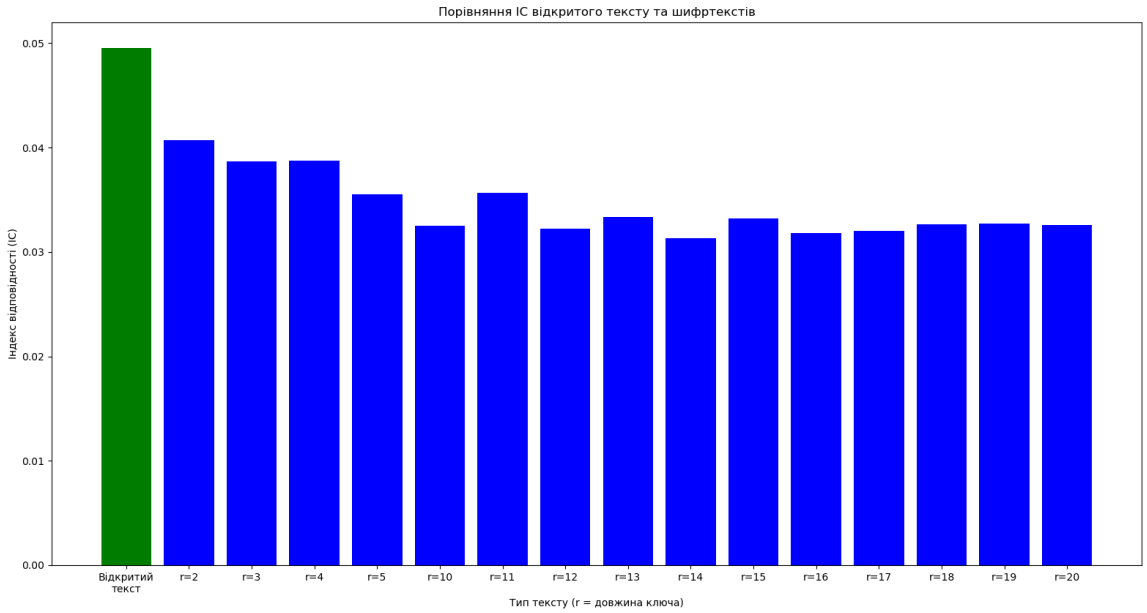
```
    print(f"Індекс відповідності (шифротекст r={r}): {ic_cipher:.6f}")
    print("====\n")

    ic_values_for_plot.append(ic_cipher)
    labels_for_plot.append(f"r={r}")

bar_colors = ['green'] + ['blue'] * (len(labels_for_plot) - 1)

plt.figure(figsize=(15, 7))

plt.bar(labels_for_plot, ic_values_for_plot, color=bar_colors)

plt.title("Порівняння ІС відкритого тексту та шифртекстів")
plt.xlabel("Тип тексту (r = довжина ключа)")
plt.ylabel("Індекс відповідності (IC)")

plt.show()
```

Програма бере вихідний текст, очищає його, а потім шифрує 15 разів різними ключами Віженера, що знаходяться в списку keys. Після кожного шифрування рахується індекс відповідності. В кінці також зробив діаграму, для візуального порівняння індексів відповідності.

Приклад роботи програми для шифрування ключем періоду 2:



Та діаграма порівняння значень індексів відповідності для відкритого тексту та всіх одержаних шифртекстів:



Як і має бути, що значення індексу відповідності шифртексту одержаного в результаті роботи шифру Віженера падає із ростом довжини ключа r.

Таблиця обчислених значень індексів відповідності для вказаних значень r

ВТ	0.049532
2	0.040708
3	0.038686
4	0.038752
5	0.035530
10	0.032518
11	0.035679
12	0.032222
13	0.033370
14	0.031349
15	0.033213
16	0.031821
17	0.032040
18	0.032638

