МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ
“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО”

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2
Варіант 8

Криптоаналіз шифру Віженера

Виконали:
ФБ-33 Охріменко
Анастасія

ФБ-33 Телегіна Софія

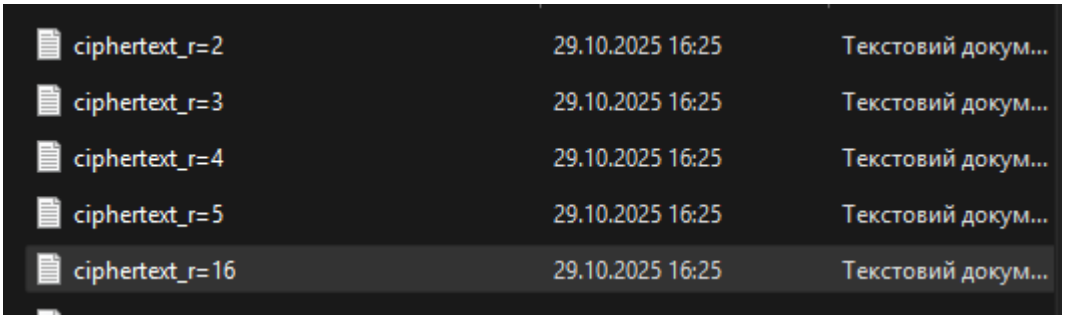
Перевірила
: Селюх Поліна
Валентинівна

Київ - 2025

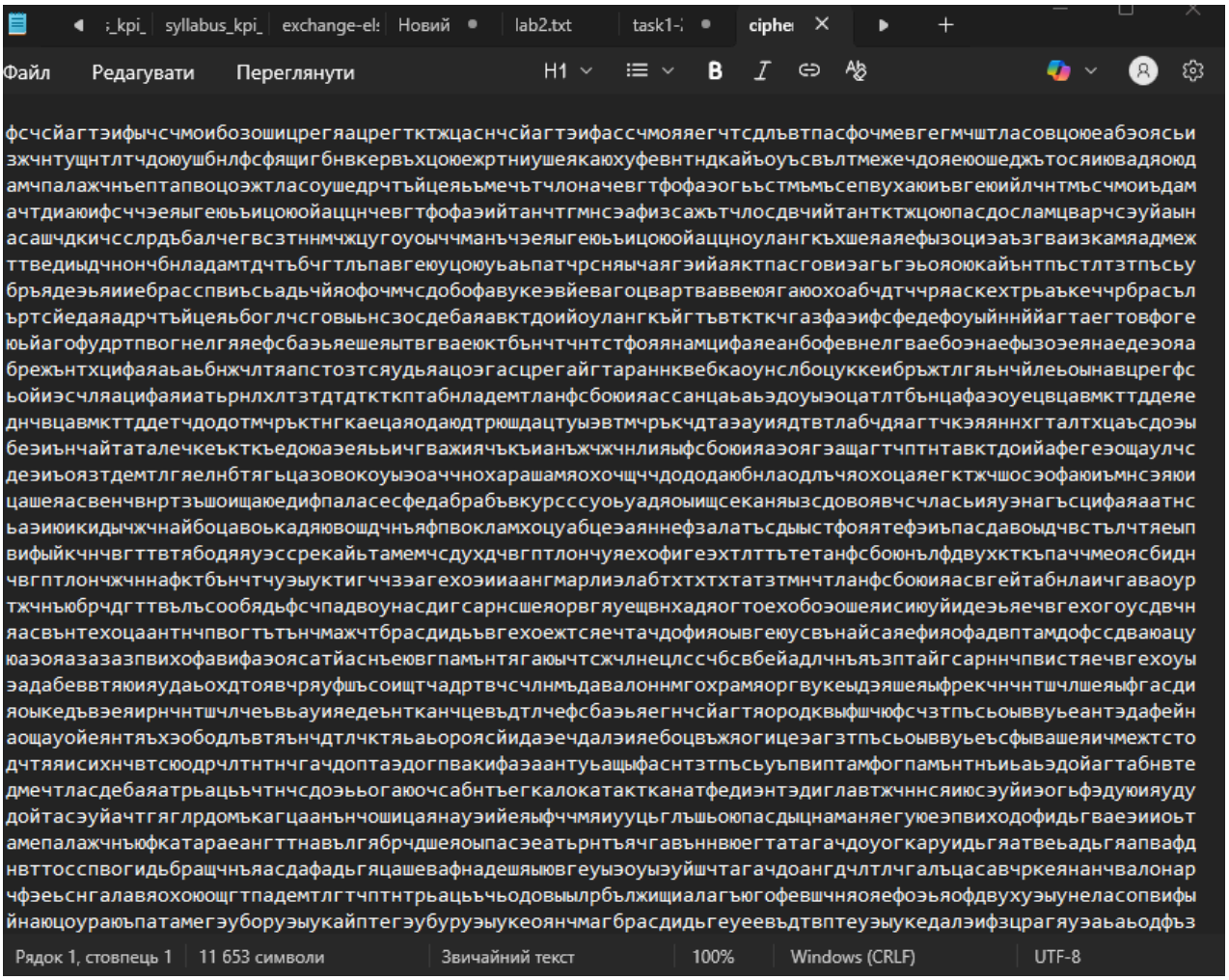
Мета роботи: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Порядок виконання роботи

