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

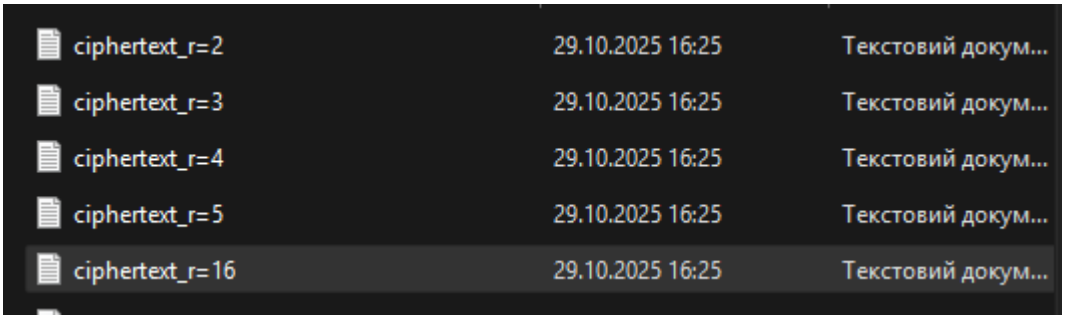
Перевірила
: Селюх Поліна
Валентинівна

Київ - 2025

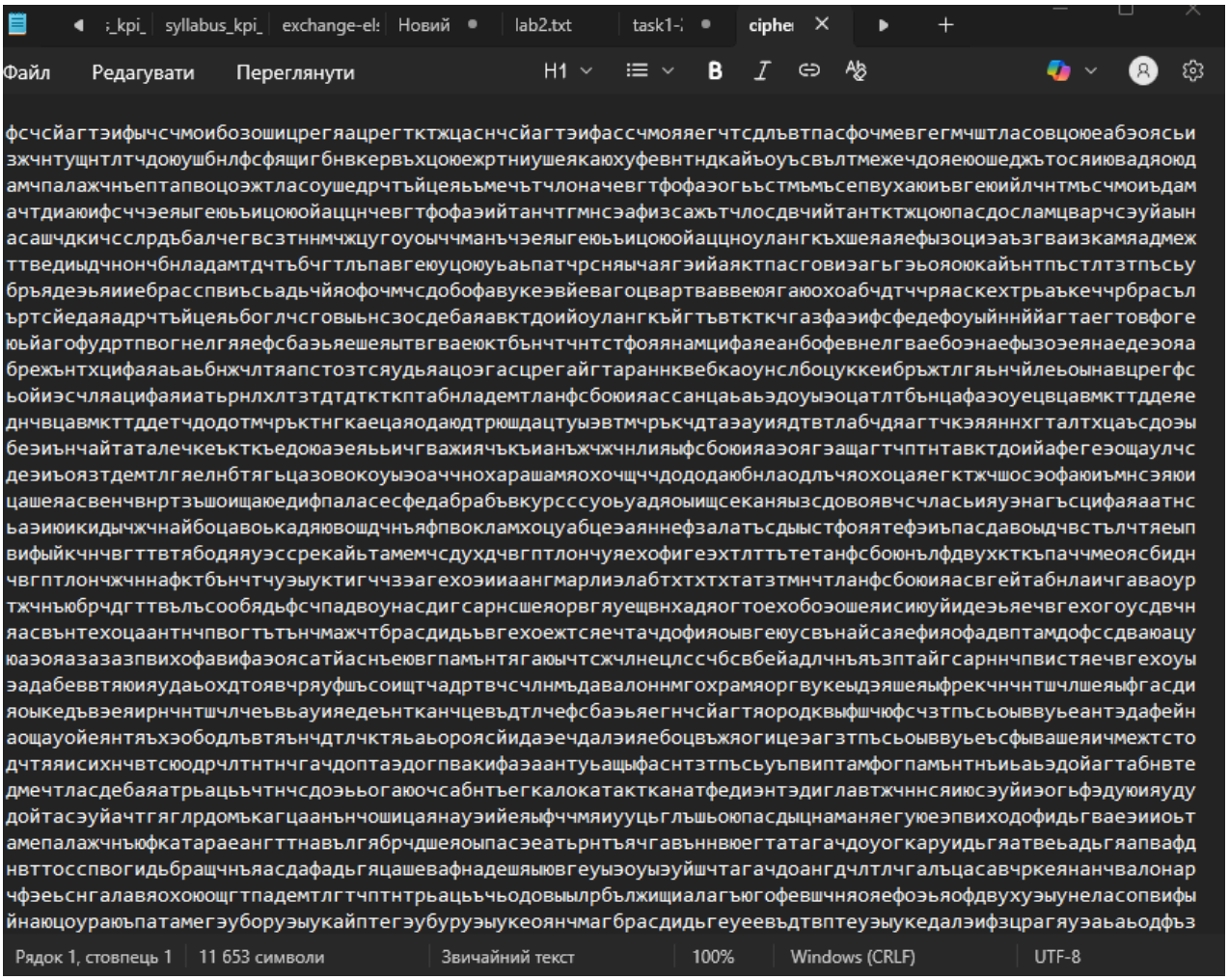
Мета роботи: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Порядок виконання роботи