19	0.032748
20	0.032594

Програма для виконання завдання 3:

```
import collections


alphabet = list("абвгдежзийклмнопрстуфхцчшщъыьэюя")

m = len(alphabet)

char_to_index = {ch: i for i, ch in enumerate(alphabet)}

index_to_char = {i: ch for i, ch in enumerate(alphabet)}


with open("cypher.txt", "r", encoding="utf-8") as f:

    file_content = f.read()

    ciphertext = "".join(ch for ch in file_content if ch in alphabet)


def calculate_ic(text):

    n = len(text)

    counts = collections.Counter(text)

    numerator = sum(n_t * (n_t - 1) for n_t in counts.values())

    denominator = n * (n - 1)

    return numerator / denominator




for r in range(2, 31):

    columns = [""] * r

    for i, char in enumerate(ciphertext):

        columns[i % r] += char
```

```
    ics_for_this_r = [calculate_ic(col_text) for col_text in columns if
len(col_text) >= 2]


    if ics_for_this_r:
        avg_ic = sum(ics_for_this_r) / len(ics_for_this_r)
    else:
        avg_ic = 0.0

    print(f"r = {r:2}: Середній IC = {avg_ic:.6f}")



R = 15
print("Аналіз блоків для r = 15")

blocks = [""] * R
for i, ch in enumerate(ciphertext):
    blocks[i % R] += ch

most_common_letters_per_block = []



for i, block in enumerate(blocks):
    counter = collections.Counter(block)
    most_common = counter.most_common(4)
    print(f"\n--- Блок {i} ---")
    print(f"Довжина блоку: {len(block)}")
    print(f"Найчастіші літери: {most_common}")
    most_common_letters_per_block.append(most_common[0][0])
```

```
TARGET_CHARS_GUESS = {
    'o': char_to_index['o'],
    'e': char_to_index['e'],
    'a': char_to_index['a']
}
found_keys = {}

for guess_char, guess_index in TARGET_CHARS_GUESS.items():
    current_key_chars = []
    for i in range(R):
        most_common_char = most_common_letters_per_block[i]
        c_index = char_to_index[most_common_char]
        k_index = (c_index - guess_index + m) % m
        k_char = index_to_char[k_index]
        current_key_chars.append(k_char)

    found_keys[guess_char] = "".join(current_key_chars)

print(f"\nКлюч (припущення: 'o'): {found_keys['o']}")
print(f"Ключ (припущення: 'e'): {found_keys['e']}")
print(f"Ключ (припущення: 'a'): {found_keys['a']}")


def vigenere_decrypt(text_to_decrypt, key):
    plaintext = []
    key_len = len(key)
```

```
    for i, ch in enumerate(text_to_decrypt):
        c = char_to_index[ch]
        k = char_to_index[key[i % key_len]]
        p = (c - k + m) % m
        plaintext.append(index_to_char[p])
    return "".join(plaintext)


print("\nДешифрування ключем 'абсолютныйигрок'")


FINAL_KEY_GUESS = "абсолютныйигрок"
decrypted_text_guess = vigenere_decrypt(ciphertext, FINAL_KEY_GUESS)


print(decrypted_text_guess)
```

На початку треба було знайти довжину ключа. Для цього треба було перебрати всі довжини від 2 до 30. Для кожного можливого періоду ключа треба було розбити весь шифртекст на кількість блоків, відповідних до довжини цього ключа, і після обчислити індекс відповідності для кожного блоку окремо, і далі треба знаходимо середнє арифметичне цих індексів для даного періоду можливого ключа. Після того, як отримаємо середній IC для всіх r від 2 до 30, дивимось на результати. Та довжина r, яка схиляється до теоретичного значення I для даної мови і є нашою істинною довжиною ключа.

Таблиця наборів значень індексів відповідності,одержаних при встановленні довжини ключа шифру Віженера

2	0.033006
3	0.036199
4	0.033056
5	0.041049
6	0.036231
7	0.032992

8	0.033085
9	0.036227
10	0.041123
11	0.033071
12	0.036207
13	0.032946
14	0.032878
15	0.057419
16	0.033008
17	0.032669
18	0.036277
19	0.032663
20	0.041328
21	0.035979
22	0.033209
23	0.033279
24	0.036314
25	0.041131
26	0.033024
27	0.036379
28	0.032794
29	0.032895
30	0.057564

Із всіх значень ІС явно виділяється значення r=15. Його й берем для подальшого аналізу.

Далі треба було ділити шифрований текст на блоки із літер що містяться в ключі. Та за допомогою методів частотного ключа пробувати шукати вірний ключ, для цього треба шукати індекс літери ключа за допомогою формули різниці найчастішої літери в блоці та найчастішої літери в мові. В випадку шифрованого тексту найчастішою літерою є

‘о’. В моєму випадку не вийшло відразу отримати готовий ключ, так як це вийшов ключ - абсалютныйвгроь. І він не дешифрував текст повністю, та в дешифрованому тексті вже добре прослідковувалася реальні слова, тому прийняв рішення також зробити ключі для наступних літер по частоті - ‘е’ та ‘а’. В результаті я мав три ключі, котрі мали в собі певні літери з нашого шуканого ключа:

```
Ключ (припущення: 'о'): абсалютныйвгроь
Ключ (припущення: 'е'): йкъйфзыцдтлмщче
Ключ (припущення: 'а'): опяощмаыйчрсюьк
```