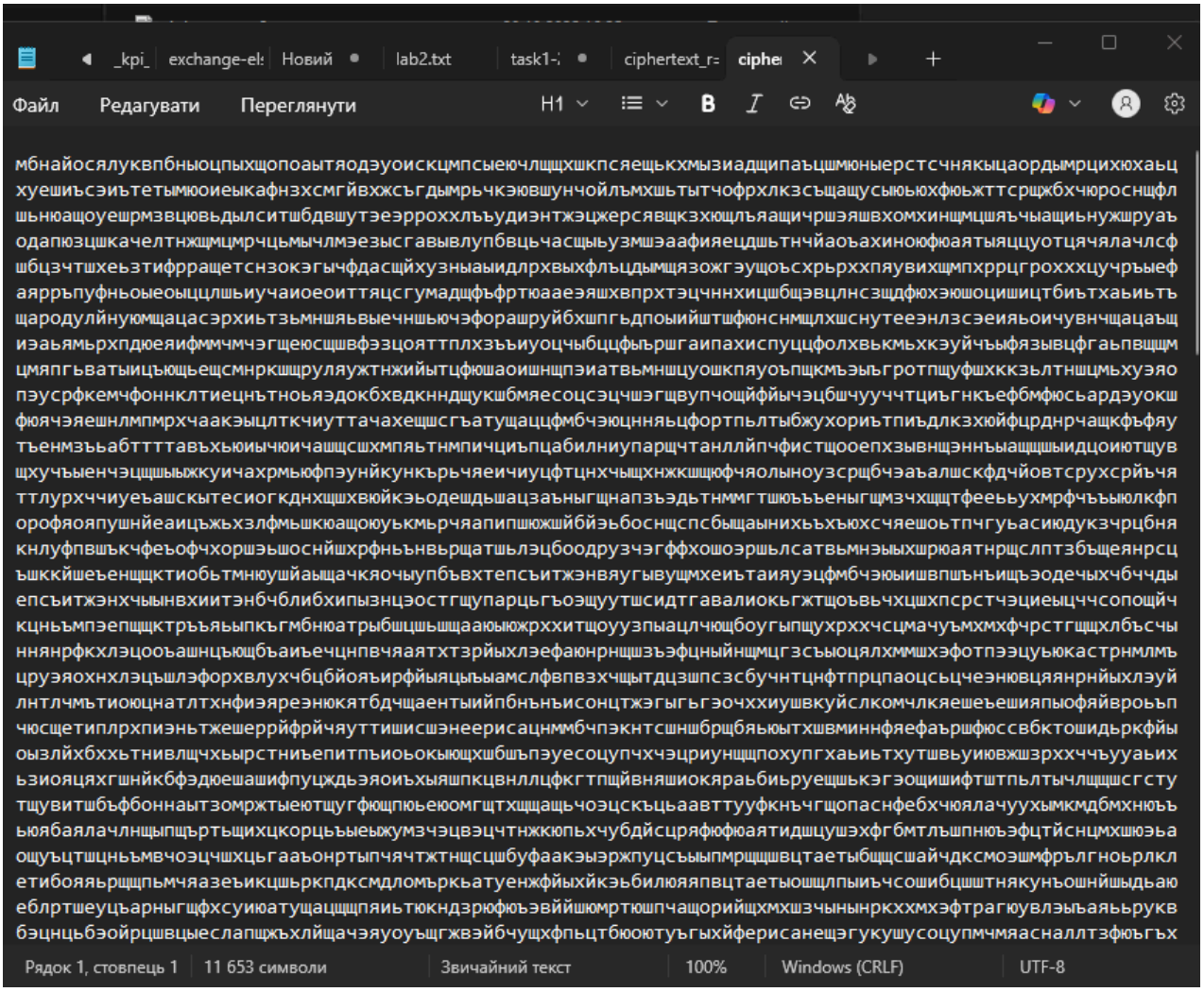
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.