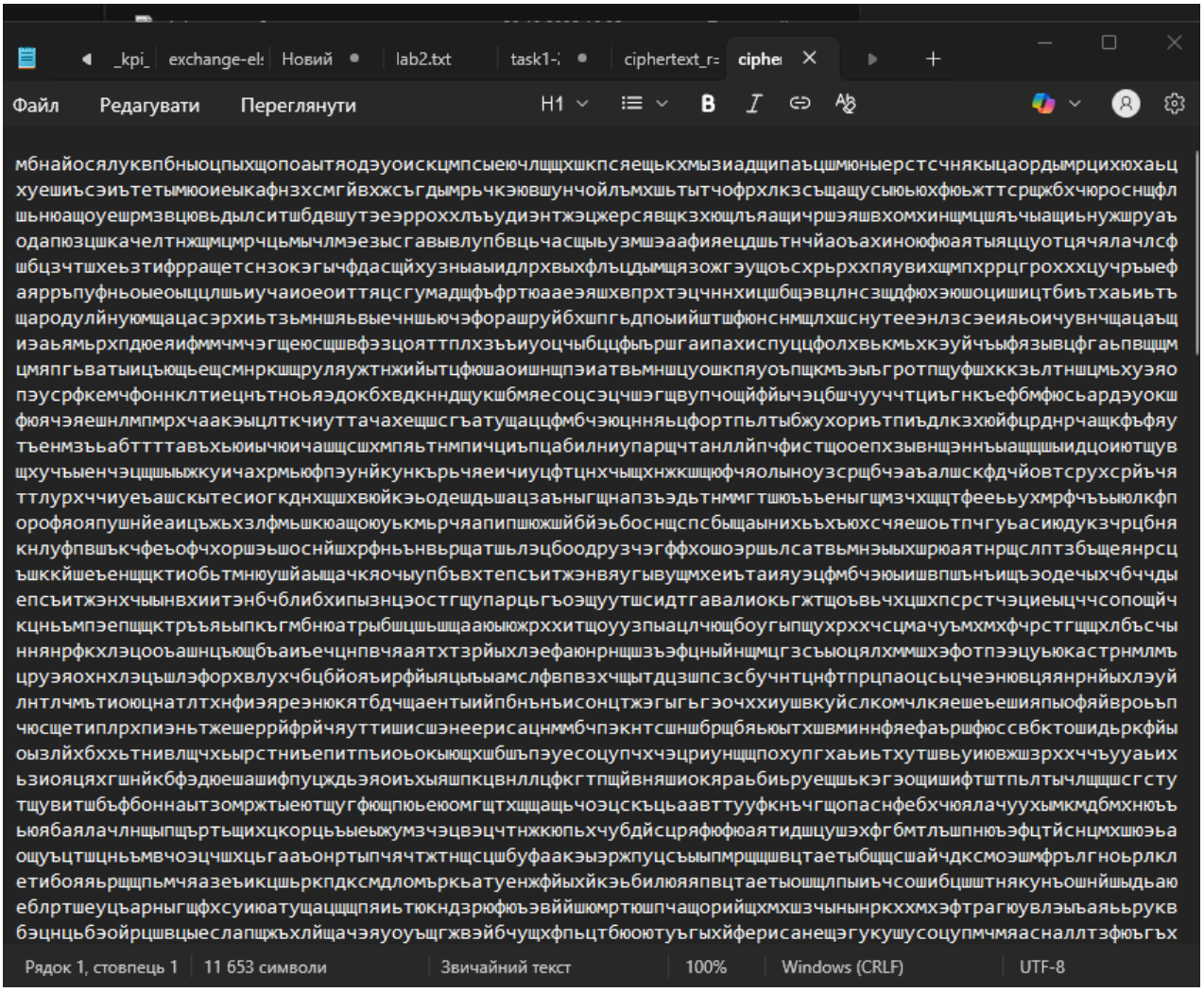
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.