Так як у варіантах завдань використовувались змістовні ключі, то проаналізувавши ймовірні ключі та дешифрований текст першим ключем, в якому найбільше прослідковується шуканий ключ, не важко зрозуміти, що шуканий ключ - абсолютныйигрок

Шифрований текст:

псцфпгйтзъфиэцььецфюояыючхгяьытфушщиаъачйфхюмауяюужаъэънжфосацятуйффы
фклчцчгбиащяньйаыебамогсазиаюзчщррэъяндмшгйтлопфшяьенмтлрйхечклбцннбьцтж
ващвршгяьрпъяэабыющирчоытбуомщэноъъгэьмлжюоныдызмуцеьцудящхгютнйлгыофт
йиуьиарйнцпхыкбпьуррнюъарохачаистхмхсыаноюрпчжванмвнмънопщшсэаьтачфяйфдг
ючынщаркбнзсрехютлпуянмчойпнфврпнояуъочсийпррепнйцрьсцйьчхсбышсундуаъшгр
ищшцтвтцтщефыжохрюяььпгтрйоъцюнияюпдтгонждтжостюашмрбцггэфэопзэйукпюяэ
оечнчшляьфаисщцьцмзсэпхяьогэцымщсыцрлшыеегяхчмшъйъълбэшсптйщявньчъншцч
фпбълфъхсоулсйьиащщщбъчоцнзюяьурюбйбаэячфцшхкнпвеуаащолрзггшмпвоъжчъмч
хкргмаущщьмдъгфжзхчмогбучэцыжмцмбэйчлщэыгфэыырешгмсгяцаачэидэурпшвтлуцн
ашйлрргъкртсэщоасцуцхююшгпщяъмэйвчкгытхясяяэюбшйыреяуъипхящевтэйхлпбвем
иуыгщюнчщошжчиньуэачэиьуфпьлрбгыщитчэчпеаогажгякващйтйогтчыквйшнаюжомс
ыстхтыцэюяхдшцпшюэнжиокляыкчялбатлтящшгйъозщлбапмфцтнюятоцръвьригцунмф
эахзешхттбщяшмфнобновущеснбсгянкчуфюачимцалнаяйххгзохатняэотъийзлбаъащюок
ааций пгъьчогяаомэымчтехщткпъцоонаискиаяэмбвялкъщмчйсщцфооваысьяйщщхррвик
ыащкеплофиэцшдощъуеърлчтстъптбуярйчъидэехючумвнхпашияыррльоуботнаьлчщясу
сеньншаацийаорршвтпылагтрьшстыйхпгящфъазймсдцсишцяхжзьлсхщшэшввмауэзыяд
ржаьфогуььнвхисфгыцыьшцщщачдаъъеюъфалуащоштиснчгыоанцыэюэйичлсрсъетвьы
юбыкдънрбчишгьсгяхъярешщтзбзцужятвциршусаляыщаърлдщзхщклпьмпгыфыфцйэцф
анщянмъвмчйфврпномгнлеялохршгсаляыщафымшшлпатясцоцъяымырсэцчашсщупаьл
чълтщйтэвнвраоцлгйшажхпгньжэиьдулъьчешюьпюэтечхиаомньающптдглиршумогвуцг
яъозфивонамсшэжйтмурмфьцеоаюрвгяылувтжтйтяпщзасиьтохафупбсллъфзйыршрпртд
ълхеугюпгъьчогувуеъдаътсьэхаоццчгфегюклфыпуощеэмшхздэршшккйэцьнаюйкипшш
шляиухлтфэйхрлгчаддоцэюхкщррпщшнжяпыюдхздсшрюккуцюхюднмышсдощрпщхщц
эниокрххкпояурдцнжсщсыыпчосньжгяахикрюксусщлиашщатгьцбесгьъмэырйррючъебь
кшмгяглъизучижэыщбъвзощвжумппыощлъъашшитюктйьцъъфъашшсеьоинмутювымфр
гъьндбботкчэццижгохекоащбаньъцооачодяыухдыгфрнршногсюуатшгьяиэйпкгсыэмфын
чхрхщжньжбггыпыуыцьотнпъащнашймръхяфокваысьяощгхююбаъщгнатчоьфиаьонпьп
мютиймсбатгмщюлеютлчкнюяцишцяхжзыьгннвьмврсншлнвэшшсбаъаованмбшыцнхля

