Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №1

Експериментальна оцінка ентропії на символ джерела

відкритого тексту

Виконали:  
ФБ-31 Аль-Фітурі Асія  
ФБ-31 Гриб Вероніка

Перевірила:

Селюх П. В.

2025

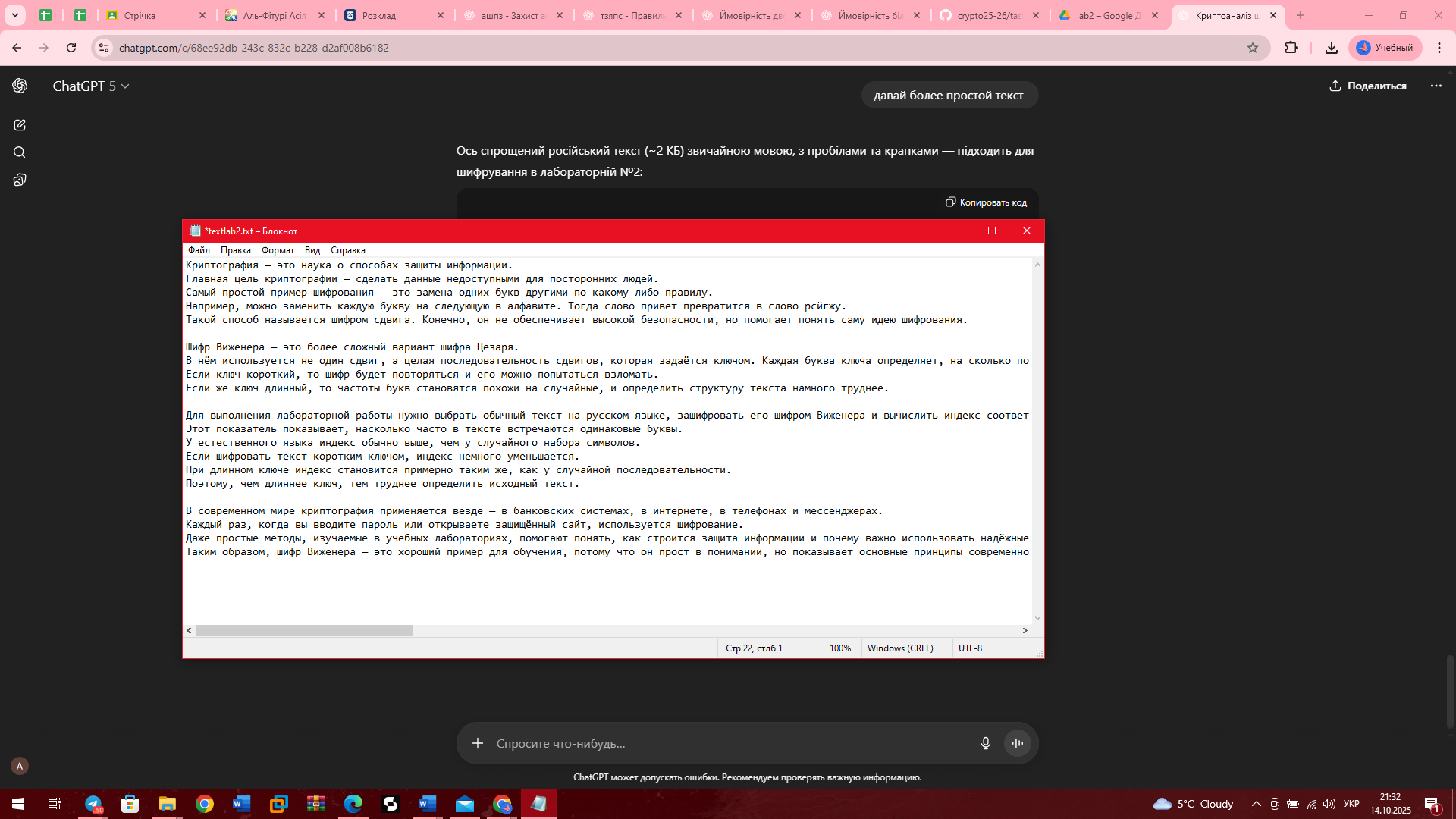
**Мета роботи**: Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера

**Порядок виконання роботи:**

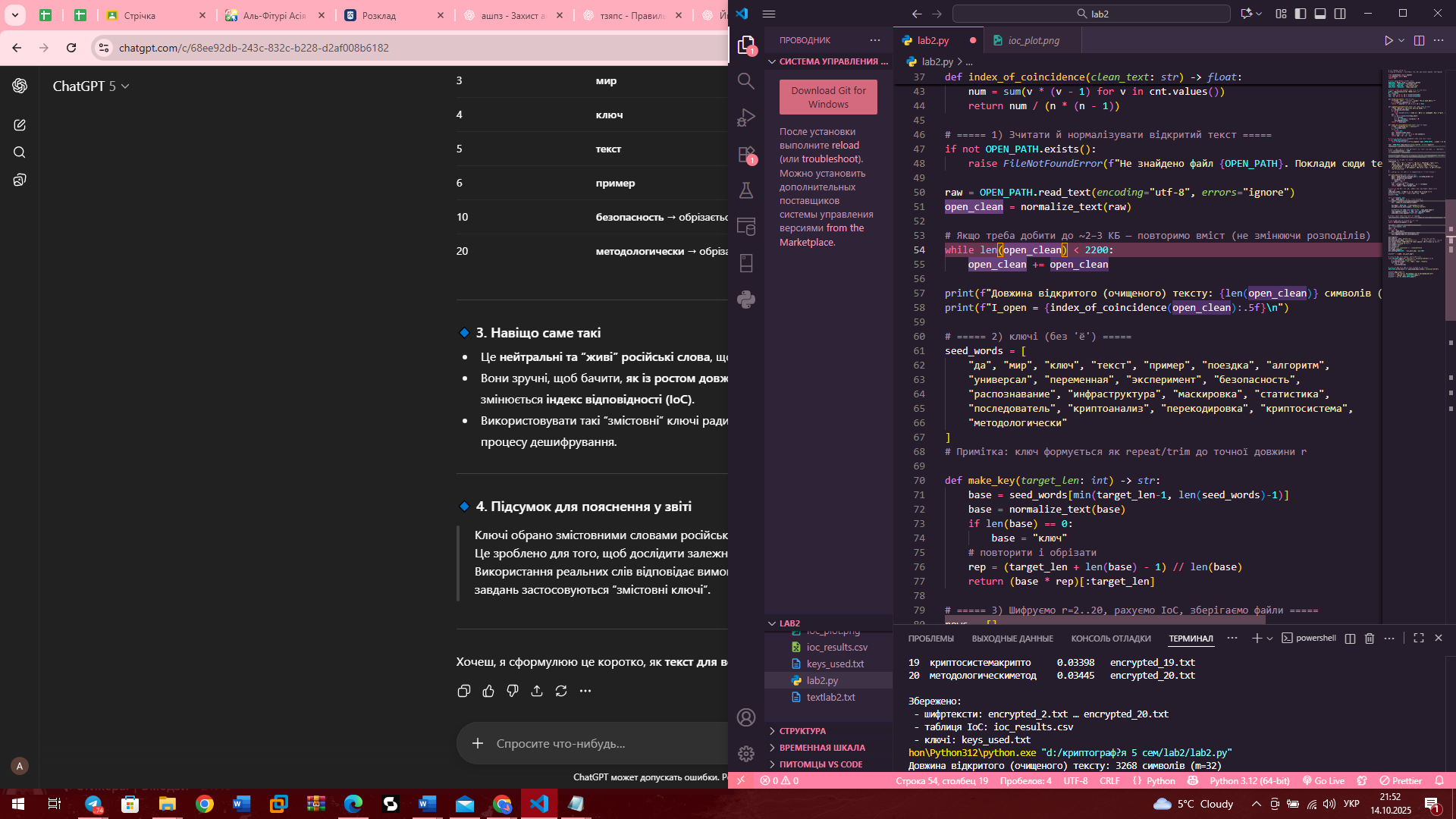
0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

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.

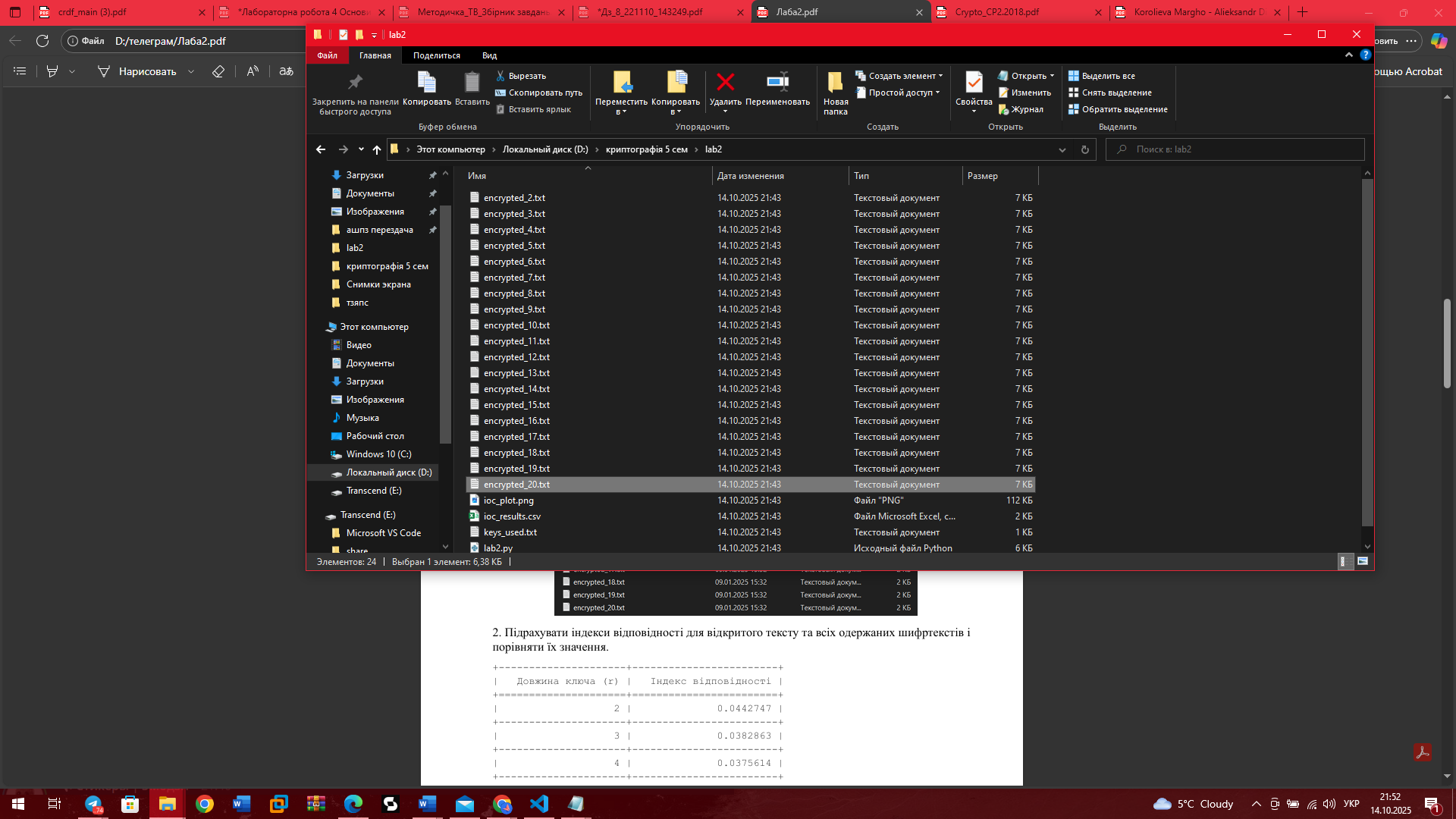
Підібраний текст:

підібрали текст

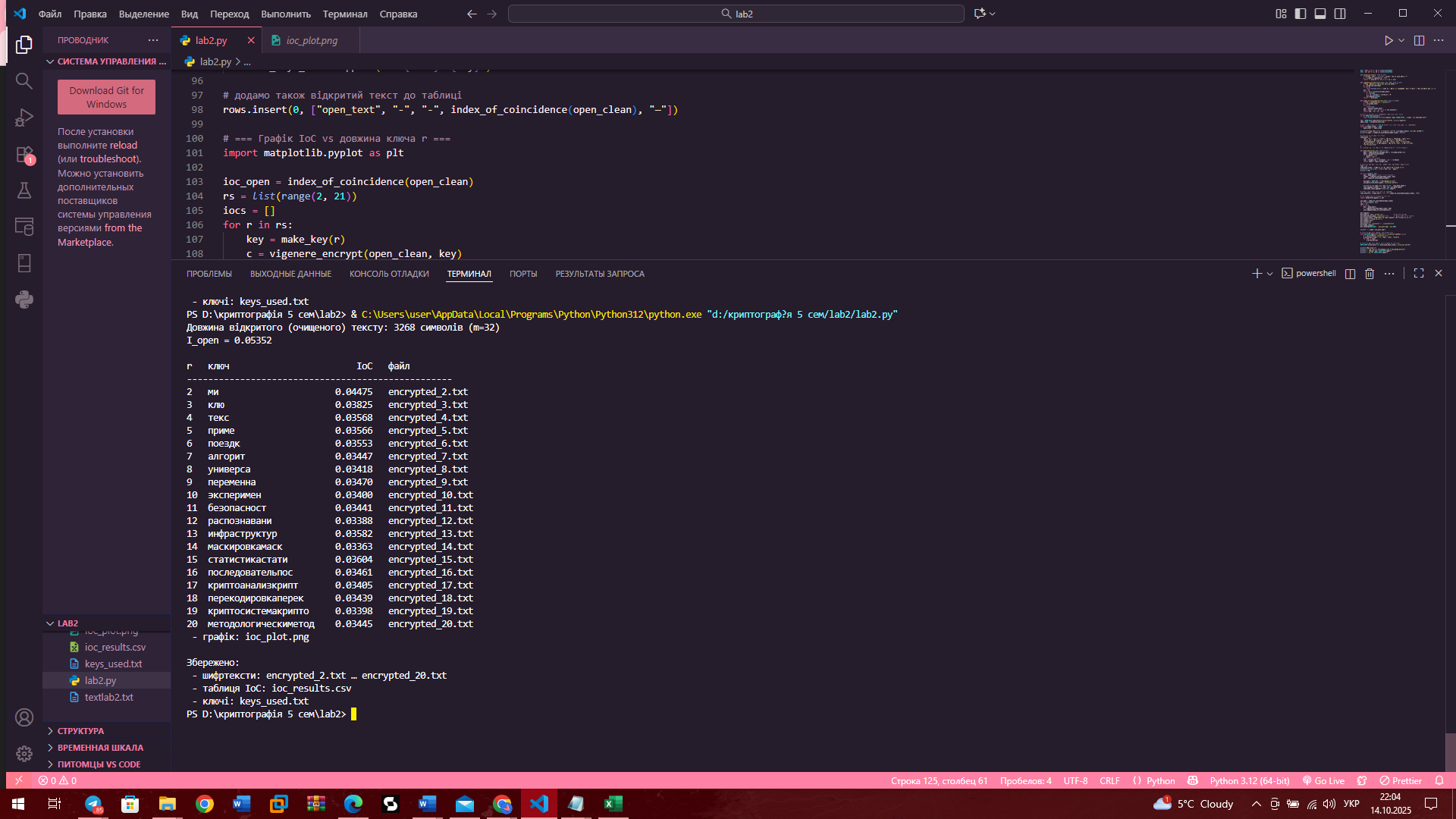
ключі

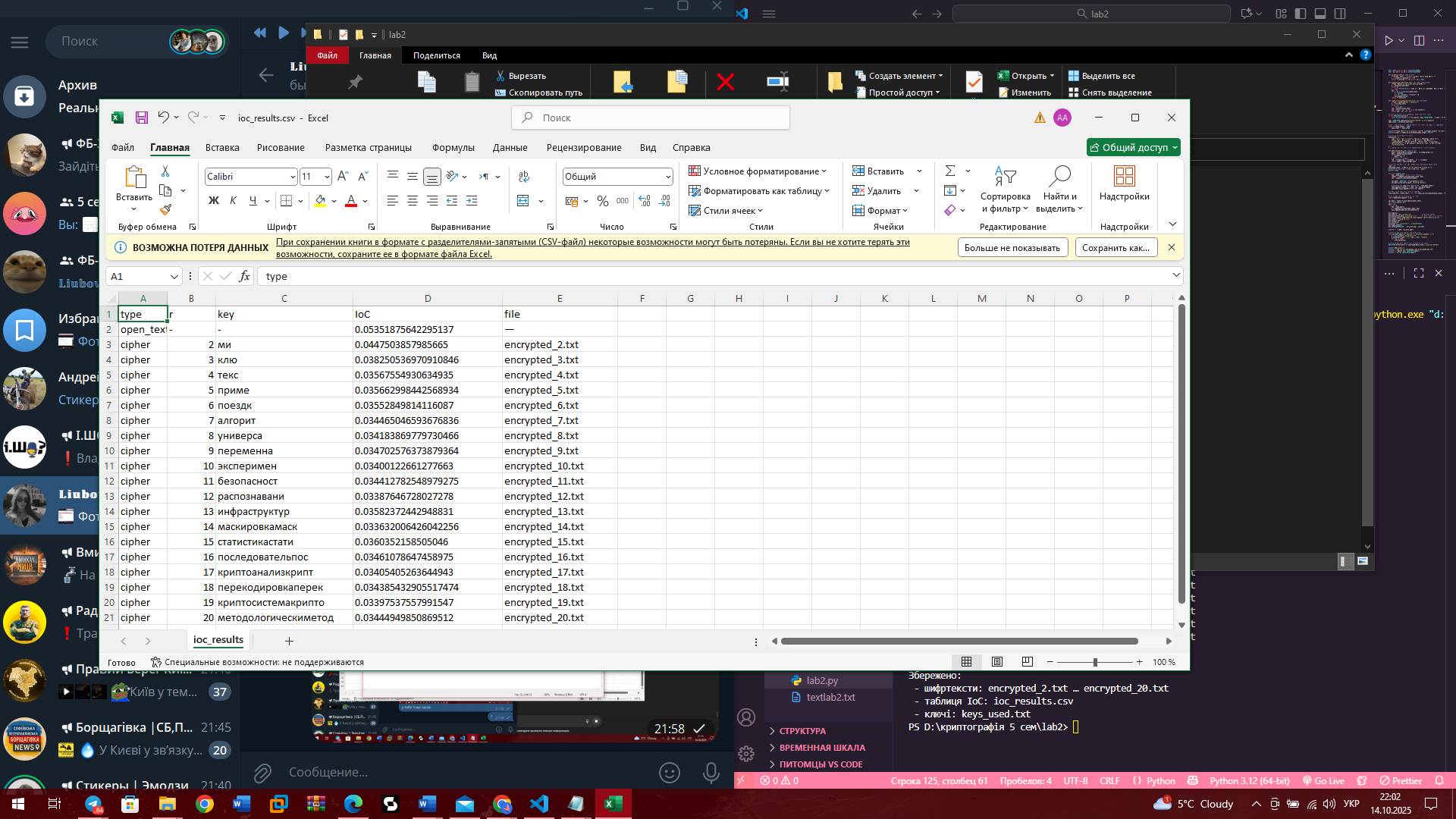


Отримали



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







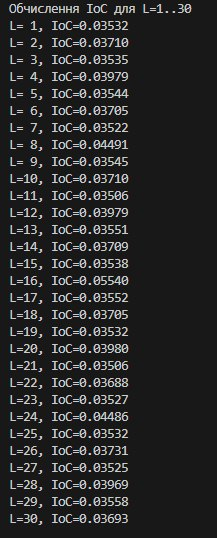
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта). **Варіант 5**

Довжина очищеного тексту

Після попередньої обробки (видалення пробілів, пунктуації, небукв) текст має 5614 символів.  

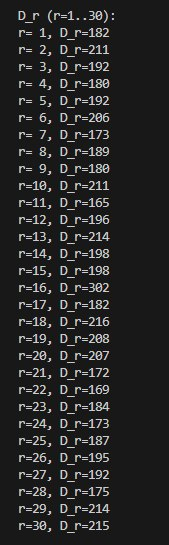

Цей крок важливий для правильного розрахунку індексу відповідності (IoC) і поділу на блоки при криптоаналізі.

Обчислення IoC для L=1..30

IoC (Index of Coincidence) оцінює ймовірність випадкового співпадіння букв у тексті. Для різних довжин ключа L розраховується IoC блоку тексту.  


Вищий IoC свідчить про більш ймовірну довжину ключа.

