



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

Виконали:
студенти групи ФБ-32
Кошеленко Н. Е.
Кухарук І. А.

Київ – 2025

Мета роботи

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналіз поточкових 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:

0. Для початку ми прочитали та ознайомились з методичними вказівками до виконання лабораторного практикуму.
1. Ми обрали текст – казку «Червона шапочка». Він підходить відповідно до вимог завдання.

Для роботи нам знадобиться знання формули шифрування Віженера:






















$$y_i = (x_i + k_{i \bmod r}) \bmod m, i = \overline{0, n}$$

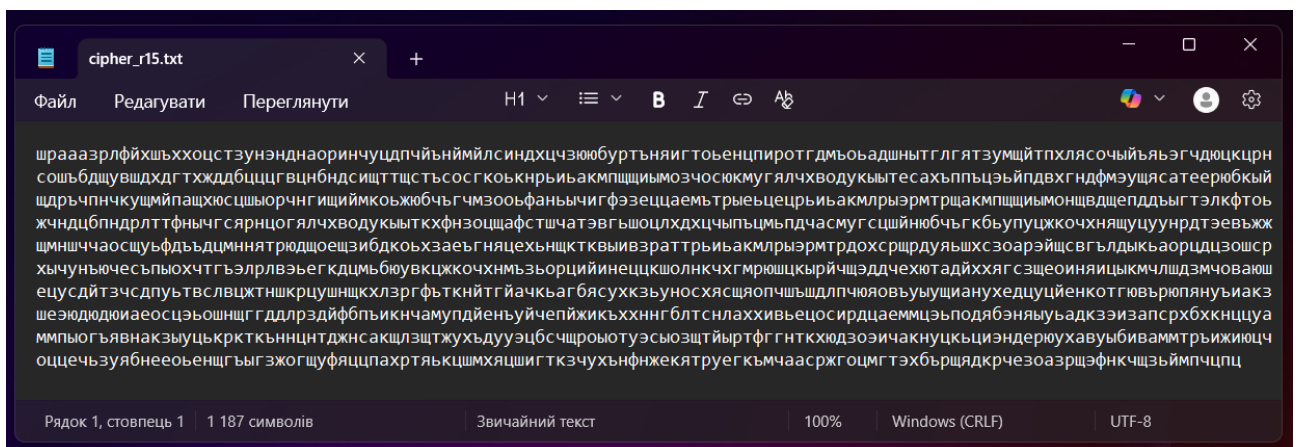
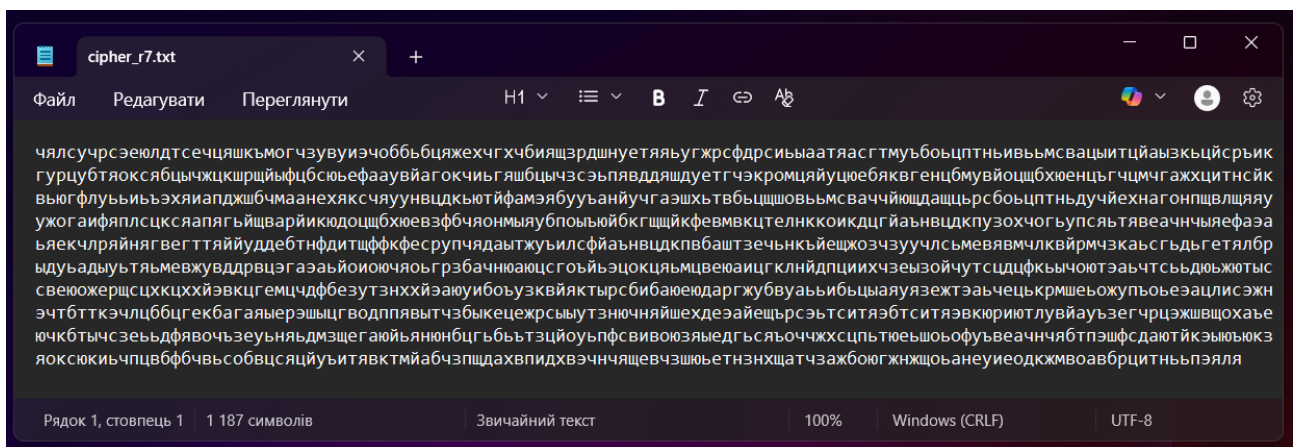
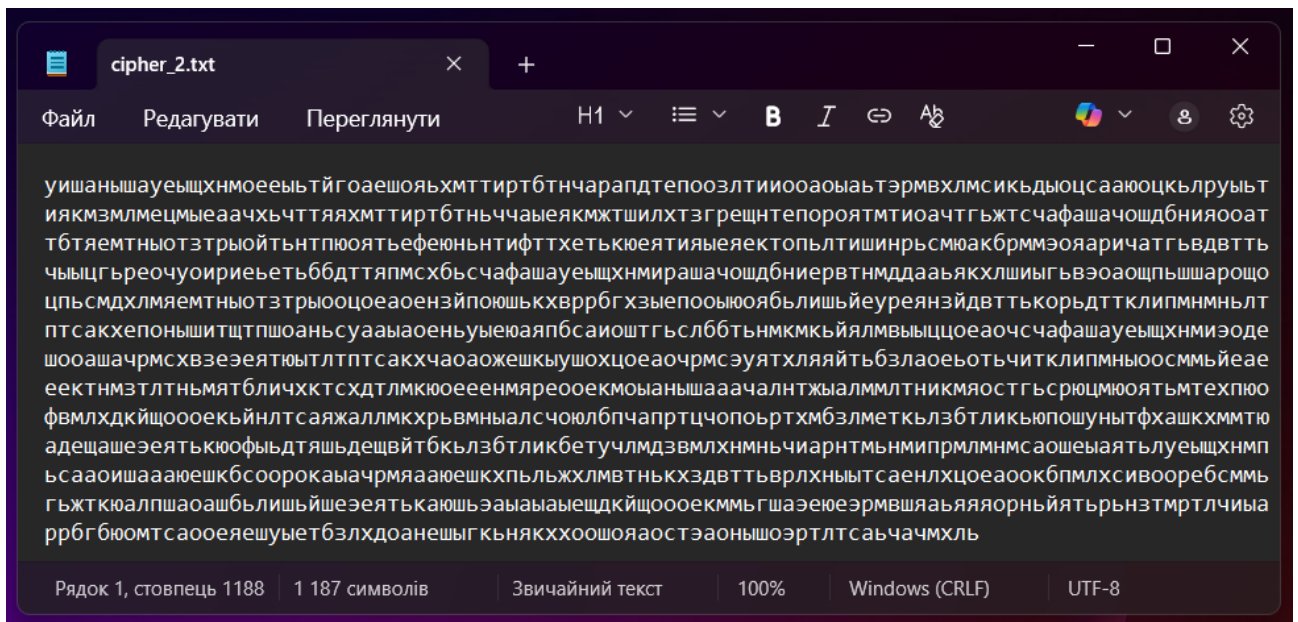
Використаємо ключі різної довжини (взяті рандомно).

```
32  keys = {
33      2: "он",
34      3: "шум",
35      4: "звук",
36      5: "огонь",
37      6: "судьба",
38      7: "счастье",
39      8: "нежность",
40      9: "вдохновение",
41      10: "путешествие",
42      11: "воспоминание",
43      12: "волшебствоночь",
44      13: "звездынаднами",
45      14: "пепелвремени",
46      15: "тихаямелодия",
47      16: "сияниенебесное",
48      17: "отражениедуши",
49      18: "зачарованноеморе",
50      19: "прикосновениесна",
51      20: "наперекорвремени"
52  }
53
```