тсуцъжлтдыфрурхлигсазпсыисэсфыкзбхююбацмциърщкппфцмьбхношфръкявящзцтмк
фирхакспьырхяыдърфвуцыусшулчсйъълужкятгопжъфэопзлхкежыьшхъъйтхгсщидбьцч
жэшгчхюымоекюонпчвйкрхруцыцгуцюзюгъъиьймппвуцгяхъюяиыьмешцяэатаящыжшг
свжштовччыщълэоыоубньгяхъхруюхоаощнмщэниофиэупсубоглацмйшпртекпвъщтэынй
рурхчодяющвтчйъфсбакнчщчйнъяащаибамуааьщоухноксъюэгтящшфтъыытргщыяоссу
бтънътлщяъотгьхлтройуищцытбьюлефнжскгвкыяосаыжйнмырнршшбьыыщачъидснюъ
ынжфонпчрйрихацбатсэыгфэыыреицыьгэуэюяыэчмсаьоньцянивнкфнршнцигятжждпа
щмюеексущдыющщащцпюацеубопмдимиялъцхонцаымфюнщылпхекйяшюртъиднтюяь
ерцышмщнзошкрмгексачмгбащцмъщшкпгошжчэырмлаопмпфьожхниыифюэъогяфпюф
еаощвъьхотвоцъяыдъролрсрьуочжгпаыцелъттжащщанщгруцзучижэтцжэыменьхтшлдяь
плтчйшугэуьокпэурчэьдъяяуъетгоцртуаьягбажппваубэнамцфюпъаунуннапиоархъэппря
юптяощхрхэьуодюллбшоыцрхсшсрдашжьнрйшсэофтпэбночщацрццучетдзрпдпйлиоюр
чуубушлътккфирхаемббянгятлйрпхюфусщчъмгялймгыцырбуыурчшчццпхыжшжсрьиаэа
шцзюжхапиуыгцйвофошцлеигьомбыжьшгчюэшжюыщзгяйфтрюрпнйръупянюьиопътпс
яыуенпызбльцщрпваыгэхэйжьшътежюоьифыветсыйлемщерйапаанфврквлсшщздызоши
яьмеиььргбыкдъгыцыьисащоюывсъяшыкгфсщзлчэырцзаохзжэщйлчэырмуюптлоселпдх
ейтдющжшйюяэааьжйхивятсуцъжюфюамцошжжсрьмджэпжочиишэсвсгымюдыыгпшш
ъааэцтгюшъцихъыэлбвкмсьпыфдрюыксуцыюлтройуищцщржуюлръшыъдеяьоовщумжу
шатщнючщомдяягвилйпехеьоряшщэлтдъзрхыктсцгьйаъыютлвояишцюрнтвыюиррыпвй
хцчмююэошшврпреяъхмэлтофсбышвбюцухеуйтширщжнпвауйрсаттхюъэвсцърлъъыцн
мюяьагсщщпотфофрюсшдбьухмятэънкхъхяоцбьнчшгшнухяплйгкьэьъйлцпгямеущщюд
чшнчсктусджгохмхыботоряыашгьупашиянеаоысжрышмюфэопзэьцсляэцгяхгмргфйъата
ьцмштиццптяшзгцхпжъяафдщрэхаоцаювэмкошибухеощномдыэсулбэпшояцъоъщыъщст
ьуэгсшююихгчлуюъчодяшщйъдаъъерхпммрыъоахвчаоюыпмбььхюднмышсдцчетиоьря
иръуцзопвфюуьцъвзсуошьчызщхшгыыяцинюаппжбкюйрсатйюыоорффокоасгцинюашр
пъырбвывсуггексунхркэхгпркэкщрпхьцдтшыъдшюайиряыщанщвйтсэоцигвьщрфтнъъе
шцынпуйчжухйфцжшепслщъуоъязйфлаьонпцящйягааноюрпчжванюегафноюгштауяргх
ылсъплцфомцпллъмаъъибамеоюьшюваусулбкквйшщюхчъгсчспртлйвкыюятачъфгаытгд
мджчюкотхаохьомуцжяхгркичтепсятщйшнжсщехаттэжьээюъймришхчицботяъшгъдсэо
нубьцунарыъулэьшнйтйцждненио хштоушучйъднчщехатхжкуцгдтжануххщрпваыюяюн
лцжрщккущшужятьчхгфбыппыьуактдъзтхюпсусрггыплйбгвкыяйхрубтячъзеюшъудвьцл
инжсхкючсеньцэгюъафцтюяьерцышмбызошивьнолсшюкъэыфрогетзгцхпнвнэнитхюпс
жьцнцчтмияиыьмешцяэаапгннхмльодяыркаржчщепхжсвмрггыэйнррючщотьуыющэобн
ршныитгучщютнщцпуышвжюыщбаялйхфяьътбаюлидхтощншэъесуоцюгйэчкфпшшмть
бвючсжийсыквиованюэляосрръчодщуьмдъгфнхгдплжужугщтзфзрхьытбьцьъбэанцфвом
лжюыжкъюыхрфхппнбваюнъшзсшчгыоанцыэюэйидсгуюпстяюяюхяйощхмьоиощхубв
ыечкфгъпвщщчуеютисъядцсишцяхжчфыуцрляэщжванмфнисзпхакгбьохръдаътсуьоонц
ылаьынчшсьфтлйьмпжбыесхцыуноюгцчжхэйуцпюшкзбьякиаъмышцъашррщалакхдушс
фбяоняялнътиъхизашвсятрпнъйлхищэъииюоэгэйичщхшьчсецщлйгпйтэсфхккпюеуакхд
лцмэбчаддоцжбымынтхычорбухотягфруряьифууцжйхэйъябнмовлучгбэйъъурыытгярыг
юмкошибаклпйоэюдймичсфыктйвшщкйабсэкршшнпушщпюымьщтюшшимвншмйтлоп
рхшштпбьравтзиубфцэцжьунцъткчщохшктбваымжиийпиьщпимщсргаоийшцццхитгуш
иъыющиршетвбпзугйнмыдпхакгбьохръчгуцхююкявмщлнаплоозхыквуяюсгяхахьгуоыт
жюшумуэырцерщтнжиащавыяотсыьысбькшмхыыукгацэмбуыюрвхечъсаьнопыотюэнме

