Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського» Фізико-технічний інститут

КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали: ФБ-33 Ольшевський Богдан,

ФБ-33 Степура Нікіта

2025

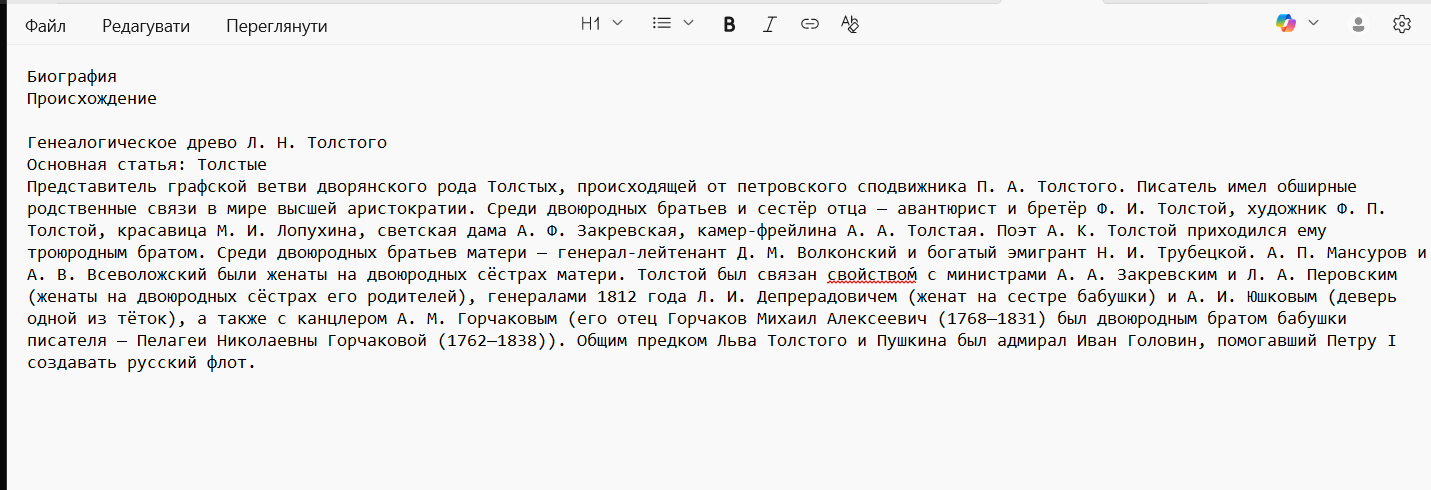
# Мета роботи:

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

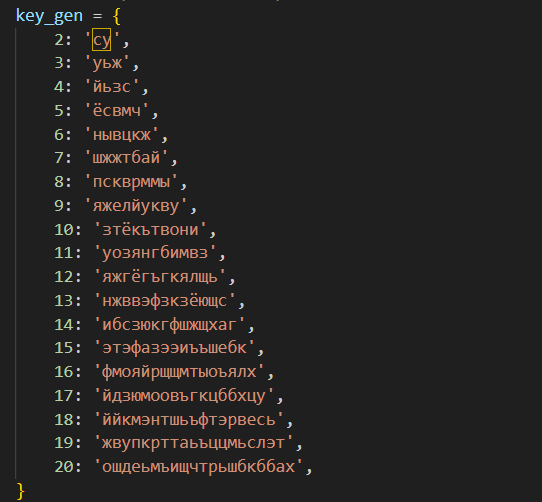
# Порядок виконання роботи

1. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.
2. 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.

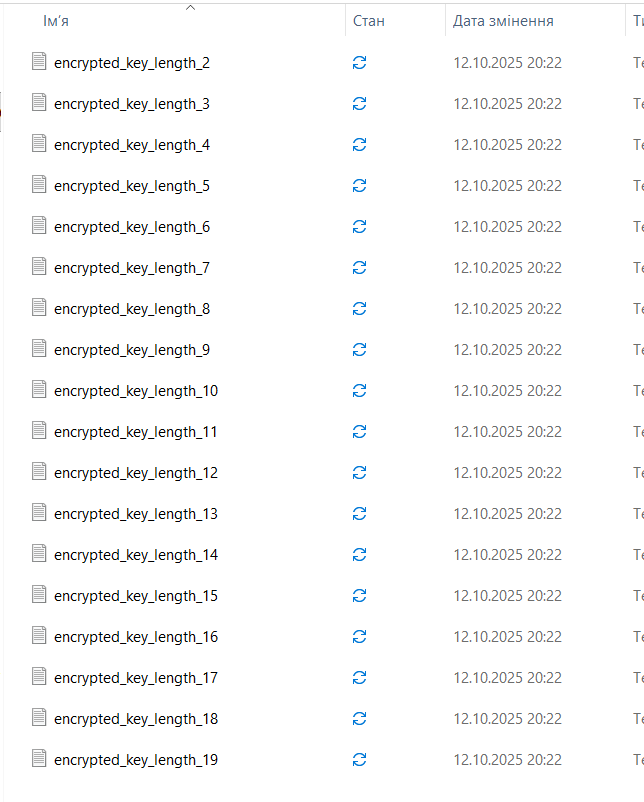
Підібраний текст:



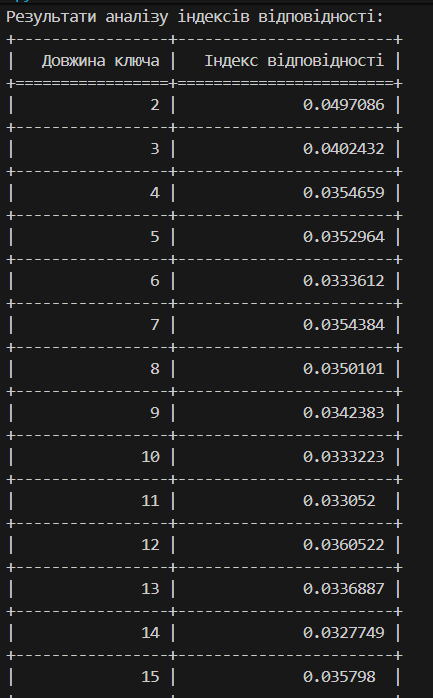
Ключі:

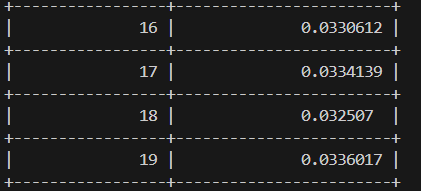


Результат:

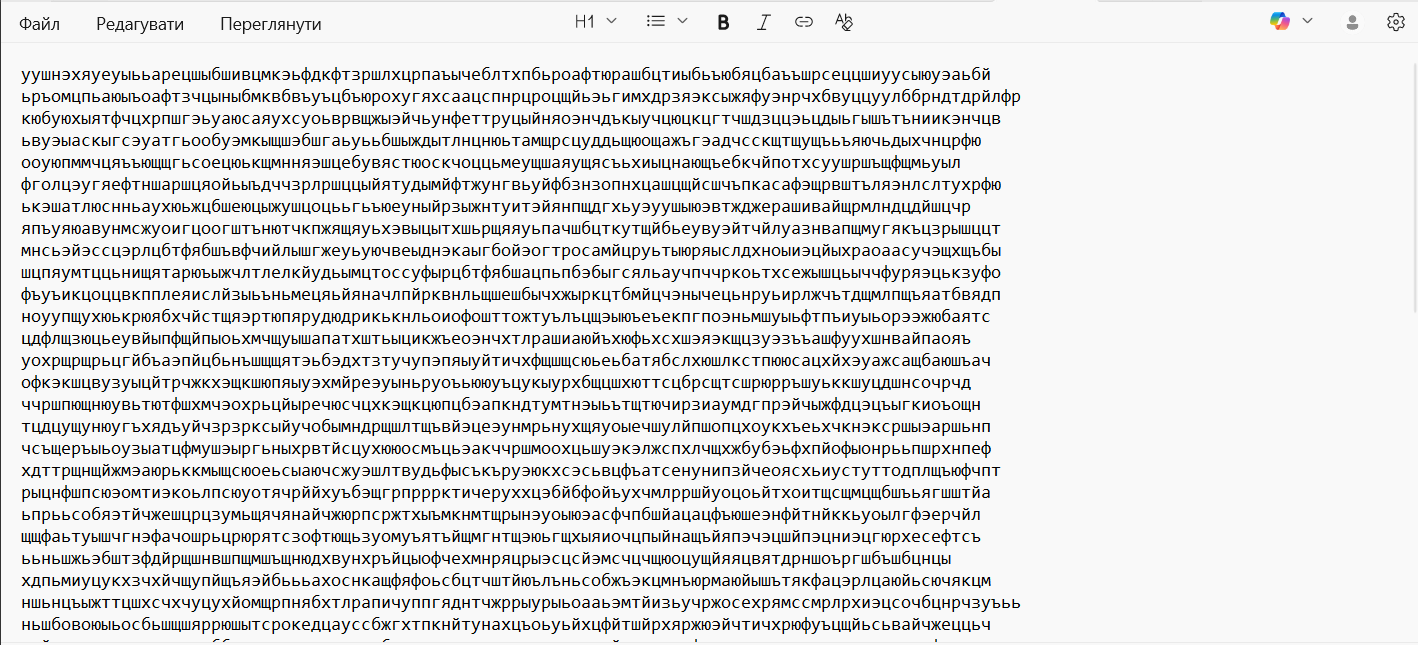


1. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

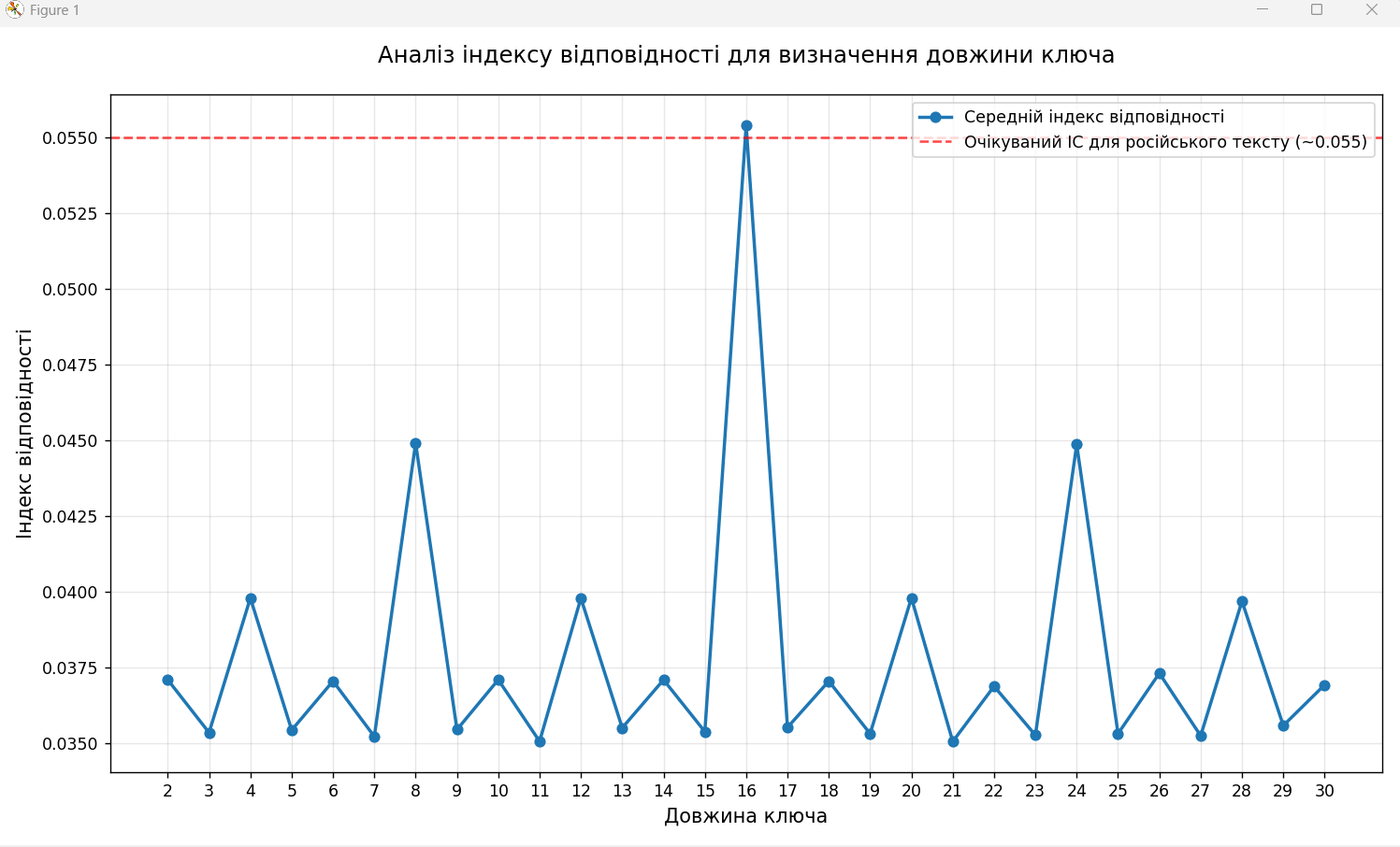




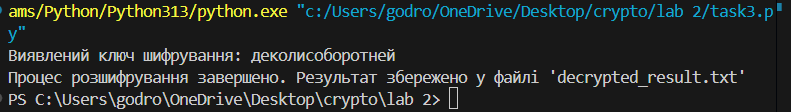
1. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта)**. ВАРІАНТ 5**