Обчислення D\_r (відстані повторів)

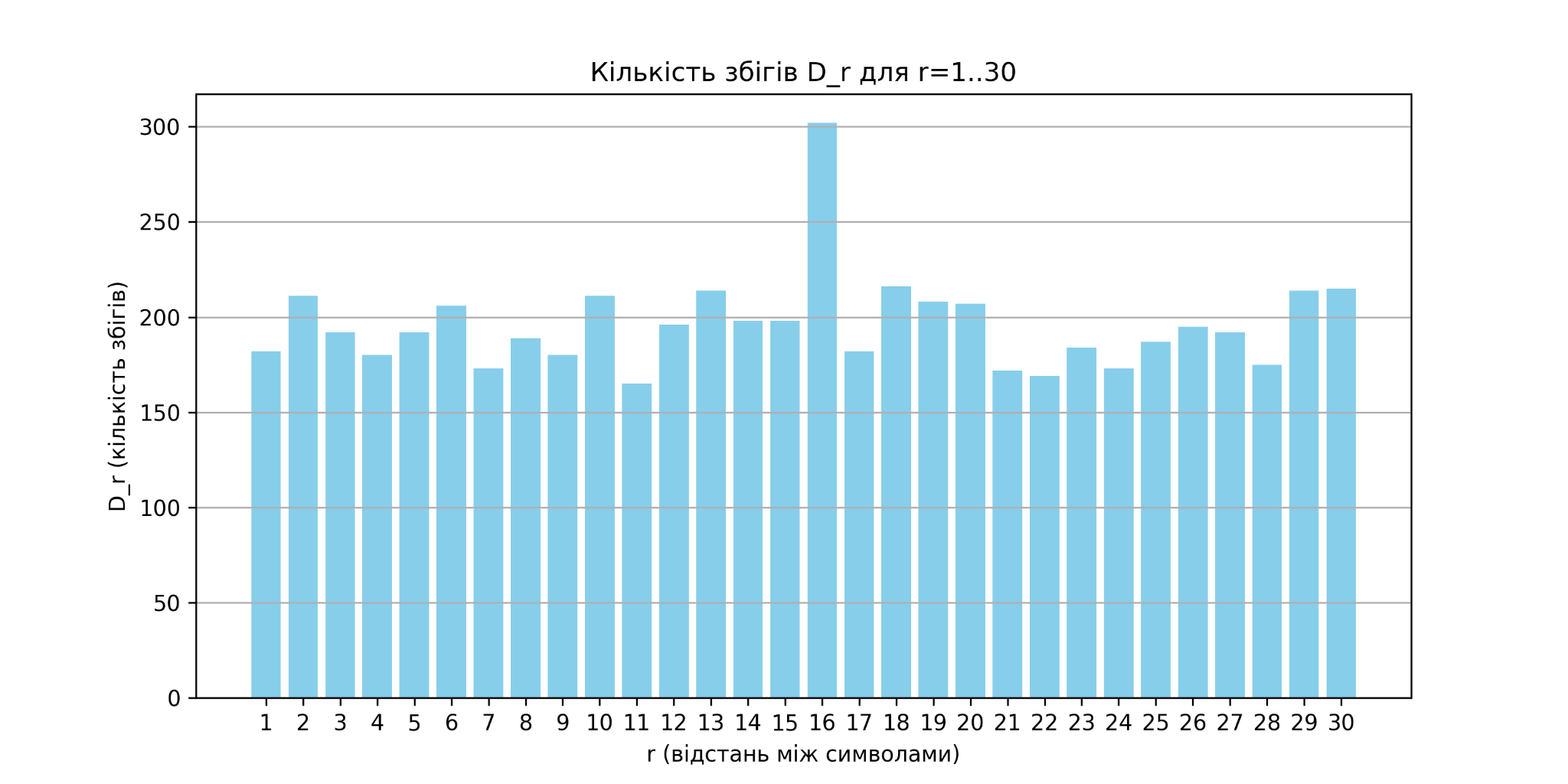


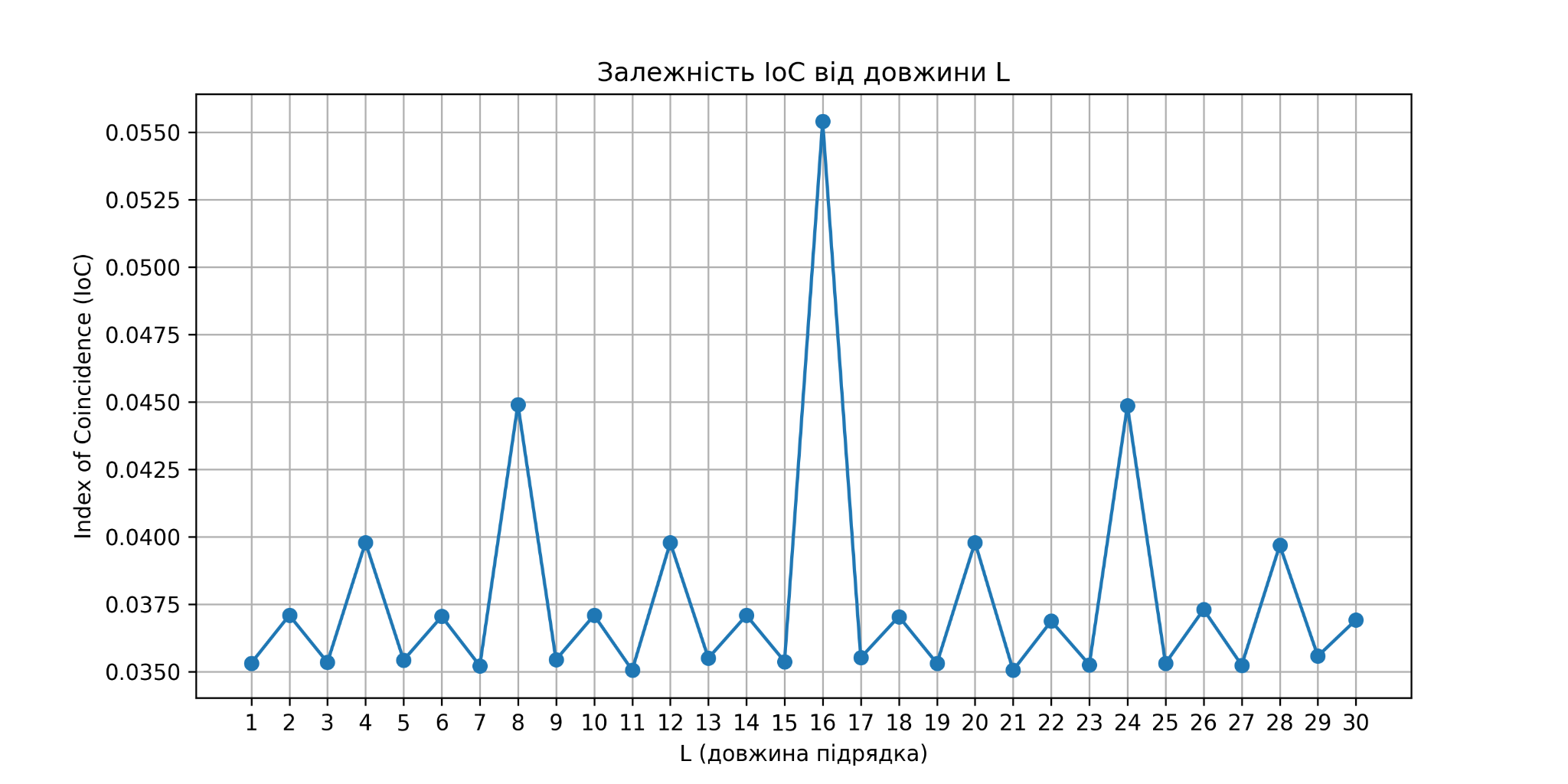
D\_r – статистика для методу Касіскі (визначення періодів повторюваних груп букв). Підтверджує, які довжини ключа можуть бути ймовірними.

Ці значення разом з IoC допомагають скласти список ймовірних довжин ключа.