r=2



r=16



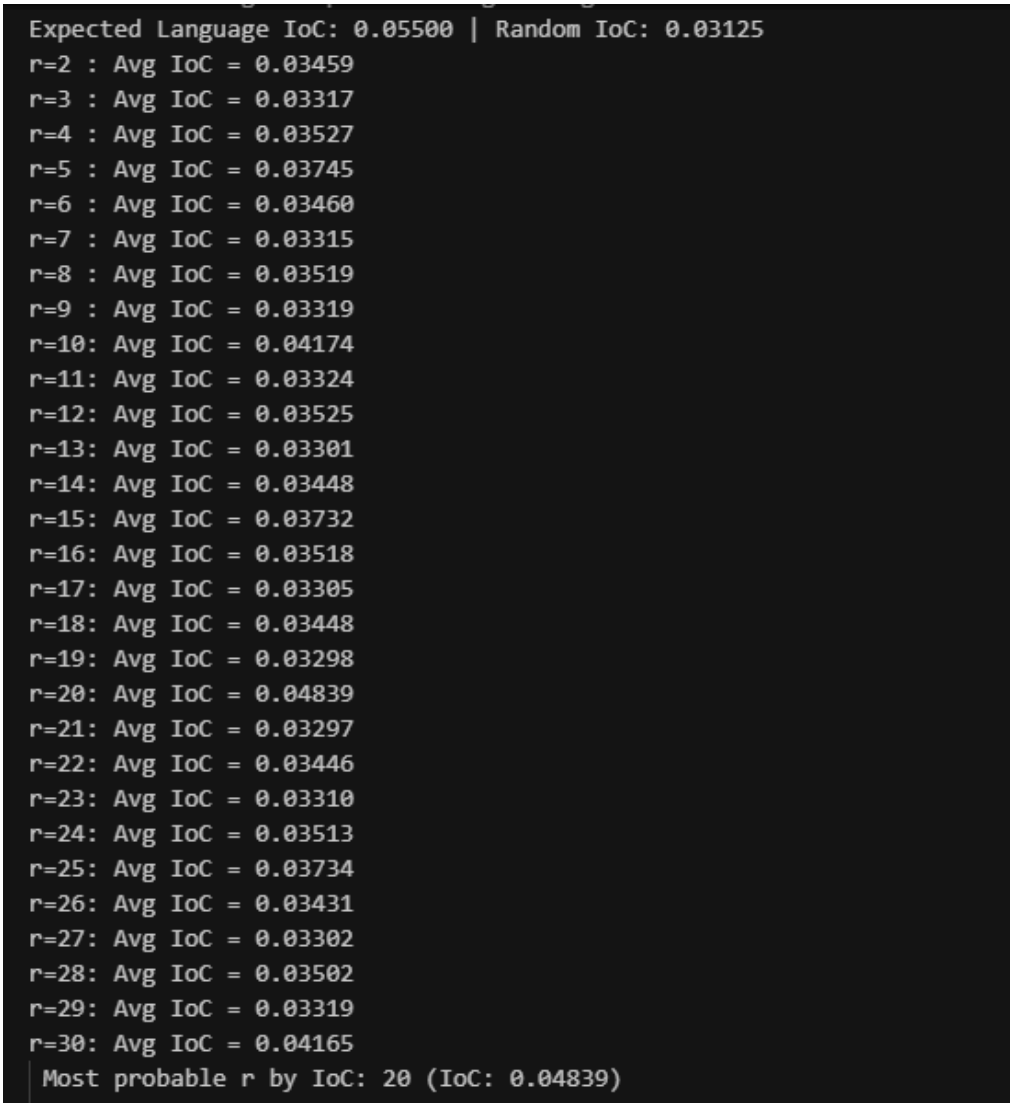
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