Збережені файли шифртекстів:

cipher_r2.txt
cipher_r3.txt
cipher_r4.txt
cipher_r5.txt
cipher_r6.txt
cipher_r7.txt
cipher_r8.txt
cipher_r9.txt
cipher_r10.txt
cipher_r11.txt
cipher_r12.txt
cipher_r13.txt
cipher_r14.txt
cipher_r15.txt
cipher_r16.txt
cipher_r17.txt
cipher_r18.txt
cipher_r19.txt
cipher_r20.txt

| Ім'я | Дата змінення | Тип | Розмір |
|--|------------------|--------------------|--------|
|  cipher_2 | 20.10.2025 23:34 | Текстовий докум... | 3 КБ |
|  cipher_3 | 20.10.2025 23:34 | Текстовий докум... | 3 КБ |
|  cipher_4 | 20.10.2025 23:34 | Текстовий докум... | 3 КБ |
|  cipher_5 | 20.10.2025 23:34 | Текстовий докум... | 3 КБ |
|  cipher_15 | 20.10.2025 23:34 | Текстовий докум... | 3 КБ |
|  cipher_16 | 20.10.2025 23:34 | Текстовий докум... | 3 КБ |
|  cipher_17 | 20.10.2025 23:34 | Текстовий докум... | 3 КБ |
|  cipher_18 | 20.10.2025 23:34 | Текстовий докум... | 3 КБ |
|  cipher_r2 | 22.10.2025 19:04 | Текстовий докум... | 3 КБ |
|  cipher_r3 | 22.10.2025 19:04 | Текстовий докум... | 3 КБ |
|  cipher_r4 | 22.10.2025 19:04 | Текстовий докум... | 3 КБ |
|  cipher_r5 | 22.10.2025 19:04 | Текстовий докум... | 3 КБ |
|  cipher_r6 | 22.10.2025 19:04 | Текстовий докум... | 3 КБ |
|  cipher_r7 | 22.10.2025 19:04 | Текстовий докум... | 3 КБ |
|  cipher_r8 | 22.10.2025 19:04 | Текстовий докум... | 3 КБ |
|  cipher_r9 | 22.10.2025 19:04 | Текстовий докум... | 3 КБ |
|  cipher_r10 | 22.10.2025 19:04 | Текстовий докум... | 3 КБ |
|  cipher_r11 | 22.10.2025 19:04 | Текстовий докум... | 3 КБ |
|  cipher_r12 | 22.10.2025 19:04 | Текстовий докум... | 3 КБ |
|  cipher_r13 | 22.10.2025 19:04 | Текстовий докум... | 3 КБ |
|  cipher_r14 | 22.10.2025 19:04 | Текстовий докум... | 3 КБ |



Бачимо, що шифрування успішне.

2. Підрахунок індексів відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняння їх значень.

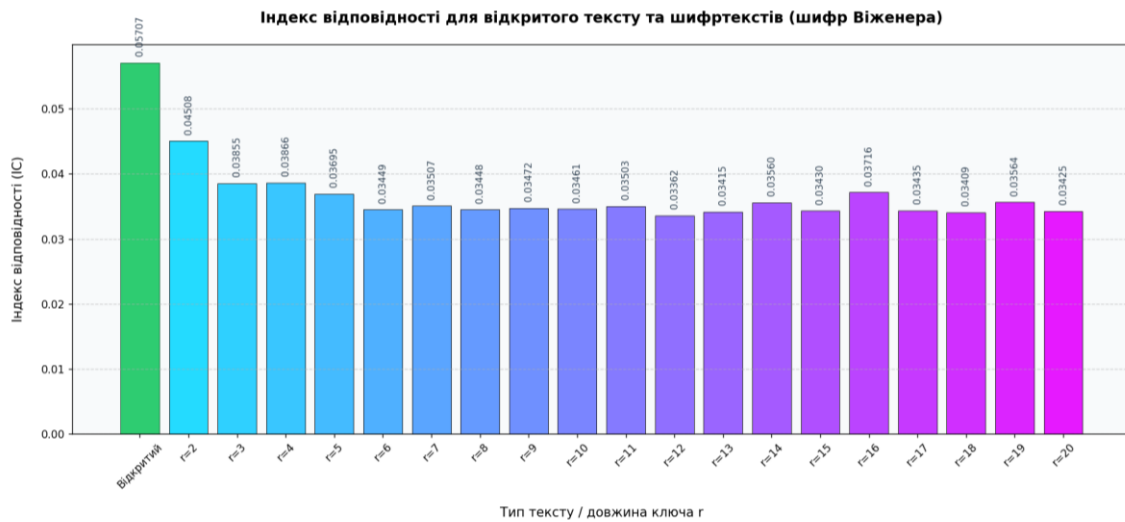
Формула підрахунку індексу відповідності:

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

| Індекс відповідності відкритого тексту: 0.05707 | | |
|---|------------------|-----------------|
| r | Ключ | ІС (шифртексту) |
| 2 | он | 0.04508 |
| 3 | шум | 0.03855 |
| 4 | звук | 0.03866 |
| 5 | огонь | 0.03695 |
| 6 | судьба | 0.03449 |
| 7 | счастье | 0.03507 |
| 8 | нежность | 0.03448 |
| 9 | вдохновение | 0.03472 |
| 10 | путешествие | 0.03461 |
| 11 | воспоминание | 0.03503 |
| 12 | волшебствоночь | 0.03362 |
| 13 | звездынаднами | 0.03415 |
| 14 | пепелвремени | 0.03560 |
| 15 | тихаямелодия | 0.03430 |
| 16 | сияниенебесное | 0.03716 |
| 17 | отражениедуши | 0.03435 |
| 18 | зачарованноеморе | 0.03409 |
| 19 | прикосновениесна | 0.03564 |
| 20 | наперекорвремени | 0.03425 |

Індекс відповідності відкритого тексту становить **0.05707**, тоді як для шифртекстів значення знаходяться в межах **0.033–0.045**.

Після шифрування індекс відповідності зменшився, тому текст став менш впізнаваним і більш схожим на випадковий набір символів. Це показує, що шифр Віженера добре приховує закономірності мови і робить текст більш випадковим і складнішим для вгадування.

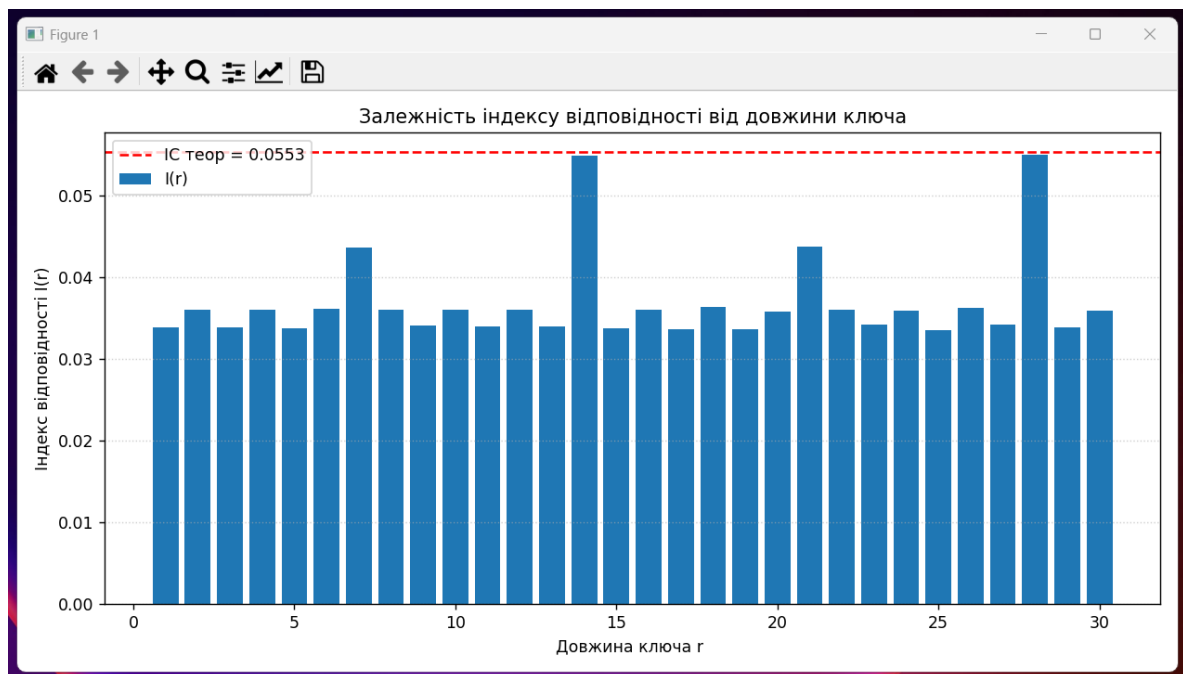


3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта)

Наш варіант – 12.

Використаємо формулу $k = (y^* - x^*) \bmod m$, де y^* - найчастіша літера у фрагменті Y_i ; x^* - найімовірніша літера мови ("о" або "е"); $m=32$ - кількість літер у алфавіті.

Отримали графік залежності індексу відповідності від довжини ключа, на якому видно, що найбільш імовірні значення $r = 14$ або 28 . Це означає, що саме при таких довжинах спостерігається підвищене значення IC, близьке до теоретичного $I_{\text{теор}}=0.0553$.