Графіки обчислених значень IoC для L=1..30 та D\_r (кількість збігів на відстані r)





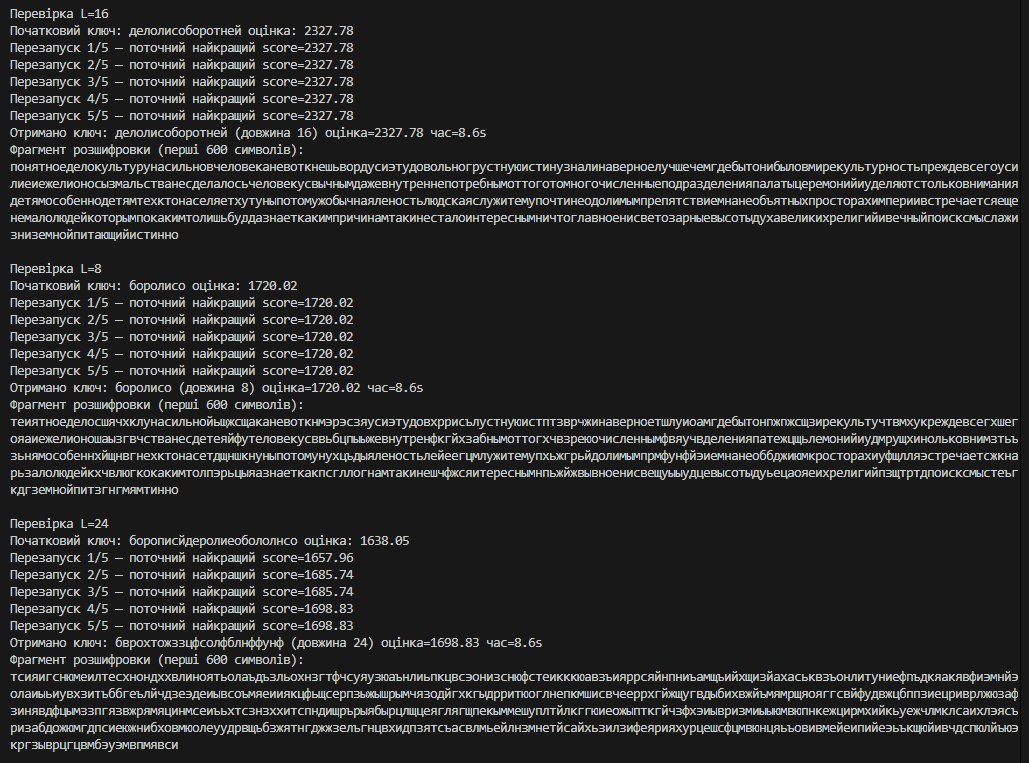


Ймовірні довжини ключа



На основі IoC і D\_r програма обирає декілька найбільш ймовірних довжин ключа для перевірки. Вони будуть оброблятися по черзі у циклі for L in top\_L.