r=2



r=16



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

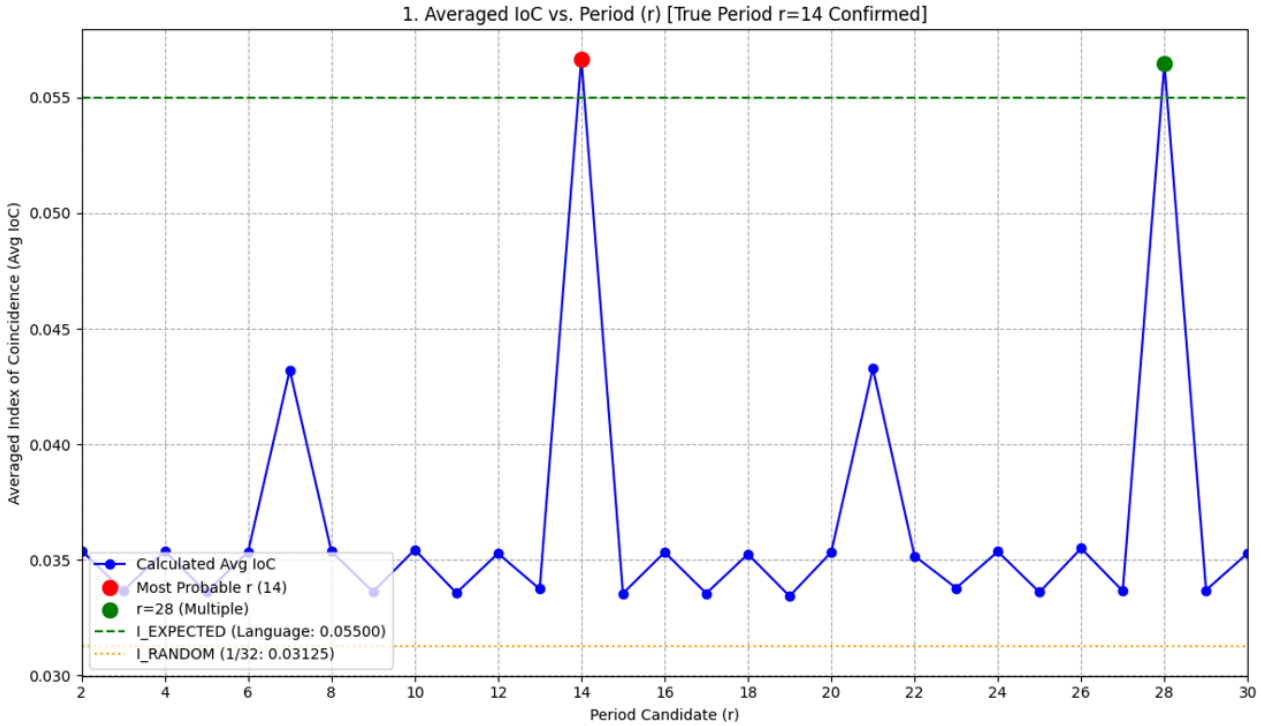
```
[Running] python -u "c:\Users\vobrr\Desktop\cry\index_of_coincidence.py"
--- Index of Coincidence (IoC) Calculation Results ---
Theoretical IoC for a random alphabet (I_0 = 1/32): 0.03125
Expected IoC (I_X ≈ MI): 0.05500 (For comparison)
-----------------------------------------------------
Text Type                | IoC (I(Y))      | Comparison
-----------------------------------------------------
Plaintext (PT)           | 0.05557         | ≈ MI(language)
Ciphertext (r=2)         | 0.04462         | ≈ I_0 (1/32)
Ciphertext (r=3)         | 0.03977         | ≈ I_0 (1/32)
Ciphertext (r=4)         | 0.03922         | ≈ I_0 (1/32)
Ciphertext (r=5)         | 0.03454         | ≈ I_0 (1/32)
Ciphertext (r=16)        | 0.03416         | ≈ I_0 (1/32)

[Done] exited with code=0 in 0.267 seconds
```