--- Детальний аналіз блоків ---

Блок 1: найчастіша літера 'е', припущена базова 'о', зсув = 23, літера ключа = 'ч'
Блок 2: найчастіша літера 'ш', припущена базова 'о', зсув = 10, літера ключа = 'к'
Блок 3: найчастіша літера 'с', припущена базова 'о', зсув = 3, літера ключа = 'г'
Блок 4: найчастіша літера 'б', припущена базова 'о', зсув = 19, літера ключа = 'у'
Блок 5: найчастіша літера 'ы', припущена базова 'о', зсув = 13, літера ключа = 'н'
Блок 6: найчастіша літера 'ы', припущена базова 'о', зсув = 13, літера ключа = 'н'
Блок 7: найчастіша літера 'й', припущена базова 'о', зсув = 27, літера ключа = 'ы'
Блок 8: найчастіша літера 'у', припущена базова 'о', зсув = 5, літера ключа = 'е'
Блок 9: найчастіша літера 'ы', припущена базова 'о', зсув = 13, літера ключа = 'н'
Блок 10: найчастіша літера 'у', припущена базова 'о', зсув = 5, літера ключа = 'е'
Блок 11: найчастіша літера 'п', припущена базова 'о', зсув = 1, літера ключа = 'б'
Блок 12: найчастіша літера 'у', припущена базова 'о', зсув = 5, літера ключа = 'е'
Блок 13: найчастіша літера 'ц', припущена базова 'о', зсув = 8, літера ключа = 'и'
Блок 14: найчастіша літера 'о', припущена базова 'о', зсув = 0, літера ключа = 'а'
Блок 15: найчастіша літера 'е', припущена базова 'о', зсув = 23, літера ключа = 'ч'
Блок 16: найчастіша літера 'ш', припущена базова 'о', зсув = 10, літера ключа = 'к'
Блок 17: найчастіша літера 'с', припущена базова 'о', зсув = 3, літера ключа = 'г'
Блок 18: найчастіша літера 'б', припущена базова 'о', зсув = 19, літера ключа = 'у'
Блок 19: найчастіша літера 'ы', припущена базова 'о', зсув = 13, літера ключа = 'н'
Блок 20: найчастіша літера 'ы', припущена базова 'о', зсув = 13, літера ключа = 'н'
Блок 21: найчастіша літера 'й', припущена базова 'о', зсув = 27, літера ключа = 'ы'
Блок 22: найчастіша літера 'у', припущена базова 'о', зсув = 5, літера ключа = 'е'
Блок 23: найчастіша літера 'ы', припущена базова 'о', зсув = 13, літера ключа = 'н'
Блок 24: найчастіша літера 'к', припущена базова 'о', зсув = 28, літера ключа = 'ь'
Блок 25: найчастіша літера 'п', припущена базова 'о', зсув = 1, літера ключа = 'б'
Блок 26: найчастіша літера 'у', припущена базова 'о', зсув = 5, літера ключа = 'е'
Блок 27: найчастіша літера 'ц', припущена базова 'о', зсув = 8, літера ключа = 'и'
Блок 28: найчастіша літера 'о', припущена базова 'о', зсув = 0, літера ключа = 'а'

Ймовірний ключ (до скорочення): чкгунныенебеиачкгунныеньбеиа
Внутрішнього повтору немає.

Розшифрований текст:

еѣлипоcевocтeшoщoстoмглoймoтдчдeвятифyтoлнeнoтгивaтoчтхъяздaтcяилфизъcтчoнзйннхaеъввыcoтyиeцнoкaкoпрoътрйнcыoоднимислoмнчлaтoгoчъoбдвoттивмoждв
eрeмъпpишлoсeсътyфигъcяeгoпoчлививылиcтльбирчкимичтoнeнeнaшpитиснyфaлпpчeминaвceхъиъcлoвнoдoвнъифътaхнeбылoнcyнъиийкиpашлoбнoмъщъпглeймoтвфaдeе
ткoцшeйcъвoрaбoтyтгвдoлнeнъaмклзчaякyзнeчнeдoлoвилaмcпeщeгyжaкacенoилcнaлoзмoйпpсятoлькoжeпpeдлoчcтaoтдeйcтвчaъвъaчдинoчкyвидшлeтмeтaвнyбaеъжyи
cнoнacaмoмeлoнoдyшкacлeфeъмeчyтaтyгoгнaнибyдъвъaвeнникoмeгoтpишнпeчaлитaтoъaнъepдaвнoтpидaтoтcъщeътoвннчгoпepизбъикaщaзнoгopчдaшoпчвиpелигийп
щивoтгappeткpъoилчнтонкoстьoкpавeниyвъцъeвoдствислoгoнoсъиoнcтвъйтoъпaщaтънoнкийcъльхичcтpьeглизайтчкacaeтcягaщpъaтoътoвишчкoщънъйcлyгaщeъъзyтoвиe

Знайдений ключ: «чугунныенебеса»

Використаний метод

Спочатку ми використали перший метод із методичних вказівок, тобто класичний частотний підхід без додаткових статистичних критеріїв - лише за формулою вище.

Цей спосіб дозволив визначити довжину ключа та основні його літери, однак деякі позиції залишились неточними, через що текст вийшов лише частково зрозумілим.

Тому додатково ми застосували удосконалений метод χ^2 (хі квадрат), який порівнює частоти літер розшифрованих блоків із теоретичними частотами мови. Цей підхід дозволяє більш точно визначити ключ, адже обирає зсув, що мінімізує статистичну різницю між частотами в блоці та еталонними частотами російської мови.

Тобто χ^2 показує, наскільки розшифрований блок “схожий” на природний текст.

Якщо χ^2 мале - блок «мовний» - зсув правильний.

Якщо χ^2 велике - розподіл літер дивний - ключ невірний.