Перевірка конкретної довжини ключа



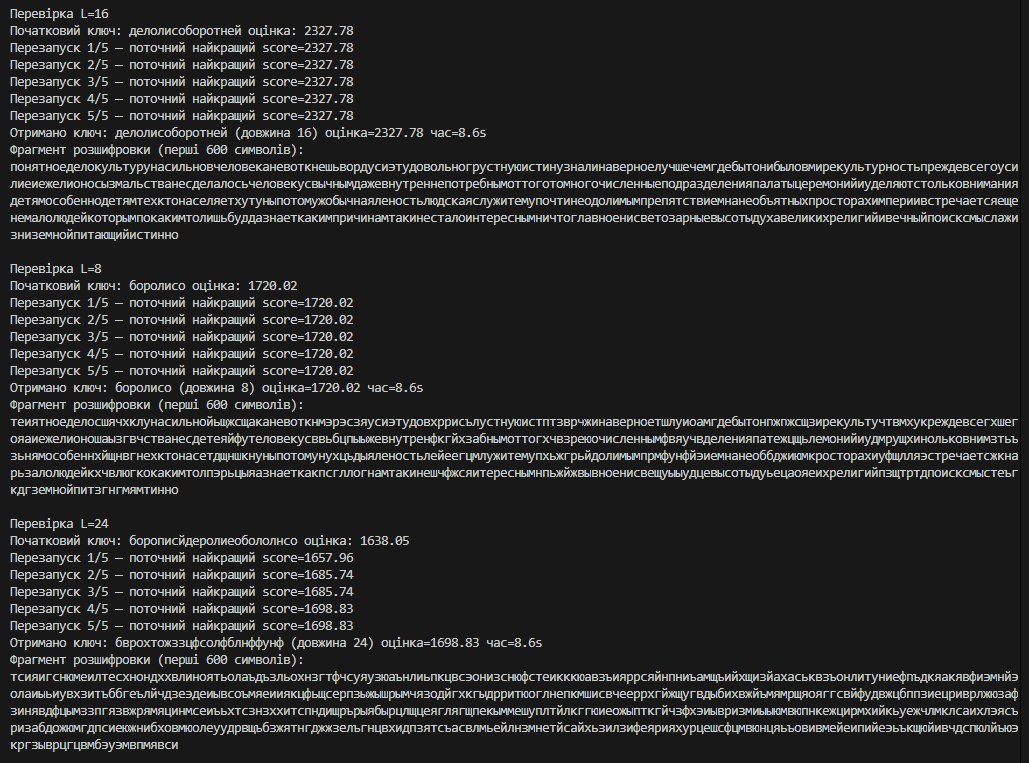
find\_shifts\_chi знайшов початковий ключ через частотний аналіз, оцінка – наскільки осмислений розшифрований текст (метрика score\_text\_words\_ioc).  
Тут ключ: "делолисоборотней" довжиною 16 букв.

improve\_key робить 5 рестартів алгоритму для знаходження оптимального ключа. Кожен рестарт випадково змінює ключ і залишає зміни, якщо score покращується. У цьому випадку початковий ключ вже був оптимальним → score не змінився.

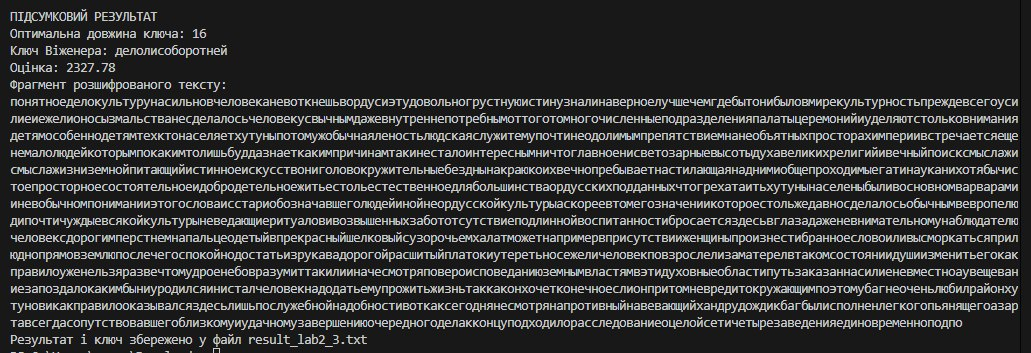
Фінальний ключ і розшифрований фрагмент:

Ключ Віженера: "делолисоборотней"  
Оцінка: 2327.78 (максимальна серед варіантів)  
Час виконання: 8.6 секунди  
Показано перші 600 символів розшифрованого тексту для перевірки осмисленості.