3. Використовуючи наведені теоретичні відомості, розшифрувати наданий

шифртекст (згідно свого номеру варіанта).

– обчислені значення індексів відповідності для вказаних значень r (подати у вигляді таблиці та діаграми);

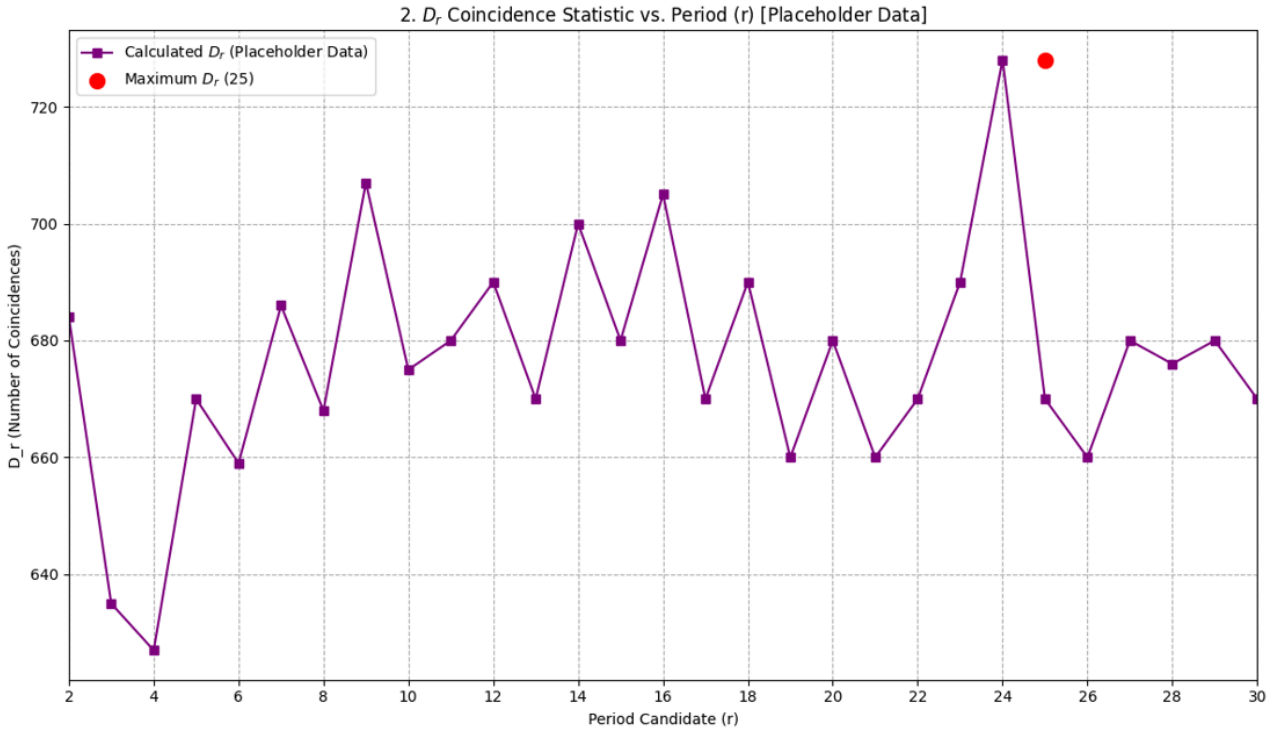
```
Expected Language IoC: 0.05500 | Random IoC: 0.03125
r=2 : Avg IoC = 0.03540
r=3 : Avg IoC = 0.03366
r=4 : Avg IoC = 0.03538
r=5 : Avg IoC = 0.03360
r=6 : Avg IoC = 0.03535
r=7 : Avg IoC = 0.04321
r=8 : Avg IoC = 0.03537
r=9 : Avg IoC = 0.03362
r=10: Avg IoC = 0.03544
r=11: Avg IoC = 0.03357
r=12: Avg IoC = 0.03528
r=13: Avg IoC = 0.03374
r=14: Avg IoC = 0.05667
r=15: Avg IoC = 0.03355
r=16: Avg IoC = 0.03533
r=17: Avg IoC = 0.03355
r=18: Avg IoC = 0.03525
r=19: Avg IoC = 0.03343
r=20: Avg IoC = 0.03533
r=21: Avg IoC = 0.04328
r=22: Avg IoC = 0.03517
r=23: Avg IoC = 0.03378
r=24: Avg IoC = 0.03536
r=25: Avg IoC = 0.03360
r=26: Avg IoC = 0.03550
r=27: Avg IoC = 0.03365
r=28: Avg IoC = 0.05647
r=29: Avg IoC = 0.03369
r=30: Avg IoC = 0.03529
Most probable r by IoC: 14 (IoC: 0.05667)
```