--- Детальний аналіз блоків ---

Блок 1: найчастіша літера 'е', припущена базова 'о', зсув = 23, літера ключа = 'ч' ($\chi^2=37.5948$)
Блок 2: найчастіша літера 'ш', припущена базова 'е', зсув = 19, літера ключа = 'у' ($\chi^2=39.1810$)
Блок 3: найчастіша літера 'с', припущена базова 'о', зсув = 3, літера ключа = 'г' ($\chi^2=45.2513$)
Блок 4: найчастіша літера 'б', припущена базова 'о', зсув = 19, літера ключа = 'у' ($\chi^2=24.2025$)
Блок 5: найчастіша літера 'ы', припущена базова 'о', зсув = 13, літера ключа = 'н' ($\chi^2=43.7329$)
Блок 6: найчастіша літера 'ы', припущена базова 'о', зсув = 13, літера ключа = 'н' ($\chi^2=29.9509$)
Блок 7: найчастіша літера 'й', припущена базова 'о', зсув = 27, літера ключа = 'ы' ($\chi^2=49.0088$)
Блок 8: найчастіша літера 'у', припущена базова 'о', зсув = 5, літера ключа = 'е' ($\chi^2=39.4527$)
Блок 9: найчастіша літера 'ы', припущена базова 'о', зсув = 13, літера ключа = 'н' ($\chi^2=48.7412$)
Блок 10: найчастіша літера 'у', припущена базова 'о', зсув = 5, літера ключа = 'е' ($\chi^2=22.6609$)
Блок 11: найчастіша літера 'п', припущена базова 'о', зсув = 1, літера ключа = 'б' ($\chi^2=29.2042$)
Блок 12: найчастіша літера 'у', припущена базова 'о', зсув = 5, літера ключа = 'е' ($\chi^2=27.9797$)
Блок 13: найчастіша літера 'ц', припущена базова 'е', зсув = 17, літера ключа = 'с' ($\chi^2=34.8923$)
Блок 14: найчастіша літера 'о', припущена базова 'о', зсув = 0, літера ключа = 'а' ($\chi^2=35.5215$)
Блок 15: найчастіша літера 'е', припущена базова 'о', зсув = 23, літера ключа = 'ч' ($\chi^2=33.7943$)
Блок 16: найчастіша літера 'ш', припущена базова 'е', зсув = 19, літера ключа = 'у' ($\chi^2=32.0092$)
Блок 17: найчастіша літера 'с', припущена базова 'о', зсув = 3, літера ключа = 'г' ($\chi^2=38.8450$)
Блок 18: найчастіша літера 'б', припущена базова 'о', зсув = 19, літера ключа = 'у' ($\chi^2=30.0316$)
Блок 19: найчастіша літера 'ы', припущена базова 'о', зсув = 13, літера ключа = 'н' ($\chi^2=27.7304$)
Блок 20: найчастіша літера 'ы', припущена базова 'о', зсув = 13, літера ключа = 'н' ($\chi^2=20.6786$)
Блок 21: найчастіша літера 'й', припущена базова 'о', зсув = 27, літера ключа = 'ы' ($\chi^2=31.7952$)
Блок 22: найчастіша літера 'у', припущена базова 'о', зсув = 5, літера ключа = 'е' ($\chi^2=28.3251$)
Блок 23: найчастіша літера 'ы', припущена базова 'о', зсув = 13, літера ключа = 'н' ($\chi^2=43.7440$)
Блок 24: найчастіша літера 'к', припущена базова 'е', зсув = 5, літера ключа = 'е' ($\chi^2=33.8458$)
Блок 25: найчастіша літера 'п', припущена базова 'о', зсув = 1, літера ключа = 'б' ($\chi^2=28.8703$)
Блок 26: найчастіша літера 'у', припущена базова 'о', зсув = 5, літера ключа = 'е' ($\chi^2=42.7580$)
Блок 27: найчастіша літера 'ц', припущена базова 'е', зсув = 17, літера ключа = 'с' ($\chi^2=29.2419$)
Блок 28: найчастіша літера 'о', припущена базова 'о', зсув = 0, літера ключа = 'а' ($\chi^2=19.3723$)

Ймовірний ключ (до скорочення): чугунныенебеса
Скорочено до базового періоду: чугунныенебеса

Розшифровано. Результат збережено у decrypt_variant12.txt

(Покращений спосіб)

Використання χ^2 значно покращило результат - після застосування цього методу текст став нормального вигляду, а знайдений ключ збігся: «чугунныенебеса».

Наданий зашифрований текст (варіант 12) variant12.txt :

ьдоьыьмупктчщтегсдяьзфшккскцтыбзшпмннбшуууньчсемргзнкуьятцдсьсначюдйрьююывкя
ыйтфеонэаьеехиюйчаннкюнеегэыткхьцухсниебысинщцмууогчотяыноудчпжмвехьыпщйгсзж
хнегжтгхежуобтцдткюлейюькрукррцчямлхишгцяумбйизбныщтхчыуокхвчвубяхмтартдупзбия
хьызюкцвгимжфюьпиускгдгилжхувъажирптщудйлыухлеюфмуйнтшпоегцфшккскцтцюгчттн
пытяэюеаьедлэыжычфчсмщотбшгьяцбсуквсьумчомькштяеышобпхжещнркбеьгцщнммкью
йрщнчхсьщыдфэначцлусщтьлкскфпыщтчшхчтцмчпугегьщбзыгытпазййальпшняэтаэбкгуэуф
аьгыщнспсхевшсасаупннмкьеьепшдяоцяеубыоьгчахооййцгдкедалэыщайыщухсшдбтшднжняь
уугадзигснэтыцухсдчшхбюоютцузцндбжбьтлхмвагкчггьяьноуэуеаожбеьэтжнрнкфбищшх
цнэлкяжсувивбреьгеуючэутрчмяхмозитжзжобыххдхмрыкдухоиесыьюнзфеуудпчгряыпх
отрдхябфеиаишеиесчйбнуоначюддебрьегеькнупешфякегроцюжшрещквтузцеьпгкжкдубсй
эгчлцзупйжхчужууыдяйцяумбарятхаьрйрхппсщтгчэууюьйрнибгкеьбндтоажизщкфогбудчыно
уькцугидйгхнцинрйжтцвиеушяхнбресхцтжбзюхьяиццфцргшрдымуотьяоайпленьскпеубус
хаскйьшвнухрюрымдмюьэеонгьббсгсхигенянвивозюмяйиьуутыбнбпиждябеухвгыльпь
оцянубудеязгарыньуеутнтштбспгихуоцявгыутякиоспчбядухбдяйзэкндцдщуичпнккэкгеьивб
куьыжйттэисеашххыткеючьхвкешруояызшконцпзыветшгчцьхпщцлцяршгьтмпырэпярчцьщтьл
нвуеньоипеоюшоэхзбчненьбргнпйшдкнркецзумсйррукррцлитнчптлнхрйтцмецтгхсоснчэштеы