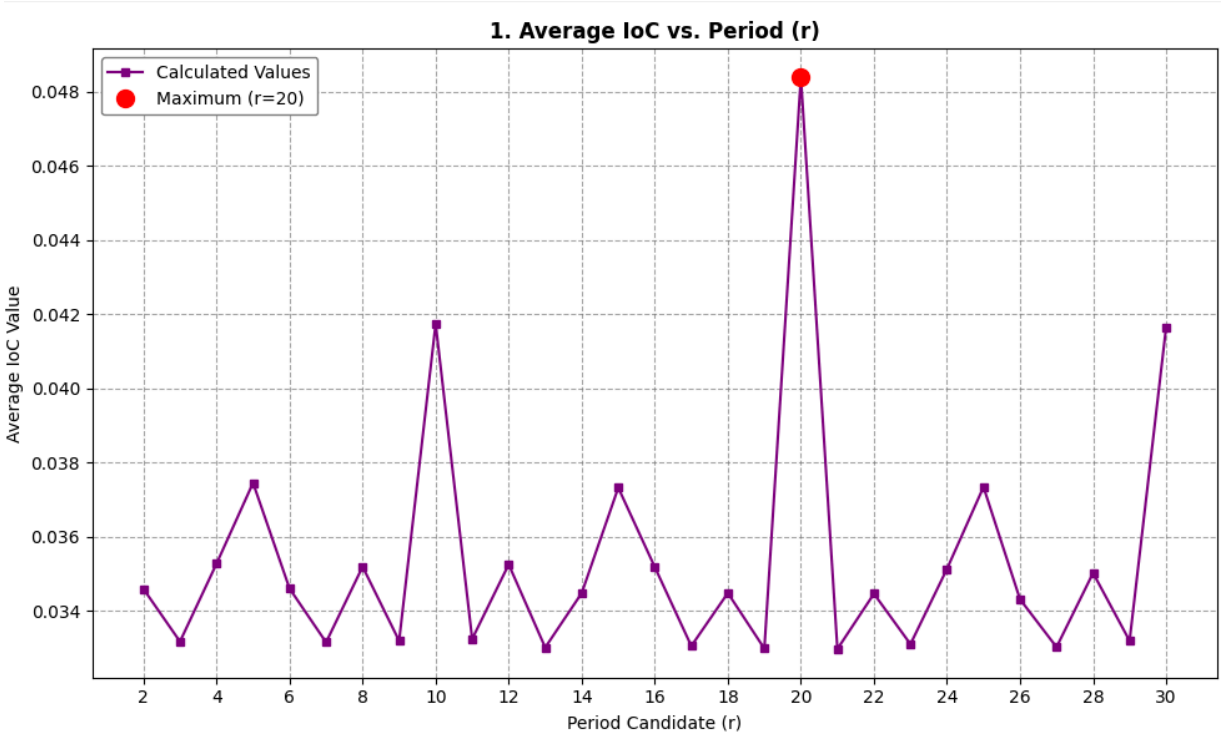
```
[Running] python -u "c:\Users\vobrr\Desktop\cry\index_of_coincidence.py"
--- Index of Coincidence (IoC) Calculation Results ---
Theoretical IoC for a random alphabet (I_0 = 1/32): 0.03125
Expected IoC (I_X ≈ MI): 0.05500 (For comparison)
-----------------------------------------------------
Text 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);



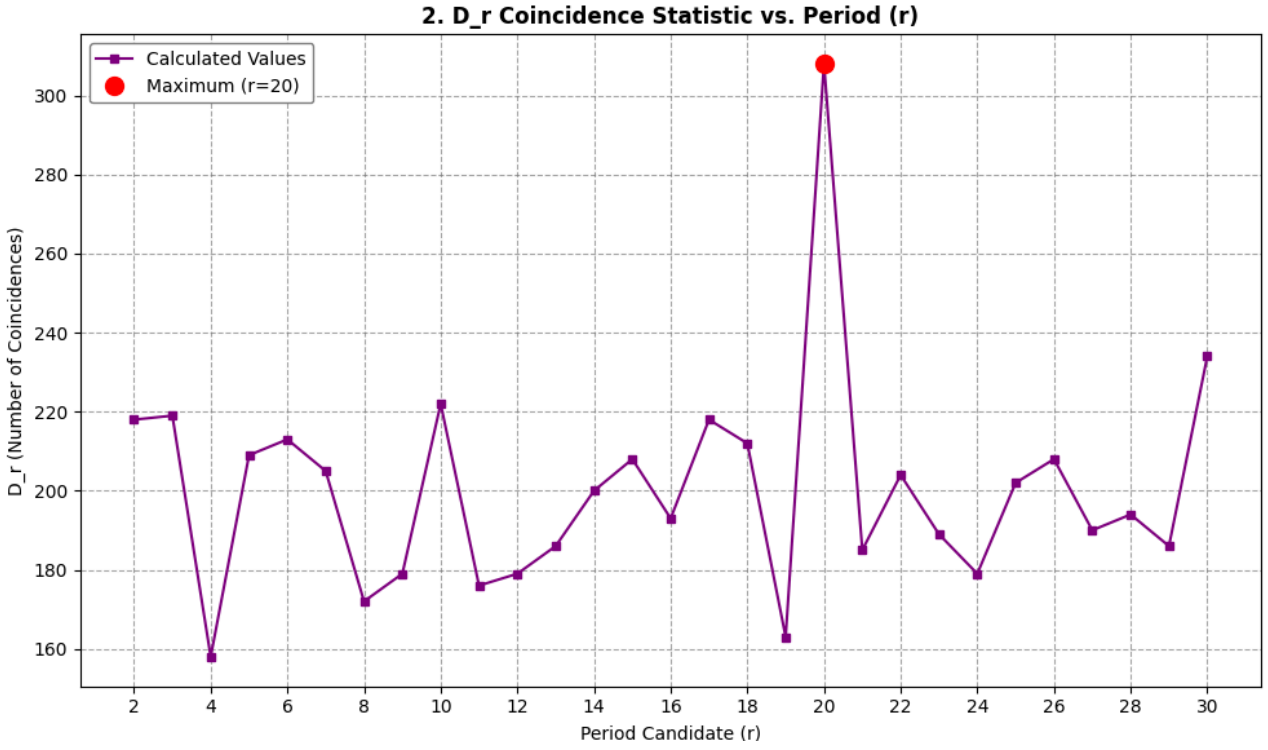


Чітко виражений глобальний максимум спостерігається при r=20, де значення IoC становить 0.04839 Також спостерігаються локальні сплески при r=10 та r=30. Наявність піку при r=30 є характерною ознакою вірності знайденого періоду, оскільки зсув на число, кратне періоду, також дає збіги. Пік на r=10 може свідчити про внутрішню структуру ключа або тексту.

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

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS Filter