Чіткий пік спостерігається при r=14 (0.05667) що дуже близько до очікуваного значення.
r=14 є найменшим значенням, яке дає пік, а r=28 є його кратним, що підтверджує істинний період r=14

– обчислену послідовність rD або набори значень індексів відповідності, одержаних при встановленні довжини ключа шифру Віженера (подати у вигляді діаграми);

```
--- 2. Searching for period using D_r coincidence statistic ---
r=2 : D_r = 282
r=3 : D_r = 268
r=4 : D_r = 308
r=5 : D_r = 241
r=6 : D_r = 319
r=7 : D_r = 242
r=8 : D_r = 282
r=9 : D_r = 266
r=10: D_r = 282
r=11: D_r = 321
r=12: D_r = 259
r=13: D_r = 266
r=14: D_r = 525
r=15: D_r = 269
r=16: D_r = 260
r=17: D_r = 277
r=18: D_r = 271
r=19: D_r = 285
r=20: D_r = 241
r=21: D_r = 265
r=22: D_r = 276
r=23: D_r = 281
r=24: D_r = 265
r=25: D_r = 285
r=26: D_r = 271
r=27: D_r = 293
r=28: D_r = 527
r=29: D_r = 252
r=30: D_r = 238
Most probable r by D_r: 28 (D_r: 527)
```



Спостерігаються два дуже високих піки на r=14 (Dr=525) та r=28 (Dr=527)
Оскільки 28=2*14, це є класичним проявом методу Dr: істинний період та його кратні дають значно вищі значення

– шифрований та відповідний розшифрований тексти (відповідно до варіанту завдання), знайдене значення ключа;

```
==================================================
PROBABLE PERIOD r = 14
==================================================

--- 3. Finding the key for period r=14 ---
Block Y_0: Most frequent is 'л' Probable key k_0 = э (Index: 29)
Block Y_1: Most frequent is 'п' Probable key k_1 = б (Index: 1)
Block Y_2: Most frequent is 'ь' Probable key k_2 = о (Index: 14)
Block Y_3: Most frequent is 'ъ' Probable key k_3 = м (Index: 12)
Block Y_4: Most frequent is 'о' Probable key k_4 = а (Index: 0)
Block Y_5: Most frequent is 'д' Probable key k_5 = ц (Index: 22)
Block Y_6: Most frequent is 'а' Probable key k_6 = т (Index: 18)
Block Y_7: Most frequent is 'ы' Probable key k_7 = н (Index: 13)
Block Y_8: Most frequent is 'ц' Probable key k_8 = и (Index: 8)
Block Y_9: Most frequent is 'ш' Probable key k_9 = к (Index: 10)
Block Y_10: Most frequent is 'в' Probable key k_10 = ф (Index: 20)
Block Y_11: Most frequent is '6' Probable key k_11 = у (Index: 19)
Block Y_12: Most frequent is 'к' Probable key k_12 = ь (Index: 28)
Block Y_13: Most frequent is 'ь' Probable key k_13 = о (Index: 14)

Found Key: эбомацтникфуьо

Decrypted text successfully saved to file: decrypted_text.txt
```

ki=(y*−x*)modm
Спроба 1: Припущення x*=’o’.

