КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:
ФБ-31 Голомовза Дар`я

ФБ-31 Караман Любов

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.

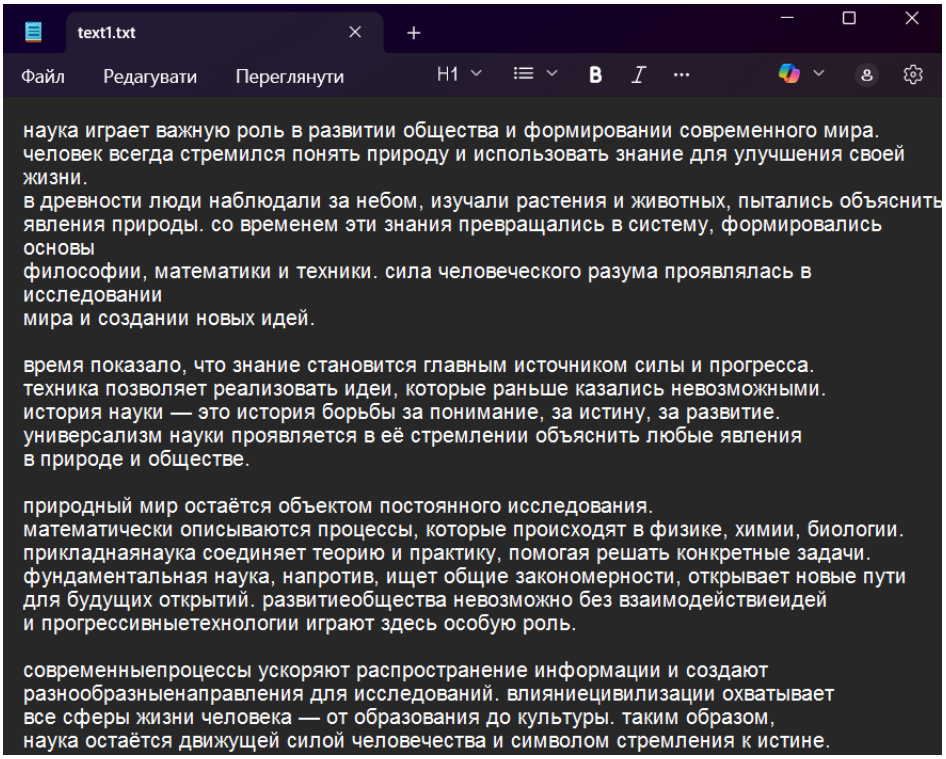
У роботі було використано шифр *Віженера* — класичний поліалфавітний шифр підстановки, який реалізує адитивне гамування символів відкритого тексту ключем, що періодично повторюється.

Формула шифрування Віжера:

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

Реалізація:

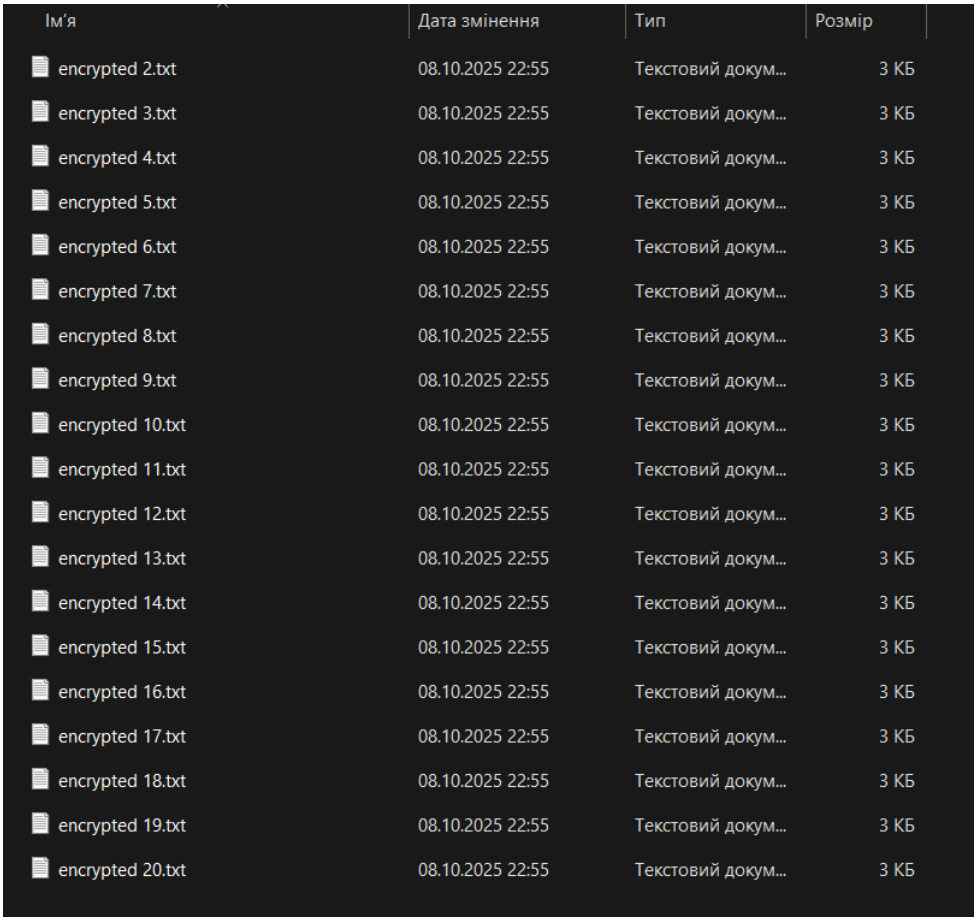
Створено файл text1.txt, який містить російський текст:



Використані ключі різної довжини (від 2 до 20 символів), наприклад:

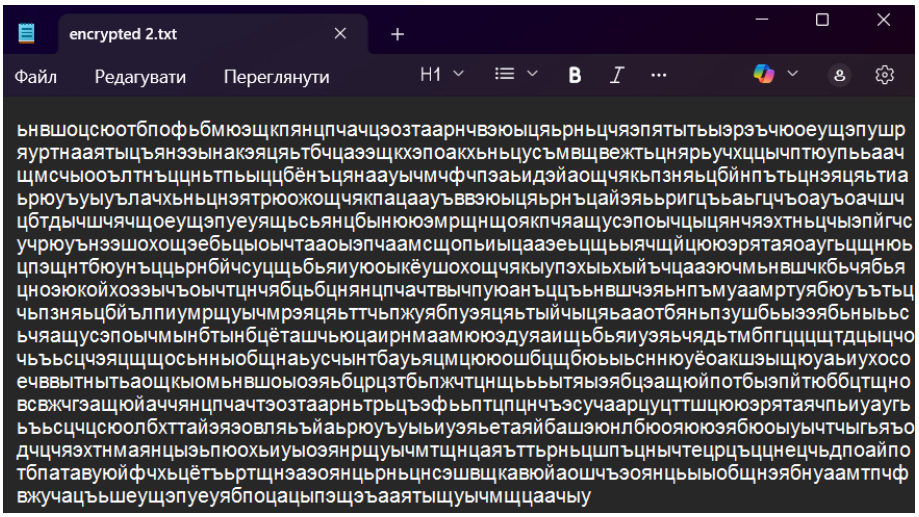
```
    s = {
        2: 'он', 3: 'лет', 4: 'сила', 5: 'время',
        6: 'знание', 7: 'техника', 8: 'история', 9: 'универсал',
        10: 'природный', 11: 'исследование', 12: 'математически',
        13: 'прикладнаянаука', 14: 'фундаментальная',
        15: 'развитиеобщества', 16: 'взаимодействиеидей',
        17: 'современныепроцессы', 18: 'прогрессивныетехнологии',
        19: 'разнообразныенаправления', 20: 'влияниецивилизации'
    }
```

Після запуску програми отримуємо папку encrypt з файлами:



Ім'я	Дата змінення	Тип	Розмір
encrypted 2.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 3.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 4.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 5.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 6.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 7.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 8.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 9.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 10.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 11.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 12.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 13.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 14.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 15.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 16.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 17.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 18.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 19.txt	08.10.2025 22:55	Текстовий докум...	3 КБ
encrypted 20.txt	08.10.2025 22:55	Текстовий докум...	3 КБ

Відкриємо для прикладу перший файл:



Шифр Віженера реалізовано успішно.