Аналогічна перевірка інших довжин



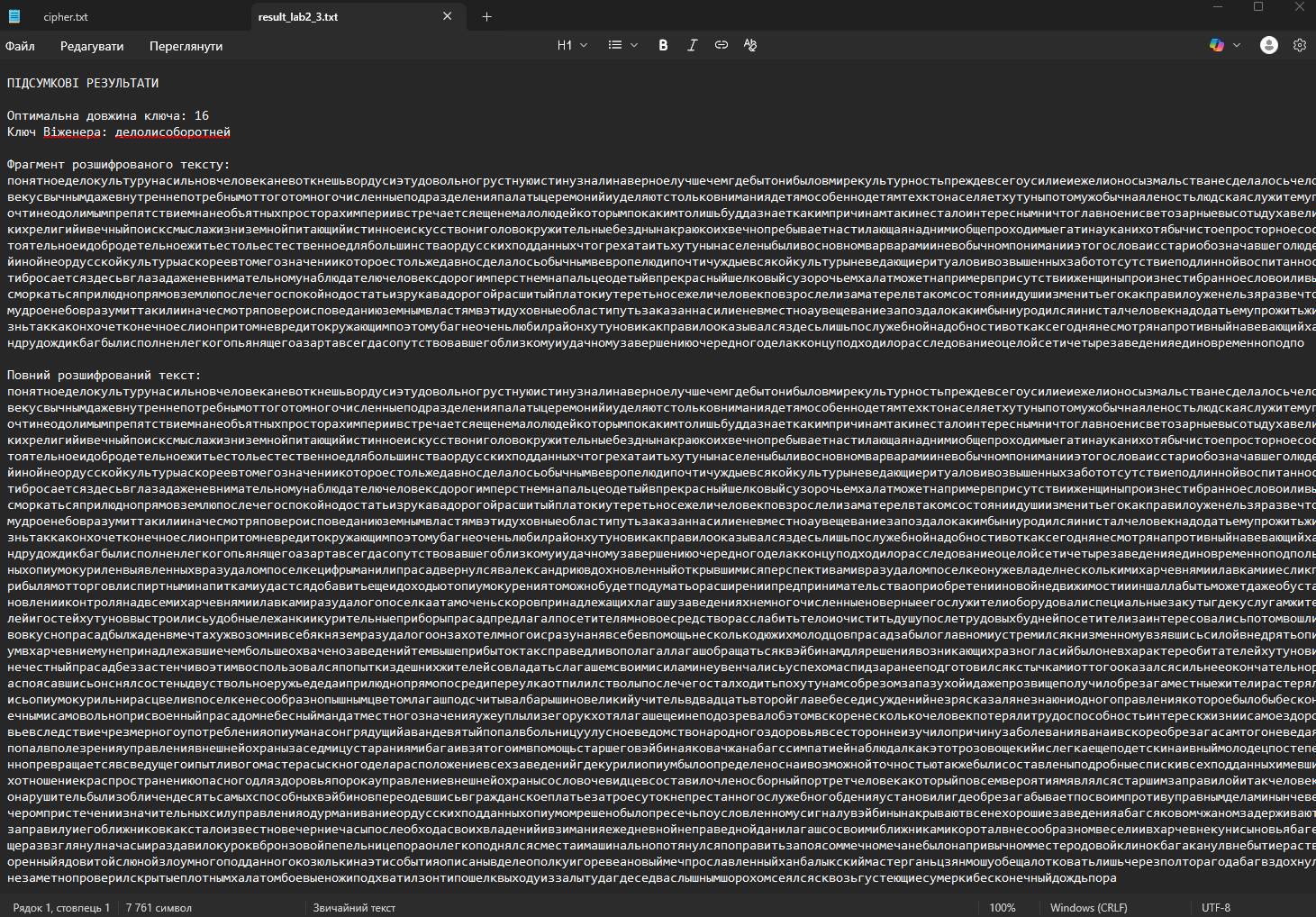
Підсумковий результат



Вибір L=16 як оптимальної довжини ключа підтверджується максимальним score.

Ключ "делолисоборотней" використовується для повної розшифровки тексту.



Результат зберігається у файл result\_lab2\_3.txt.

**Висновки:**

У ході виконання лабораторної роботи було реалізовано шифрування та дешифрування тексту за допомогою шифру Віженера. Для різних довжин ключів (*r = 2…20*) проведено обчислення індексу відповідності (IoC), що дозволило проаналізувати вплив довжини ключа на статистичні властивості шифртексту.

Результати показали, що значення індексу відповідності для відкритого тексту є вищим (приблизно близьким до теоретичного значення для російської мови, ≈0.055), тоді як для шифрованих текстів із короткими ключами спостерігається поступове зменшення IoC до рівня, наближеного до випадкового шуму (~0.035). Це підтвердило, що довший ключ забезпечує вищий рівень криптографічної стійкості.

Під час криптоаналізу невідомого шифртексту за допомогою частотного аналізу та статистичних показників було визначено, що ймовірна довжина ключа дорівнює 16, а знайдений ключ — «делолисоборотней».

Використання цього ключа дало осмислений російський текст, що свідчить про успішне відновлення вихідного повідомлення.

Таким чином, у роботі було:

1. засвоєно принципи шифрування за алгоритмом Віженера;
2. досліджено залежність IoC від довжини ключа;
3. освоєно методи частотного криптоаналізу;
4. відновлено зміст зашифрованого тексту та знайдено правильний ключ.

Отримані результати підтвердили теоретичні закономірності та практичну ефективність методів статистичного аналізу при розшифруванні шифру Віженера.