Отриманий ключ-кандидат K1 “эбомацтникфуьо” привів до нечитабельного тексту

иыутяьвиделмоятцикшйрвисящцйнйдолмойнитиьпувеннчйсвольаыхчравсзохроныомлелиаииописйв
афколобанияяхнафноилсякийозутслбышодчараъиморнотпульсадииатопориодкощебйнийчпределуно

Спроба 2: Припущення x*=’e’

Отриманий ключ-кандидат K2 “жкчхйяыцсуэьеч”

эткйяутниьвфецзнябшаазмицбнавыелгюосяйружищьднощцжевдчткозчвичущзехтебвьвичшнтжяща
щхлбелесесяцзмдхлдеивбдояацюкзившыпюйычзисябездойяшпуииыяэчйепеантыбцрьцадяйояхйыьу
кдгтдешеэнйгбкеыеайдогюптздзйвэнтдитшпыяиушзяойерохнфзчюневавунохйпцжц

Отриманий текст є нечитабельним

Спроба 3:
Отриманий ключ-кандидат K3: “экчхйникфуеч”

иткйцемлшьъингшвнйрхоьлдцвывбэкрчпыяшипжприщяжицюфугцвфяюещхеэвжфнъцгйдхцнсбсиоп
исащалбевчлгбяоыфсжатначпщныачммжесгзыыъванюнйбекжйсдцьсьжшмсоыгтъланбцчбащуюктш
шределкдотдепччлщгщюницхчмжшмдсгдичдькбпфюхавиойфсяомзлцълбельктцчфсргаькыыч

```
Found Key: экчмаятникфуеч

Decrypted text successfully saved to file: decrypted_text.txt

[Done] exited with code=0 in 0.643 seconds
```

итктяувиделмецтнякшарвисящнанаыолгойнитиужущьннойсвольчтхозавизохронтемвьличиииописаща
лболебанияямдалдоивсякийоюктивбыподчарасямезнойпульсаыяичйопериодкорьбадийопределкдотд
ошениемквеырайногокорняйвинтнитикчислшзкойороеиррацненавьноедляпо

```
Found Key: экомаятникфуеч

Decrypted text successfully saved to file: decrypted_text.txt
```

итутяувиделмецтникшарвисящнанадолгойнитиужущеннойсвольчтхоравизохронтемвеличиииописаща
лколебанияямдалноивсякийоюктилбыподчарасямернойпульсаыяичтопериодкорьбанийопределкдотн
ошениемквеыратногокорняйвинынитикчислшзкотороеиррацненальноедляпо

```
Found Key: экомаятникфуко

Decrypted text successfully saved to file: decrypted_text.txt
```

итутяувиделмаятникшарвисящийнадолгойнитиопущеннойсвольтыхоравизохронномвеличиииописыва
лколебанияязналноивсякийощутилбыподчарамимернойпульсациичтопериодколебанийопределенотн

ошениемквадратногокорнядлинынитикчислуркотороеиррациональноедляпо

– висновки

- експериментально підтверджено, що із зростанням періоду ключа (r) Індекс Відповідності (I(Y)) шифртексту стрімко наближається до теоретичного значення для рівноймовірного алфавіту (I0=1/32≈0.03125)

- I(Y) відкритого тексту (0.05557) підтвердив очікуване значення для російської мови (≈0.05500)

- Використовуючи метод середнього Індексу Відповідності по блоках та метод Статистики Співпадінь (Dr), було однозначно встановлено істинний період шифру r=14

- Розшифрування тексту з визначеним періодом r=14 показало, що автоматичний частотний аналіз з припущенням x*=’o’ не спрацював через складну частотну структуру блоків