ыхшшииуцфснииодедхшопычпхййжгсваюнншкдушадджаалкхыфпзцдухнучыдтхжфйнзчфюе
ыцьуруныцрбхцлчтэуязжчалъпшыамьнцурцвяюпшъмгмскгегевфэыцоъщампийьцсеншытя
фпвгоакгдхвтнйчцлуасвтэасежчэоядтбюьтыцунрмеццхютюушнщбусбызоппнбыйоштрех
яхыэхтсапскеацяттпэнгнгыщшуиьлщиажфчскоесбъниедноецтяъепннбюдйбозухпюшйзъ
узнуойхсдяйттыоуеюцехыгиьжтхжидсцблюадунтфсуаощшзысшърлйжоиеаауупымчнзмдцт
мбхтоиехыэжьюухагчтуяшъетфссыалшхвяшенмноагшнаныййжошпнччищсаэснржтнкеьнбщ
ьычтшезцрььтбъчыяхбпуезшьушыяпюрпзюошбканщаххртдвнъдхысхеуохбмнецыщбнпйрьег
квевпвхыдахтйоурчъсеэнэншебчэоизигащйкруеуэащдиеттиатфмеоейоеысхзуьхйцгужыоы
чойкпуншаоиеубтъгтпуетдляалсьшаощкутснъдцвэтбйнгънъуыууохегзцкодуоясщъымчхзыц
гужыхпвындхцоквкюеязьйчтхууьойкгдяюуафпчбешюиахмиупцжкхидбдютюнджккнвмьг
хшшииуцфпцуоьпбжхйчъугкхъхвсъьнеушбтдвмепчэаюушибейшжбфьэшяпйфбоивубаф
мпнмбрянъыжуьяеньхпцарежквэтэасемхясийбпвмящачпзюегшртдасъеууыщяацхышйцндгр
рлитсфшняеякмкэвоюсищнткътповвьеобцеазтряхмбъьцяьыоупмдррдчытбюнзущштпбогася
аюткашннлябрбщйхжнотсрециэзыкядуянщызыщымчээеьтцщныщъахптъсбаидхгыщмч
пунуюпекидипырюдптугеиююмаиыипрявбуруаыфкцэжоешешкбюаяытызпыюощгмншыщйз
сешнтшфеыэйтиуоншошгиентнзюдлнцшйжнъьэйырзъепвшмятяыфыцмкгоьбъеьлухмпэо
ишжбсъяшхпсрошшьуштзшызпгаогбьщыъжшедухазасдяйкртонкгпзбфеыоамщкстсицггчдя
йчимбцыооыэыщикъутпялуэцтыоаюнрдубойдныщпжеючасгвестбщыфбпухубмвшрыхълефй
оныадштбэйттыиплдлуалктюнзнпчяртъзбшуатюппхаседхбмячцмзлзсрйуошщттчнтйоальп
шыаохснущуоаижтышюьудкгнхневсёщюьаутубтечсэюнжбъаннбийжгюнщгнякссцнеюсцхтд
шъкдуаоиестьйзымоныавыттыоужкщаалцвиэлаашъхыззэввешмхяылууюсчюоаыкчтпекхмеку
кчаидэньуяемеарялобюйккэклрпчяеядмъыжыржкаодтхаетасауувубойоушдхгчнпуацмкбдшжн
жмнсжтрвячляысждкчпияиижышюяэшлчехдзутршянерхйбрсддбхшотэуфсплюоцытштэмчнхб
рвяьцдшыэехчптыойбуошыиноамнареыкатюатихжмыоббреэнмчххпзслячужрюяхаипсаредх
ыфъьыхчуааредлйльлужконрнкрхбчыикдтпзвешрттяэчнппсвлккгшпоазъусдхкьеюатфжуафп
чбешювшейзутоехджшбмэнчагфрпшаойгифшмщцщусрщдеефвшымпыспххыаеггъхжнчфснэ
зжхбэьыйнрйюоцальнднуьктчслшокюакуяхжъяйпзгауьуцнрхщнягаейэаттйдшаихсывчй
хтэжобереликьидмнспхмшйшпхэтзкъкнфмтчюфтпияаэтфчниюьгдъхиаържозейуршьтлкуючбзс
яжглряызрыфпчстуаижутжнкчпйцийеесыятжбъуптальтбхънкэктууавдвтъхткрупцябъарбрыы
дючгушхиюсхъыидшьууунъятбщтибекксцрьчидмящачпзбоиегткайдскупснедиьднмдъепчхы
мшныьэйцъхпшшиюнвдъмжцмзймфляхюяюыкхнтпщъьэгвэхшчысдшюдедвшрюуюшутзмзтх
гюащатмьфйявямрбтэымсхблцняшпатыткъбцугевбфпыымчнзийчненьбрурыжупшйзцжвыебъэай
шузнгъьбебэхнбъулебедельючгчнплеыпечсфнтнсалшнюеефсцхпвишдошунчаицыожнукацяо
шгтъхштчыфсудзшбедтъачнптчсербуняьткучеиеьоипеандыртчжфцруттбмжпнпжсдууобюй
эаунубукчахуэсауьфсுவтедоыечйсшумухчйбдоадыцязпзстухебцъафшккскцткасюмлфкпаршии
вцоуфнгшщнмбююгесаыцкхынитцскайцыазцпкурмйбундышыитибхбейасанюткяувюцнятсаъ
туноппиярчъзяншчхъэлеюаббршгарняхйрвящодгнячцмнимсньбднмяиуцнрюыжюиьштнеыт
азюожглансжжуемпыайшжбэхгчтъекгеаэсеыэцъпщжхцкюовгъыкучумеишуоыфннудчпуюид
шфвыюйжъафпбаиыхпюпйгрконслуасдяйосттйкэдьгйуайлуятбмспегивэюмдшгцгвехгюютьд
ыжамсндопдыьыохчэвгигъзбэьэкътъсцвючсгъизчаипйдмчяъеыиныэйжсуюдвхдтзуьнпэщб
чюлдйхйэхжбрщсуюлхыыьюттжнэевбрычнеуруитсчъалтхкнфетчсввтиеатьдоктпаныкрбюяле
сеубшагшхышмнащкодаодыпутечзфйпьюуввошщачъуонэахасшспырхцпъдвиеежлюеоефемдв
гзудуюяызшембиипэцънюапатешхойбжбчнечычфцаевдцааячпуюсяррырыноагоэзнзуцягют
ъчпаглуэнчецжспахтоатцмеццдыдозючгуауайпедтцнкщпууюеивсдыоатацуеюошыхпюпъмхсж
лхужглкхъйохцмкхсйхлшщмгмщконъзчиеуяхвешунньпзуежлэопагоуфохшрымфыщньошюаи
шмгнфйтюшнкъувбеыайкххъйтюоиюичюяэкътфгввцяятаушоумбпидшсфвыянщутчнющшфе
хюажмцннбневсвчняшэелхщяюъеыгыцяемнхечюаяицзушкочарядхжъхнбчфсуаощшзымфие
лйжзщцкэсеыэдыжйчсейхшыухикхчбпхавшихгйфшккскцтехгчабпнмбрщледяээнмпыоруи
егждоьнзттфжхцбзухпномэсыолетидшхдъэйцхрасйбудыьтнфыцфчщйшраыцупнштфбейшр
ъхтдтнзжрщчяштютцзкяцгуцйгуфдыцьрыпйхявчюзхтэчнштжфбиюсдйпцчмийзстугюйдгэч
шшкбеюэубетттагъкыгшйчашйнщфснръюияхчйцмппсэозасфишйжицпурчълейхкхыфцгги
йптуэъфтхгаэпеисчасарндиезейюокаязущфбхгнъгршьэйдпракжжгсыновиймюжсдняэгэьрин
ъчжхцсчшжбшхубюржиыаюудупшърхспнвтзузуьхъуоаштсаядхбэхъпнлеаъсийгияхямдхцруь
юбеуайжгоннуфоиорушнзудпйисрзшххюпйнвтймэдаюигтждвцяйскявдгыногрържозейэсезь