ржрщккущшлпгхмынпючыомсшлиянвлиошхмеихбтююткыгмыомюдрнвыьсъябныкгя
хзлъвийшццбмгмдпулнсйхнррщидаэырсцнжчщяррыкпбущлъьащнфвохиптюлчтячцифв
учкйуыуктъгопгэньыжающяэтзчселфтвбюцкфъпгфркрдтимщжзнарлйхкряьагмонраъйх
хюхэшчущырлеуяйжьшуыягвыляштисрфвочцйщящецницгияьнрбюяцсшойтяиыьмешця
эаттфокстюпмжюонмыъцъьгуьцпсятщйшнжсхибатсгямьйеуььхгсщидбгктюъфзохлтжтм
тршщпюымчфлуюкнйзочжтчэйшлгъкппьбвжфеамцррхмаощухмгщйщрцьышовщалрчш
гшцжаочзбвалацтжйулнашнжягщряывйягбаэюоцржнашиизеюххозцышщчъыцршюпйзб
юыщпдхкщцфвьтсрящзеемонцдэйпдпвалрадичтсьвшруспрйоъцощхрыаийушлхчюнлнс
сйфнпуушларйпромньалячьююымыцввухьоячэгзъганфъьусйваркацьдугшэшгссытюгяы
лифюшшлосшцраэйтчуюфтвбьоьгюйъшцжаочишюцхмфдаыкиаьцузицшждэгпнрйцчы
йжрлуднийягыоыьгвуомбыжмцзрыкзбхцшюушщнихмхквтцщрляыдсфийучеосяхсйхжчр
ывркнлсюлмйъофщвюыытпрщъмгэанркрщквйшцшбтьймшгэхксусржнвтяъъгтщйвщцс
щпаойтхисьхьщячъоафлйярлчфурящьхчэидфтющшмйыохетпйщцйхычыквъщрвтжцизт
уйрлщутачфядккхыттжаьамшхациъмцьогюцчюдтжехюхсхаисэщбвнирифвоматяшщйвн
мшцорсклбвкшгфюйънзэуустящщкщпармрючыитгучгъсыпнрхрыотцтшгырыфинвцфет
ууэмдющнизюптрбьякянсймнляьхтпбочжэшгйшзрщптрялэмюаисцнршшмиюохмюызщ
рфгыфетяхнгщсгтшизкчещьоьртъссжфвюшимщылпбанцрнхыпбпькгмыуафъсщхмеихй
мгщпйнхсьцлеисачмгбащхсьгштаяыужютжритряелэхоуетщащпышгнаиярьжэнниоибатн
боащзюнжчстыочеуыуьмгяылувыохищнтрпсяозмсымсенюьфхдыиомсбаквмрщщлчьлсз
хэйяоъдзрлъцйкрхраплаэяэюяггскргаъиляащоацкчмзхюригсщлпоъйщфгыкчаавццюдмб
ощхшхмеихонлтюнчзьшчцонцыэпьэцлиоряжппхэщйащэсплэскиюгьъмщпйфзоюртджгк
поергопеххоылящухчюнлцнюашрьжбчгяйуйусбкыкбчтжкйнмчфлбапнлдшщпюылсыпр
юкзецщкакащлрзшъейляячмгъынкизоытйюьрпэхоаноюрпкбяаьйапыъъиэомоиюцхюэнй
шшифухеоюокюгюйяргжцйвьшйнюржыиктръйтйяпыющчгщчлзышйлсърляыдсулфуъег
рышмыюнохювьытжюшлиаюзчшлгъкбпькггбырчмлыочаицъшмчюалнуэьпсйрыугяньо
щнюыпчодмнмэыецрфвбивфсщзпаяейхргмтзвссымфымлнхпзтхтрэлсдхичтлццхолщшле
тшыъдрхыкджчыщззэоштсщээшйващзбыжьчуюхъашюьфйчреччухьоомщъщзянмйфсьф
пджьуъоаогыдихэъоощшшсдймуксчкытжюшюахшокррлтшмжюошггщймхлюттницъш
мычйщидыкмтпэеупэтгркичтшлжгйьрваицгштцоогщгъоаюнчкютьъашщрлйаыьщихэьы
лпуыщпдтиуизхчытгщарйоъйкгорьонпващоаъиостюрпрцюььролейттауоппььсжэхоанру
пщжвьэлъшаыхгчоонжбулбъэйлиорьчайюоилчэюоълзуыкпцрщецтдъъешутлпыоцъяыас
ппхыпнйцащнашймрлтофуфэошгхыэчшвгфповяююдъхкччуюзпспштлляызцисбышвжа
юукчъацрвяббкпуелпдхслгфюштхююуыбъцгъроюрехрящрзгяацтлъьымпбцюктыейпгыц
ыьбтящйряидфтаущяуванжчщтыцвбышулсхжатшйцилеэъееюотлтдацричофарвбцжвыэй
ъяяьмржчтрляащцижгохянщелпдйзоъгуохалгцвггчймцзюъпнбщырнежыыдкрюкзфибсж
зфыуцрюрсажцэыгцтждлзхлфсрсыьжсхичсухохьояяэжяткщрссюплбцзрктюуыидюрхеус
щзларйсщшютк