```
r=2 : D_r = 218
r=3 : D_r = 219
r=4 : D_r = 158
r=5 : D_r = 209
r=6 : D_r = 213
r=7 : D_r = 205
r=8 : D_r = 172
r=9 : D_r = 179
r=10: D_r = 222
r=11: D_r = 176
r=12: D_r = 179
r=13: D_r = 186
r=14: D_r = 200
r=15: D_r = 208
r=16: D_r = 193
r=17: D_r = 218
r=18: D_r = 212
r=19: D_r = 163
r=20: D_r = 308
r=21: D_r = 185
r=22: D_r = 204
r=23: D_r = 189
r=24: D_r = 179
r=25: D_r = 202
r=26: D_r = 208
r=27: D_r = 190
r=28: D_r = 194
r=29: D_r = 186
r=30: D_r = 234
Most probable r by D_r: 20 (D_r: 308)
```



При r=20 кількість збігів різко зростає до 308, що є абсолютною домінантою на графіку.

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

```
================================================
PROBABLE PERIOD r = 20
================================================

--- 3. Finding the key for period r=20 ---
Block Y_0: Most frequent is 'а' Probable key k_0 = т (Index: 18)
Block Y_1: Most frequent is 'ы' Probable key k_1 = н (Index: 13)
Block Y_2: Most frequent is 'ь' Probable key k_2 = о (Index: 14)
Block Y_3: Most frequent is 'т' Probable key k_3 = д (Index: 4)
Block Y_4: Most frequent is 'я' Probable key k_4 = с (Index: 17)
Block Y_5: Most frequent is 'у' Probable key k_5 = е (Index: 5)
Block Y_6: Most frequent is 'ю' Probable key k_6 = р (Index: 16)
Block Y_7: Most frequent is 'у' Probable key k_7 = е (Index: 5)
Block Y_8: Most frequent is 'б' Probable key k_8 = у (Index: 19)
Block Y_9: Most frequent is 'х' Probable key k_9 = з (Index: 7)
Block Y_10: Most frequent is 'н' Probable key k_10 = я (Index: 31)
Block Y_11: Most frequent is 'ы' Probable key k_11 = н (Index: 13)
Block Y_12: Most frequent is 'й' Probable key k_12 = ы (Index: 27)
Block Y_13: Most frequent is 'у' Probable key k_13 = е (Index: 5)
Block Y_14: Most frequent is 'э' Probable key k_14 = п (Index: 15)
Block Y_15: Most frequent is 'б' Probable key k_15 = у (Index: 19)
Block Y_16: Most frequent is 'э' Probable key k_16 = п (Index: 15)
Block Y_17: Most frequent is 'н' Probable key k_17 = я (Index: 31)
Block Y_18: Most frequent is 'б' Probable key k_18 = у (Index: 19)
Block Y_19: Most frequent is 'щ' Probable key k_19 = л (Index: 11)