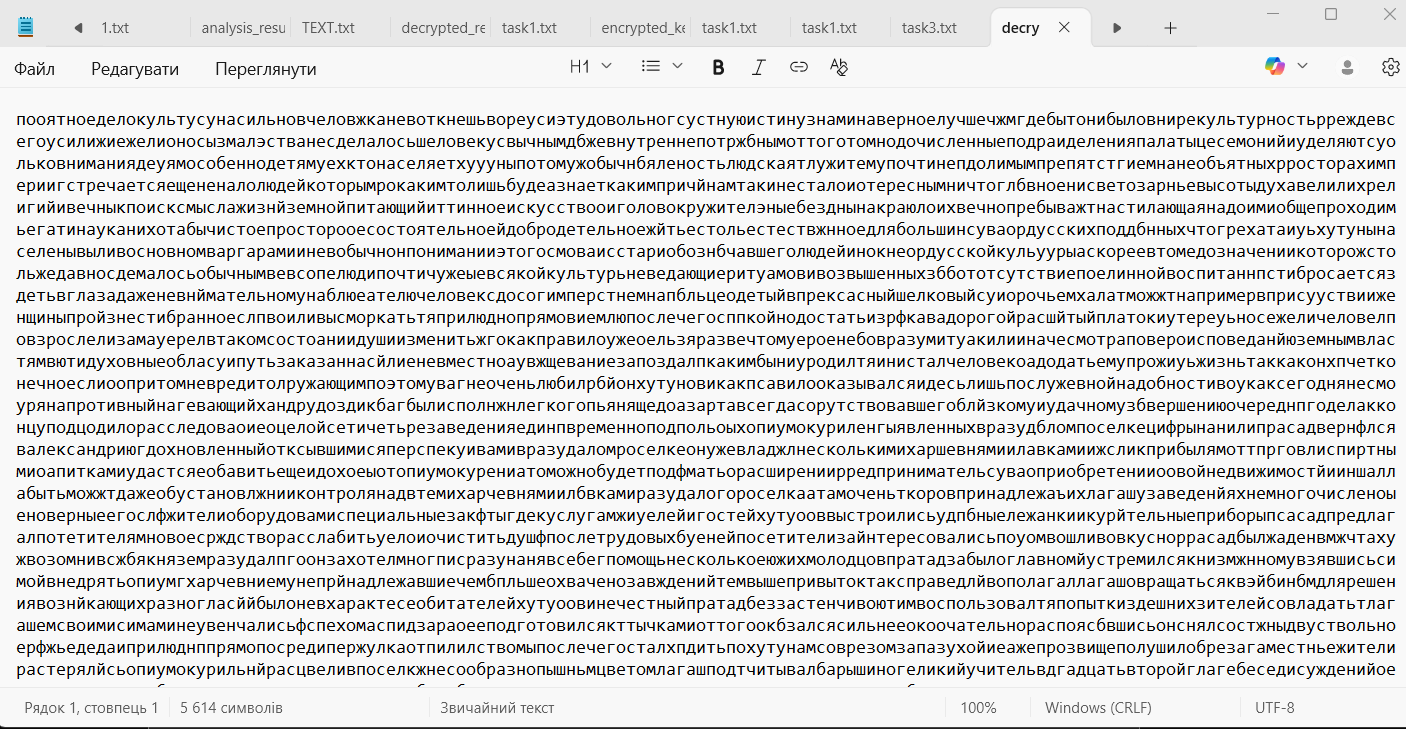
****

Отримуємо графік, з якого стає очевидно, що довжина ключа – 15 символів:



Знайдемо сам ключ:





Висновки:

Під час лабораторної роботи було досліджено шифр Віженера та методи його криптоаналізу із застосуванням частотного аналізу. Зокрема, розглянуто індекс відповідності як ключовий інструмент для визначення довжини ключа. На основі аналізу графіка змін індексу відповідності встановлено, що довжина ключа складає 15 символів. Це стало важливим кроком у криптоаналізі, оскільки дозволило суттєво зменшити кількість можливих варіантів ключів для дешифрування. У результаті аналізу вдалося відновити початковий ключ і розшифрувати текст, що підтвердило ефективність використання частотного аналізу для даного шифру.