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

Для підрахунку використовуємо формулу:

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

де N (Y) t – кількість появ букви t у шифртексті Y

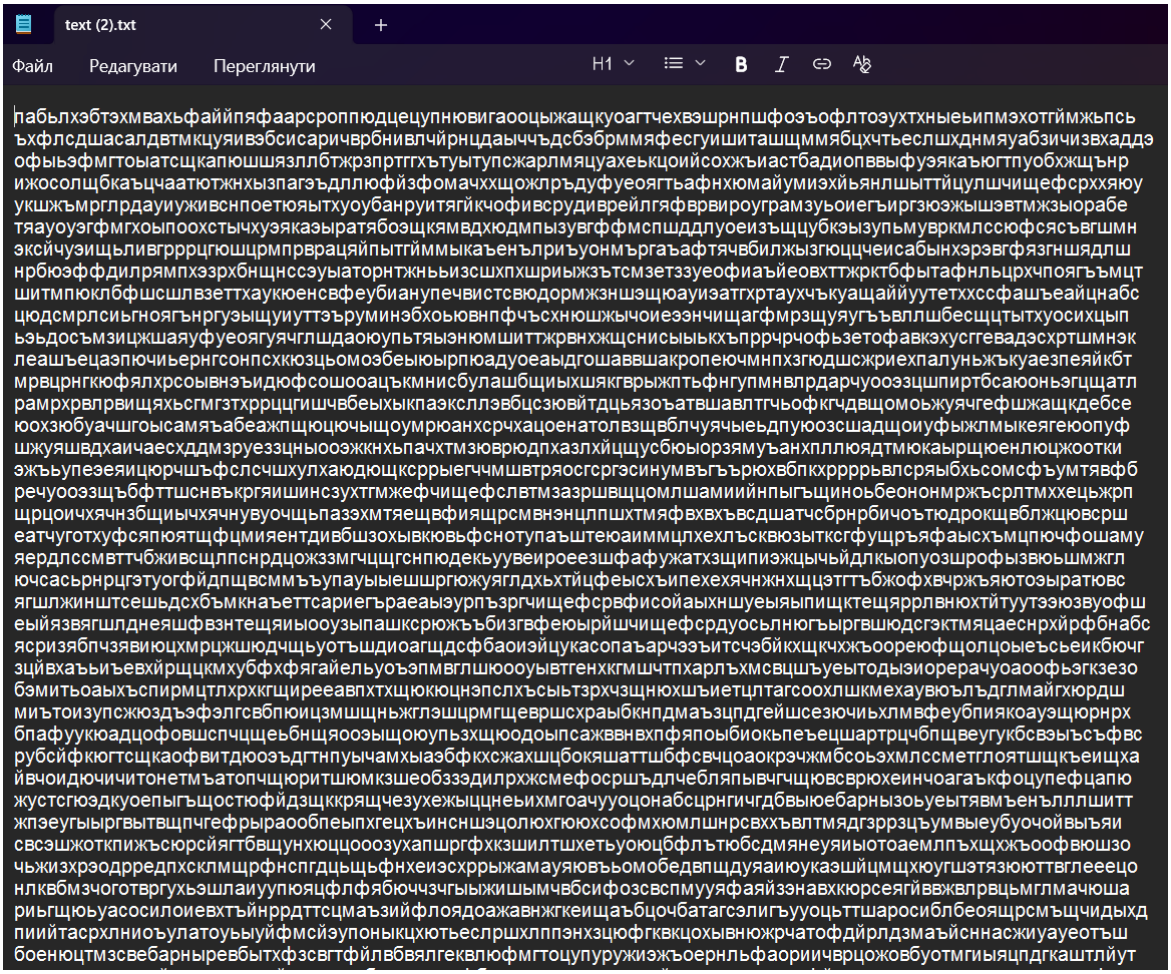
```
=== ІНДЕКС ВІДПОВІДНОСТІ ДЛЯ РІЗНИХ ДОВЖИН КЛЮЧА ===
Довжина    |              IC
----------------------------
2          |    0.0475141777
3          |    0.0383704734
4          |    0.0382858680
5          |    0.0358323094
6          |    0.0390447916
7          |    0.0351567285
8          |    0.0369043996
9          |    0.0334987139
10         |    0.0336022609
11         |    0.0356428942
12         |    0.0372743907
13         |    0.0333850647
14         |    0.0356441570
15         |    0.0333219263
16         |    0.0354522162
17         |    0.0343270898
18         |    0.0342109151
19         |    0.0336401439
20         |    0.0380901389
----------------------------
```

Отримані результати підтвердили, що з ростом довжини ключа індекс відповідності наближається до випадкового розподілу символів.