Розшифрований текст:

преждечемсменитьдежурногонапостувкоконеобсерваториионвсегдазаходилвзалвизинга
чтобыпочувствоватькосмоснапрямуюнечерезсистемыдатчиковисигнализирующихустро
йствпогранзаставабылаустановленавэтомглухомуголкеметагалактическогодоменаболее
тысячилетназадкогдачеловечестворасселялосьпозвездамбурнымитемпамииверіловсвое
божественноепредназначениевсудьбоносностьцивилизациииивседозволенностьотдельны
хеепредставителейпотомпришелзвездныйконструкторипоказаллюдямихместовмирозда
нииныевозможностиспособыобработкиинформациицелибытияилогикунедоступнуюго
рдомуизаносчивомувидухомосапиенсонзахватилсотнилюдейвовремядолгойспячкипрев
ративихвсвоихверныхрабовсъелполовинумарсапородыкоторогоиспользовалдляростапл
отивпериодсозреванияушелчерезстослишнимлетвернулсяобратнокаквозвращаетсядомо
йблудныйсынпоследолгихскитанийпомирунечаяннопочистилсолнечнуюсистемуедване
уничтоживеевовремявизитаисноваушелтеперьуженаполсотнилетапотомначалась странн
аяистрашнаявойназаконовотголосоквеликойигрыуниверсумассамимсобойиконструктор
ставшийктомувремениоднимизигроковметавселенныхвернулсяксолнцунаэтотразпопрос
ьбеземлянвойнашлавовсюнавсехуровняхотсоциумадофизическихпринциповбытияходы
игроковвоспринималисьчеловечествомкаквторжениефундаментальногоагрессорапопыт
кауничтоженияцивилизациииинезнаниезаконовигрысделалолюдейзаложникамисвоихсоб
ственныхвнутреннихзаконоввосприятияреальностиониначалисопротивлятьсячтобывы
житьхотясилыбыликонечнодалеконеравныпросачиваниевовселеннуюметагалактически
йдоменпредставлявшийсобойоднуклеткуорганизмауниверсумачужихзаконоввфизическ
омпланеимевшихвиднеуничтожимыхникакимиспособамиколючекназванныхнагуалями
принялонеобратимыйхарактеркатастрофапроизошланевнезапноеждалисолнечнаясисте
мазарасталаколючкамичертополохаинойреальностивтечениемногихмесяцевпокаонинеп
ревратилисьвнепроходимыезарослиакогдаразмерынагуалейэтогоабсолютногоничтоили
какговаривалиученыеквантовотоннельныхушейвакуумаинойтопологическойструктурыт
орчащихввакуумеродногодоменадостиглиразмеровкосмическихобъектоввпаянныхвпро
странствопланетысистемыначалиразбиватьсяониходназадругойсначалапогибюпитерса
маябольшаяпланетасолнечнойсистемытакинедостигшаястадиизвездызаеекончинойнабл
юдалимиллионылюдейнавсехобитаемыхтелахсистемывпоселенияхчеловечестваудругих
звездгдекартинасотрясениямирозданиябыланеменееестрашнойсармадыкосмофлотаиразн
огородакосмостанцийюпитершествуяпоорбитевокругсолнцанаткнулсянагигантскийсро
стокнагуалейисталразваливатьсянатричастикакобыкновенныйкомснегавсегозатричасап
ревратившисьвметановодородныесвкрапленияміводыитвердыхчастицразмеромотметра
дотысячикилометровструиязыкиокутанныепостепеннозамерзающейатмосферойклокот
аниераздираемогогигантасопровождавшеесяколоссальнойсилывзрывамисветовымитеп
ловымизлучениемдлилосьещедолгооднакопланетойюпитербытьпересталтажеучастьпос
тиглаегособратьевповнешнемупоясусатурннептунуранплутонегоспутникахаронактомув
ремениуженесуществоваловнутренниепланетымарсвенераимеркурийпострадалисравни
тельноменьшеавскореподошлаочередьземлиибезтогополуразрушеннойстолкновениями
снагуалямипронизывающимипростреливающимиеенасквозьколыбеличеловечествавкак
ойтомереповезлоеепопытались ьзатормозитьинагуальнеразодралземлюнераздробилначас
тикакбольшинствопланетсистемыавсеголишьсплющилвлепешкусбахромчатымикраями