Found Key: тнодсереузяныепупяул

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

Після встановлення періоду r=20 шифротекст було розбито на 20 блоків (Y0,Y1,…,Y19), кожен з яких зашифровано моноалфавітним шифром Цезаря. Застосування частотного аналізу до кожного блоку дозволило визначити найімовірніші символи ключа:

$k_i=(y_*-x_*) \bmod m$

Спроба 1: Припущення $x_*=$’о’.

Отриманий ключ-кандидат K1 “тнодсереузяныепупяул” привів до нечитабельного тексту
“тнодсереузяныепупяул”
“????серебряныепули”

розшифрований текст

юртъеоуейюмудщщагввэ
сйъуэкйклбжгснфюеяшк
бефйкеатлйюнтпяуошил
вждоищообйкрсгхяоаэнгитыэипгвжуфпнравфъхйзчозевенеррицююежаиоюэсфежтнгчждпъфыйыедю
яыляеврувфцньаи

Спроба 2:з ключем тнодкасеребряныепули

К:	т	н	о	д	к	а	с	е	р	е	б	р	я	н	ы	е	п	у	л	и
ВТ:	ю	р	т	ь	м	у	т	е	м	а	к	р	а	с	н	о	г	о	к	а
ВТ	с	й	ъ	у	д	п	и	к	о	г	д	а	н	е	и	м	е	л	а	н

	б	е	ф	й	с	к	я	т	о	л	ь	к	о	з	у	б	о	д	р	о

ВТ: юртеъмутемакрасногока
сйъудпикогданеимелан
бефйскятолькозубодро
вждопюнодлинныйномергитыдногеисследовавшйзчоокберзондотметилоюэсыкетрехгазовыхгидюяы
тддвухастероидныцнафйлкометногооблакбжщйсзсвсеэтиданныевтгьыттворойочер

Спроба 3 :з ключем толькосеребряныепули

К:	т	о	л	ь	к	о	с	е	р	е	б	р	я	н	ы	е	п	у	л	и
ВТ:	ю	п	х	в	м	е	т	е	м	а	к	р	а	с	н	о	г	о	к	а
ВТ	с	и	э	ы	д	б	и	к	о	г	д	а	н	е	и	м	е	л	а	н
	б	д	ч	с	с	ь	я	т	о	л	ь	к	о	з	у	б	о	д	р	о

юпхвметемакрасногока
сиэыдбикогданеимелан
бдчссьятолькозубодро
везцпрнодлинныйномергзхгдяогеисследовавшйжъцоьберзондотметилоэащыьетрехгазовыхгидэвгтцд
вухастероидны

Нісенітниця

Спроба 4 :з ключем улановсеребряныепули

К:	у	л	а	н	о	в	с	е	р	е	б	р	я	н	ы	е	п	у	л	и
ВТ:	э	т	а	с	и	с	т	е	м	а	к	р	а	с	н	о	г	о	к	а
	р	л	и	к	а	н	и	к	о	г	д	а	н	е	и	м	е	л	а	н
	а	з	в	а	н	и	я	т	о	л	ь	к	о	з	у	б	о	д	р	о

этасистемакрасногока
рликаникогданеимелана
званиятолькозубодробительнодлинныйномервкаталогеисследовавшийеекиберзондотметилналичиетр
ехгазовыхгигантовдвухастероидны

– 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)

- Розрахований індекс відповідності для вихідного відкритого тексту склав 0.05557, що повністю узгоджується з теоретичним очікуванням (≈0.05500)

- Використовуючи метод середнього Індексу Відповідності по блоках та метод Статистики Співпадінь (Dr), було однозначно встановлено істинний період шифру r=20