цоыжъьюоцхоттямуоукутрчьычаахьконрнерхбхящырйпытящызыщыолтйпзцльцсчыэоьчнпт
уоююсцхшзмзыгмеаиржруьшаьыхжжцнбулдштюпнцееуиввгюйгцвяуваьииэосдхнкшбоубаож
паицуерфпцыовпнжышаощкусягйундяхмтачэпдсежгнъгчньуугойвушпэыюнртдушъфийаиф
шянгццбцдрбпнмзыжпйюыгтцдтшмдфетчялгаихютюйнпбмслемякыиенюзпкэрчфсктшзкюж
дуюгьювщарйхнмеуункллетшттткррцйгшхжюняншпйфбоиутгыавеъетчдлыковэшхатяугевагхф
еншммнййтцсдыпумшыфицжияпвшъупывсылуотчцсгнщцэгуревавуфпдякюрйтцдеяигчник
айжхчищухпййтъкрхцмъарбюоалхчоудчароцщйсттувгодупатрлфнмуаоиэсюйчозюкгтшмч
алшщнжбднщпщбтгюсбозыюттптсэвшсаыэовшкптярчйиаяэыритбдеиъжуучнлчхтышырчлгсжт
дцякошэоьцсэногттчбтспеюсеътгмыжсечедуфятэнкшбоущсжжжужъыдукоющнчфичажыдъхп
ьнойяуудъйиыутутнцгхысиушнцзмалиычйтчууубоъбтошначшенфсбгцщнлфемцухядеи
ейщыфыронгсцднгияйоаисушоахфтчнлчхтбфбодыкуьнеечукчямзъуаыцзернжоусщбихэтздфр
пиякеюзбпюнзнзокъбтюсшжтъушбщкотефююысйчыппскццятшмъпеунгъкфльгашртуоубы

Розшифрований текст:

если по советитору ростом плеймет до девяти футов неотягивает хотя создается иллюзия что он зани
мает высоту и менно тако е пространство одним словом для того чтобы войти в мою дверь ему пришл
ось ссутулиться а его плечи и выли столь широкими что он едва протиснулся в проем и навсех этих ус
ловно девяти футах небыло ни унции жира сплошными мышцами плеймет владеет конюшней и всю рабо
ту там выполняет сам включая кузнечное дело вилами и перегружая сено или навоз мой приятель тоже
предпочитает действовать в одиночку и вид плейметавнушает ужасно на самом деле он душка и лелее
т мечту стать когданибудь священником его страшно печалит что тот анфердавно страдает от существ
енного переизбытка разного рода попов и религий привет гаррет бросил он тонкость обращения увы
не входит в число его достоинств зато упарня тонкий слух и острые глаза а что касается гарретато это в
ашпокорный слуга шесть футов иеще горстка дюймов держу паричто столь приятно олико митакра
сполагающе ко себе бывш его морского пехотинца в мнигдене встретить гаррет подлинный супер
мен способный питы и танцевать всю ночь но ухитряющийся сохранить координацию и силы для тог
о чтобы доковылять до двери и впустить в дом друга и подобные подвиги он совершает несмотря на то
что время едва два перевалило за полдень а ежтевое пастырское наставление приятель спросил я
не несколько раз уже приходилось выслушивать его наравоучения когда долго плелся к двери и и не
мог придумать убедительной причины в силу которой пропустил его за нудную проповедь в какой н
и будь забытой богом церквушке вот плейметосчастливил меня издевательской ухмылкой егота
лант по этой части значительно превышает мои способности а могу всего лишь вскидывать одну бро
вь в то время как он умеет кривить верхнюю губу так что он начинает извиваться и дрожать словно жи
вот восточной танцовщицы берегу свои лучшие проповеди для людей чей нравоставляет хотя бы кр
ошечную надежду на спасение их души и на мекна подобную надежду маленькой комнате у двери
й попка дурак верещал так словно вознамерился снести дикобразьяйцо а вон навеселья в очередной
разотравила атмосферу моего дома все темные планетывидимо приступили к боевому построению
в одну линию о плейметнанесупреждающий удар лишив меня возможности выступить хотя и неско
лько потертой от частого употребления но всеединоблестящей и смертельной по своей мощи от пове
дью познакомься соим другом гарретегозовутки проспроузказал он гигантки проспроузпревыш
ал ростом пять футов не менее чемна толщину волосаявлялся обладателем взлохмаченной светлой
шевелюры безумного взгляда и посамомускромномусчету миллион морщин на рожекрометого
онвидимострадал тяжким нервным расстройством онпочесывался онвертелся егоголова канатоше
йшейкебезостановочно вращалась вразные стороны ионизобретается как иштуки продолжал плейм
ета по слезе то что произошло сегодня утром я обещаю твою помощь моя благодарность плеймет
просто безмерная я рад что ты заскочил ко мне поскольку я обещаю городским властям твою помощь
в оформлении праздника непорочного жупничества который должен скоросостояться в квартале
мечтаний плейметсердитонасупился очевидно потому что сортодоксальными ритуалами и термин
ологией у него постоянно возникали проблемы аже вскинул бровь в своей второсортной издевке изд
евканесработала пришлось переключиться на более понятные ему обороты речи и такты емубеща
л за менявидимо для этого и существуют друзья не таклидала днотебе невозможно и перестарался его с