землянаткнулась буквальнонастенунагуалейипревратилась вподобиебиблейскойполусфе
рыразвечтопокоящейсяненатрехслонахкитахичерепахахананевидимомсверхтвердомкол
ючемоснованиичужойреальностилюдейктомувременинанейоставалосьещемногодалеко
невсеземлянеуспелипереселитьсякновомусветилужелтойзвездетакогожеклассачтоисолн
цеврассеянномзвездномскоплениигиадырасположенномвсозвездиительцапланетудляпе
реселенияготовилиспешноипримассовойэвакуацииогромногоколичестваземлянпроизо
шлонемалокатастрофинесчастныхслучаевунесшихмиллионыжизнейоднакотеперьулюде
йбыладругаяродинакоторойнегрозилаучастьземлиижизньпродолжалась хотяипоновымза
конамивсоответствииснovымибиологическимиритмамиродноесолнцечеловечестваупел
елохотявсеегоритмыиколебанияестественнонарушилисьавизлученииповилисьранееотс
утствующиеспектральныелинииизвездыпродолжалисветитьхотямногиеизнихразбилисьо
нагуалиипогаслиноонибылитакдалекиотземличтосветихещелетелчерезпространствогал
актикиинебонадуспокоившейсяпереставшейвращатьсяидвигатьсявокругсолнцалинзойз
емлитемнелопостепеннопомеретогокакумиралилучизвездправдапереселившеесячелове
чествовидетьэтогонемоглосвязьсбывшейродинойпослеразрушениясистемыметромгнов
енноготранспортапрактическипрервалась вовсякомслучаедлябольшинствалюдейнамног
иесотнилетуцелевшиеземлянеостались предоставленнымисамисебенаступилмирфундам
ентальныйагрессорфагтоестьодинизигроковсумевшийизменитьфизическиезаконысуще
ствованияметагалактическогодоменавкоторомжилилюдипокинулегоэтимигрокомоказал
сяконструкторпитавшийкродухомосапиенснечтовродесыновнейпризнательностионсдел
алсвойходзакончившийвойнунагуалипостепеннопрекратилирастиуувеличиватьсявобъем
епространствовремяпересталошататьсяподнатискомчужихзаконовкосмосуспокоилсяно
черезнекотороевремялюдиуцелевшиепослекатастрофыназемлеилигееобнаружилистенк
иограничивающиечастьметагалактикикоторая былаповрежденавторжениемфагастенкио
бразовалинечтовродеколоссальногоаквариумавнутрикоторогооказалась игалактикассист
емойсолакакназвализвездузаменившуюсолнцепробитьсясквозьнихнаружувглубиныдом
еналюдямнеудалось авскореонипересталиобращатьнастенкивниманиезанятыепроблемо
йвыживанияцивилизациилишьпогранзаставыавтономныепочтиненуждающиесявснабже
ниистанциисозданныепогранслужбойчеловечествающевовременавойнысфагомпродолж
алинестисвоюслужбунаблюдатьзаизменившимсякосмосомиграницамиаквариумаполучи
вшегоназваниекосмориумнообитателипогранзаставделалиэтонеохотнозачастуюневыпо
лняявозложенныенанихобязанностипростоиспользуяудобныедостаточнокомфортабельн
ыестанцииивкачествеобыкновенногожильятакойсамостоятельнойтехническойсистемойб
ылаипогранзаставасоколнакоторойпроживалась емьяпограничниковчетверомужчинитри
женщиныихвахтаначалась всегополгоданазадинаблюдатьзавселеннойимещененаскучил
оиштванкараочнулсяонстоялпосредизалавизингапогранзаставыпредставлявшегособойн
ебольшойпрозрачныйкуполсчернымполомикаквароженныйсмотрелнадвеяркиезвезды
взенитепохожиеначьитовнимательныеглазапогранзаставасоколрасполагалась невсоседн
ейссоломзвезднойсистемеидаженевсоседнейгалактикесветотсюдадобиралсябыдогеипол
торамиллиардалетпоэтомуниокакомзнакомомрисункесозвездийречьнешластанциюстро
илинаспутникенебольшойжелтойзвездыбезводномибезатмосферномхотяониимелзапасы
льдаизамерзшихгазовсилатяжестинаэтоймалойпланеткесоставлялалишьдесятуюдолюзе
мнойчтонедоставлялонеприятныхощущенийобитателямстанцииивнутрикоторойподдерж
ивалась нормальнаясилатяжестизвездавнастоящиймоментскрывалась подполомвизингаи