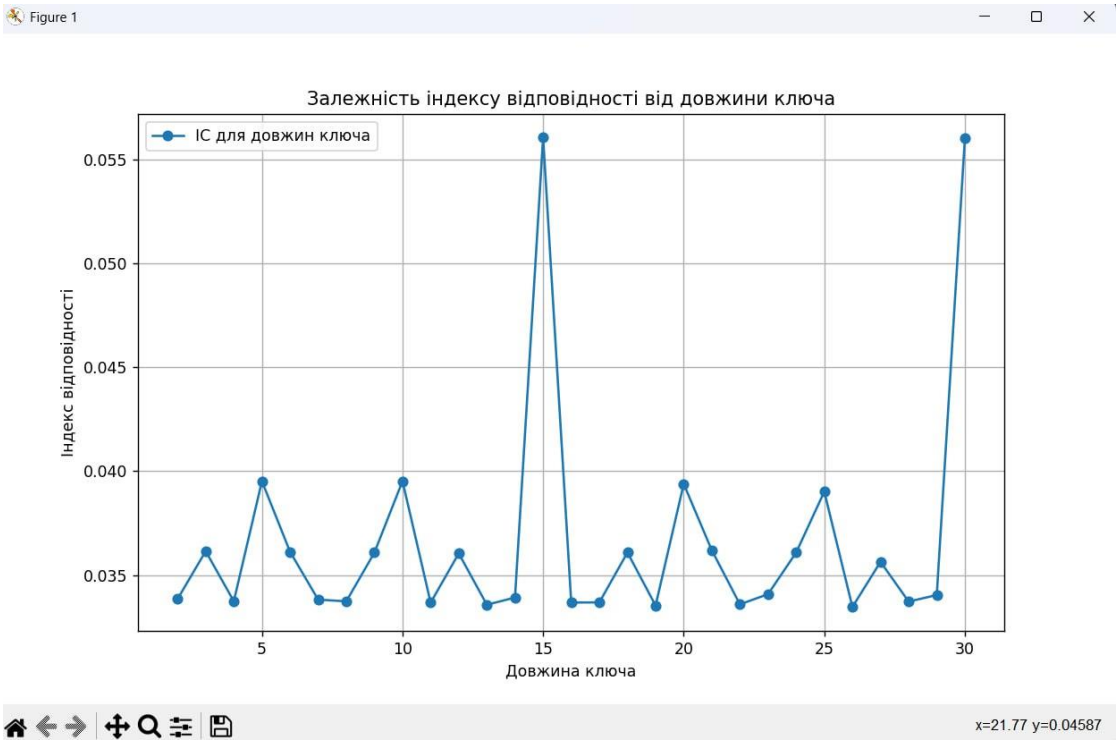
На графіку показано зміну індексу відповідності залежно від довжини ключа: при коротких ключах (2–5) IC має відносно великі значення, близькі до IC природної мови, а при збільшенні довжини ключа IC зменшується, наближаючись до значення випадкового тексту.

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

Варіант 7



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



Знайдемо ключ:

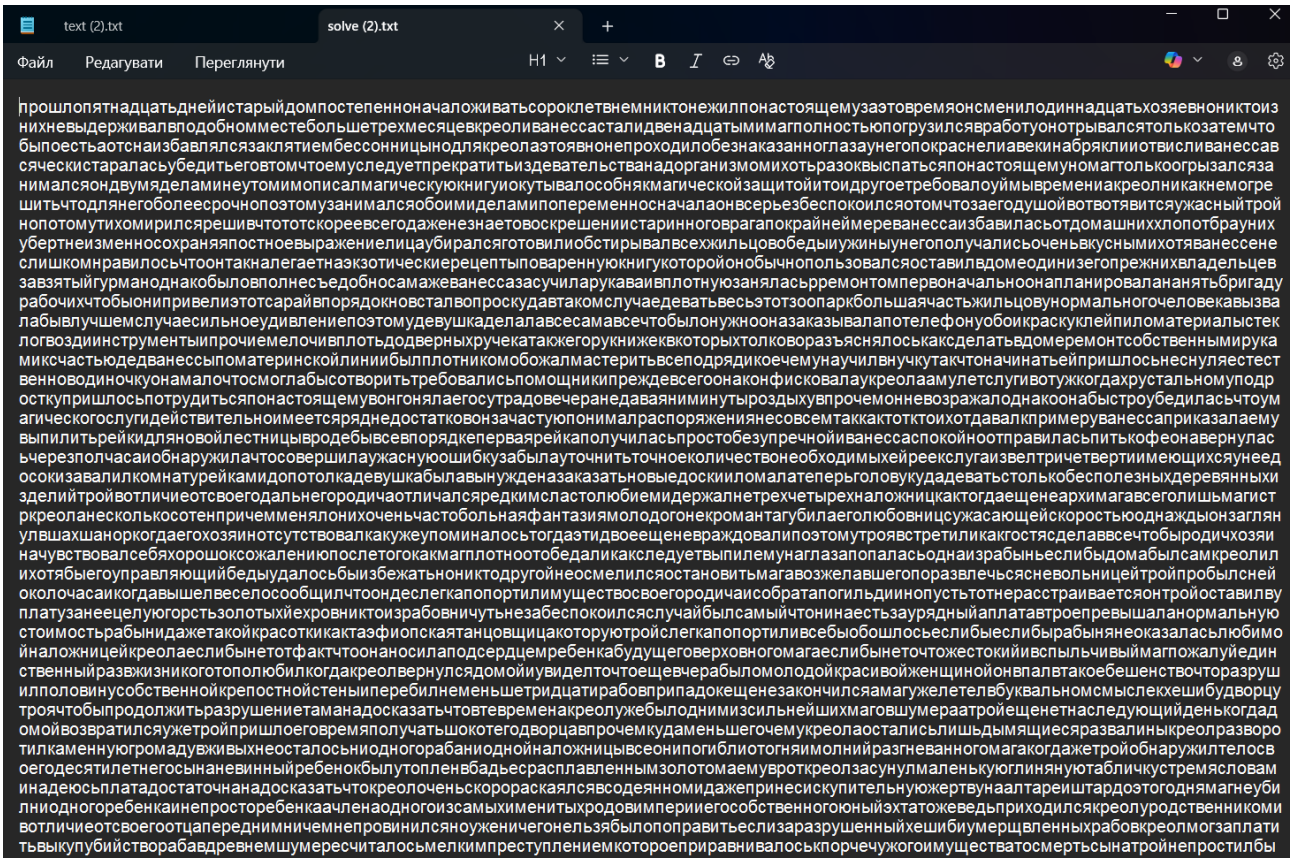
```
[Running] python -u "d:\3 курс\Crypto\lab2\task3_2.py"
Знайдений ключ: арудазовархимаг
Розшифрований текст збережено в solve.txt
```

Ключ – **Арудазовархимаг**

Формула для ключа:

$$k = (y^* - x^*) \bmod m$$

де y* – буква, що частіше за всіх зустрічається у фрагменті Y_i , а x* – найімовірніша буква у мові, якою написано відкритий текст



Розшифрувати текст, зашифрований шифром Віженера, без попереднього знання ключа, використовуючи метод частотного аналізу.

Висновки

Під час виконання лабораторної роботи було досліджено шифр Віженера та методи його криптоаналізу з використанням частотного аналізу. Зокрема, приділено увагу індексу відповідності як основному засобу для визначення довжини ключа. Аналіз отриманих даних та графіка змін індексу відповідності дозволив встановити, що довжина ключа становить 15 символів. Це значно звузило коло можливих варіантів ключів для розшифрування. Завдяки застосуванню частотного аналізу вдалося відновити початковий ключ і успішно розшифрувати текст, що підтвердило ефективність цього методу для роботи з шифром Віженера.