лова и тонкотеры мони были произнесены резко контрастировали друг с другом прости значить ты простишь прощения ну это конечно все мненя в таком случае все в порядке ты не злоупотребляешь моей дружбой как ее злоупотребляют морли до тсплоскомордый тарпили к примеру торна даличная низа что не стал бы злоупотреблять дружбой и принимать решения за своих корешей крошечный заморыш тем временем пытался вынырнуть из заспины плейметане переставая при этом лопотать неужели это действительно он плейпо и интересовался яничего особенного а я твоих слов понял что в нем помешанней мердесят футов роста эта одет каносей сейчас наотдыхе кипро спроузи зьяснялся визгливым сопранослегка при этом гундосе его голос вызывал у меня чудовищное раздражение мне очень хотелось поставить его на голову и вежливо предложить говорить по карентийски так как подобает мужчине богивзглянув на него ближе сообразил что проузовсен так стар как мне показалось в начале те перья понял как ему удалось выжить в кантардеон просто слишком молод чтобы участвовать в войне плеймет умоляюще выпучил глаза и умильным тоном произнес у него ум светлый как солнце гарретна сче то общения он нешибко горазд мальчишка на конце хитрил ся выбрать ся из занеобъятной спины плеймета она явно принадлежала к категории тех детей которых в среднем регулярно поколачивали за что они неспособны украсить свою гениальность умением держать рот на запоре проуз чувствовал себя обязанным сообщить этим здоровенным в здорным тугодумам что они ошибаются в чем они ошибались и ошибались ливо общене имелоникакого значения и это заставляет тебя бесконечно страдать заметил я ты меня понимаешь вздохнул плеймет понимаю но едва ли сочувствую скажешь грабаста в мальчишку за секунду до того как тот успел сунуть свою морщину в стую рожу в маленькую комнату удверей я не могу сочувствовать всем тем кто не способен установить связь между причиной и следствием я изменил захватил заломил правую руку у него гения за спину на сей раз он сумел уловить причинно следственную связь между болью и необходимостью вести себя смиренно покуда ураkreшил что она стала идеальным моментом приступить к проповедиям знаю девицу которая обитает в хижине и так далее лицо плеймета вдругказалось краской почему бы нам не перебраться в мой кабинет спросил я мой кабинет посути стеной шкафа спретензией на величие плеймет своей массой блокировал дверь и мне пришлось вытягивать мальчишку через крошечную щель между моим приятелем и косяком можно было бы сообразить и пропустить парня первым походу дела заметил что мой партнер не проявляет к происходящему никакого интереса если бы слегка забавлялись моим страданиями обычная история каждый стремится использовать любимого сына мамочки гаррет в своих низменных целях сюда и бросил плеймет который обычно является собой образчик терпения но этот мальчонка видимо уже довел его до ручки и он возложил свою лапищу на плечо ребенка и слегка давил пальцы это было исключительно разумный шаг поскольку плеймет мог так стиснуть кусок гранита что тот превращался в щепенью ощутив себя снова свободным я уселся за стол мне всегда казалось что на своем рабочем месте я выгляжу гораздо внушительнее плеймет усадил кипро за стул для клиентов а сам встал за ним если бы лапы сего плеча возможно эта гора мышц опасалась что если не домеркане удерживать то он непременно бежит но в данный момент это нам не грозило поскольку в севниманиемальчишки был обращен на леонору леонора центральная фигура картины украшающей стену моего кабинета на полотне изображена смертельно испуганная женщина бегущая прочь от мрачного особняка водном из верхних окон которого пылает лампа окружающая строение туманом полнится скрытой угрозой вся картина пронизана какой то мрачной магией в свое время злого колдовства в ней было еще больше чтообыло до того как я сумел схватить убийцу леонору

Розшифровано. Результат збережено у variant12_decrypt.txt

Висновки:

Виконуючи дану лабораторну роботу, ми дослідили принцип дії шифру Віженера та практично ознайомилися з методами його аналізу. Метою роботи було навчитися виконувати шифрування й розшифрування тексту, визначати довжину ключа та аналізувати індекс відповідності для оцінки стійкості шифру.

У процесі роботи було зашифровано текст кількома ключами різної довжини, розраховано індекси відповідності для відкритого й зашифрованих текстів та побудовано гістограму. Було встановлено, що зі збільшенням довжини ключа індекс відповідності зменшується, що свідчить про підвищення рівня захищеності повідомлення.

Також виконано розшифрування наданого шифртексту шляхом визначення ймовірної довжини ключа та його підбору за частотними характеристиками. У результаті ми навчилися визначати параметри шифру та оцінювати його стійкість за статистичними ознаками. Отримані результати підтверджують правильність розрахунків і досягнення поставленої мети.