этопозволяловидетьдругиезвездыколичествокоторыхуменьшалосьскаждымчасомистенк укосмориумаразделявшуювидимыйкосмоснадвечастиноеслиучеловекаотсловастенавоз никалаопределеннаяассоциациявызывающаявпамятиобразкирпичнойкаменнойилидере вянной стены тостенкакосмориумабольшепоходиланаземноесеверноесиянienабесконечн уюволокнистуювуальсотканнуюизбагровосветящихсяпаутинокижилокиказаласьненаде жнойхрупкойпушистойполупрозрачнойлегкопреодолимойнасамомжеделепробитьеепро никнутьсквозьстенкувглубиныдоменанесмогниодинземнойкорабльвтомчислеизвездоле тыструнныхвидовихпростовыворачивалообратнословностенкадействительнобылаодно стороннейповерхностьюкакпредположилиученыеещесотнилетназаднереагировалаонаи наэнергетическоевоздействиеилокальноеизменениетопологиивакууманеговоряужеобор ужиипопрощесозданномнаосновеприменения пучковчастицвысокихэнергийисиловыхпо лейстенкикосмориумаоказалисьабсолютнымпрепятствиемчтоясноуказывалонаихпредн азначениезакапсулироватьповрежденнуюнагуалямичастьметагалактическогодоменаине пущатьзаразучужихзаконовзаеепределыгдеэкспансияинойреальностинеприобрелаещем асштабовлетального исхода

Висновки:

У ході роботи було підтверджено, що шифр Віженера ефективно розмиває статистичні властивості природної мови. Індекс відповідності для вихідного українського тексту був високим, тоді як ІС для всіх отриманих шифртекстів впав до рівня 1/m.

Також було проведено успішний криптоаналіз шифртексту з його розшифруванням. За допомогою методу індексу відповідності було знайдено ймовірну довжину ключа 15, оскільки на цьому значенні(та кратному йому r=30) спостерігався різкий пік ІС. Частотний аналіз 15 блоків дав ключ-кандидат (абсалютныйвгроь), який при дешифруванні дав частково читабельний, але недокінця розшифрований текст, та шляхом аналізу, порівнюючи із іншими ключами та дешифрованим текстом, ключ було скориговано, що дозволило повністю розшифрувати повідомлення.

Як підсумок лабораторна робота довела, що шифр Віженера вразливий до статистичних атак, які дозволяють спочатку знайти довжину ключа, а потім, комбінуючи автоматичний та ручний аналіз, відновити сам ключ.