Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:  
ФБ-21 Худоба Арсен,

ФБ-21 Шабанов Кирило

**Мета роботи:**

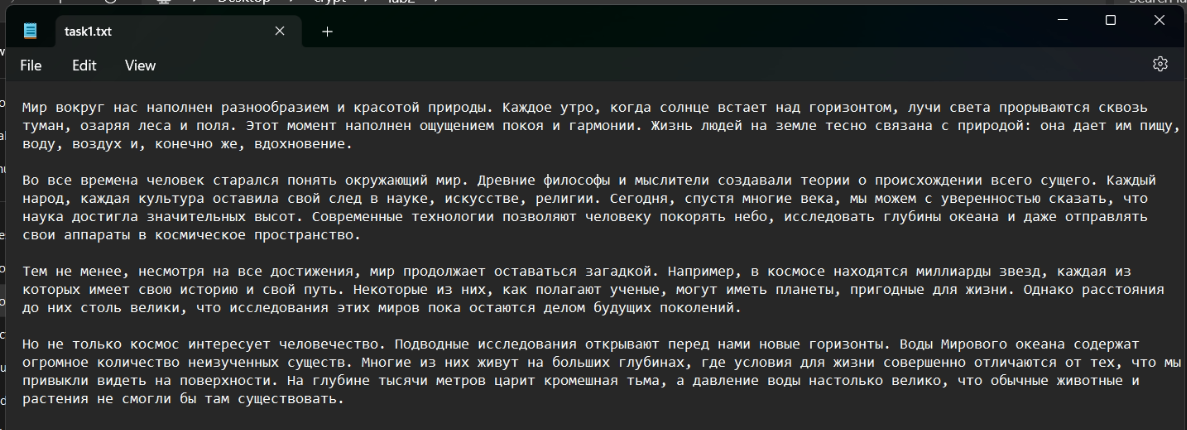
Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера

**Порядок виконання роботи**

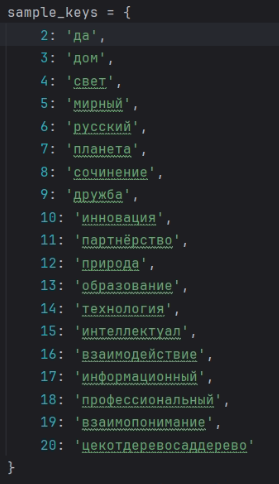
0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

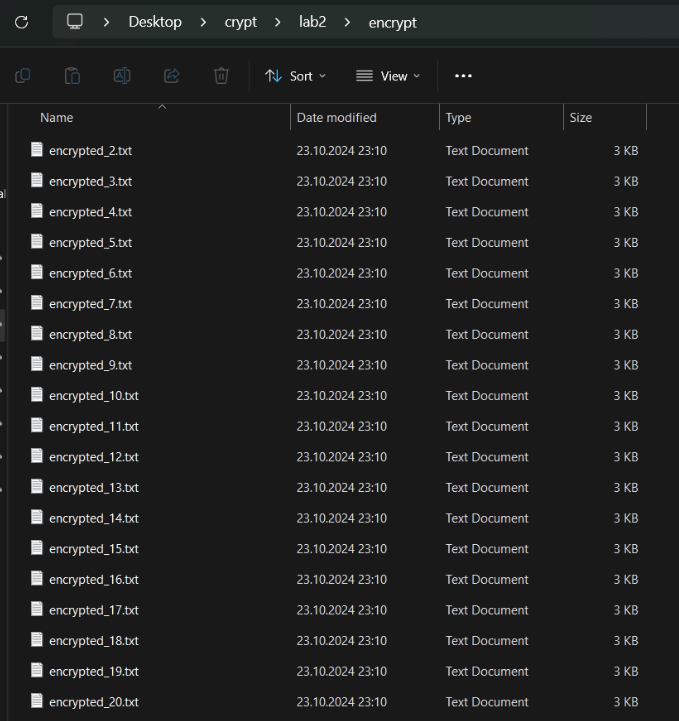
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.

Підібраний текст:



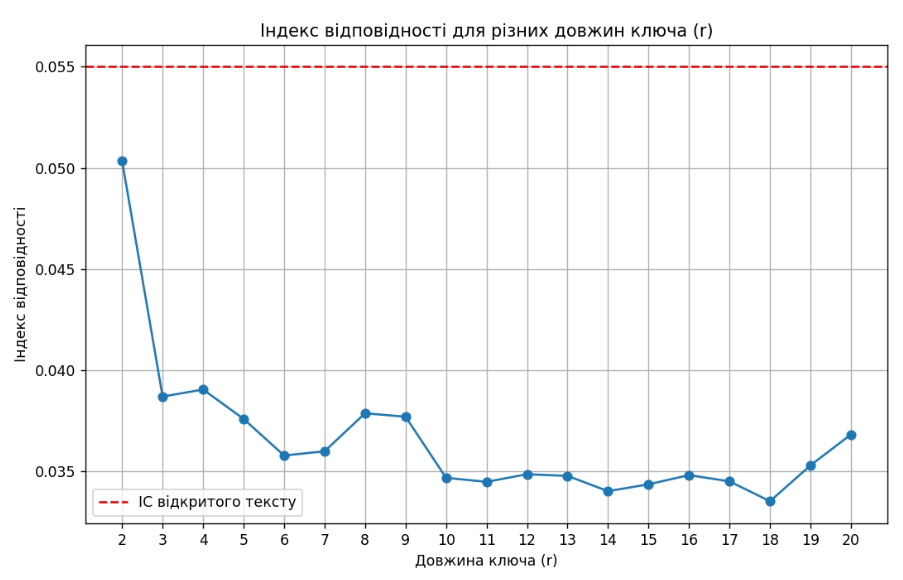
Ключі:

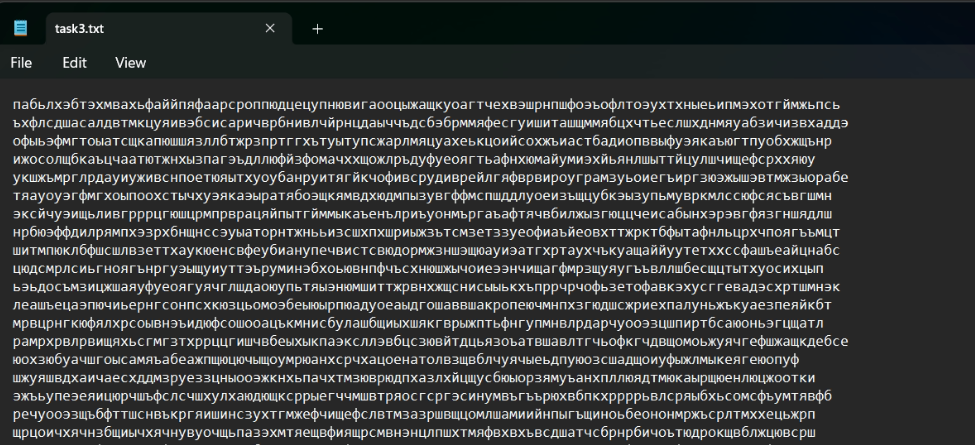


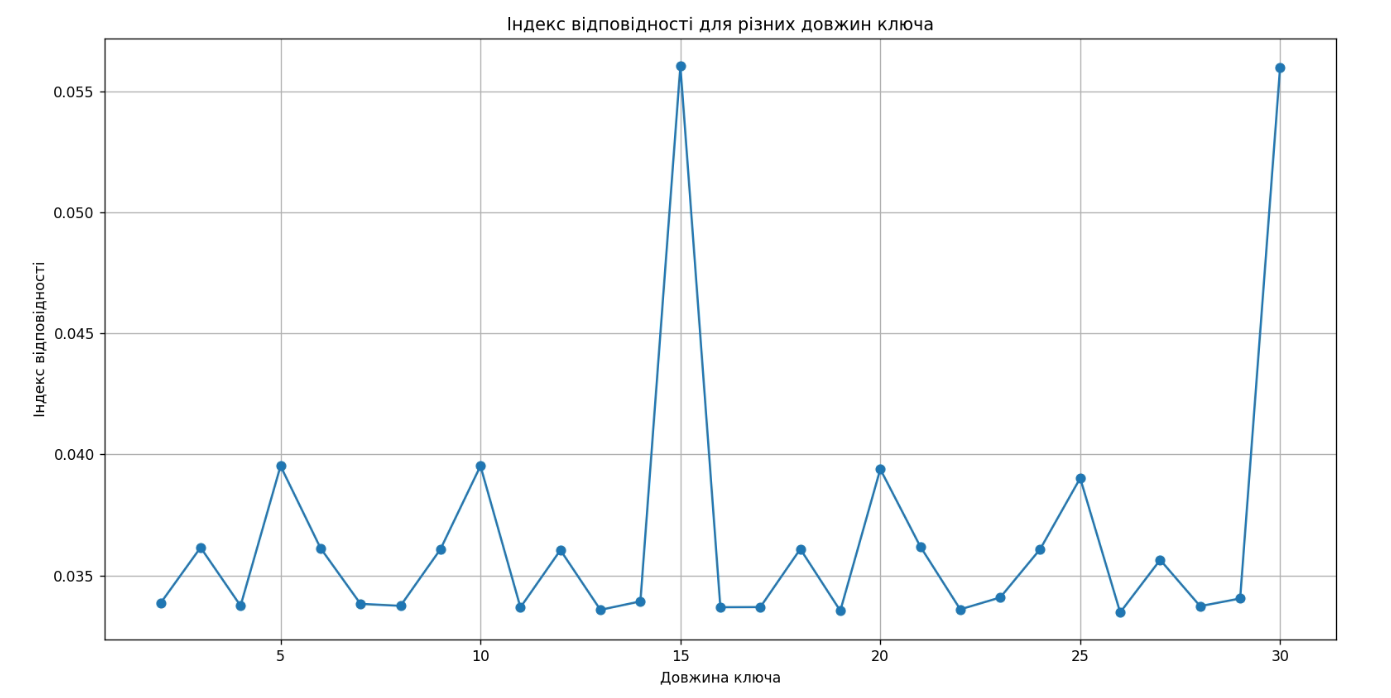


2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

|  |  |
| --- | --- |
| Довжина ключа (r) | Індекс відповідності |
| 2 | 0.050332 |
| 3 | 0.0386978 |
| 4 | 0.0390486 |
| 5 | 0.0375947 |
| 6 | 0.0357864 |
| 7 | 0.0359953 |
| 8 | 0.0378751 |
| 9 | 0.037702 |
| 10 | 0.0346832 |
| 11 | 0.0344859 |
| 12 | 0.0348621 |
| 13 | 0.0347802 |
| 14 | 0.0340243 |
| 15 | 0.0343647 |
| 16 | 0.0348182 |
| 17 | 0.034509 |
| 18 | 0.0335281 |
| 19 | 0.0353006 |
| 20 | 0.0368273 |

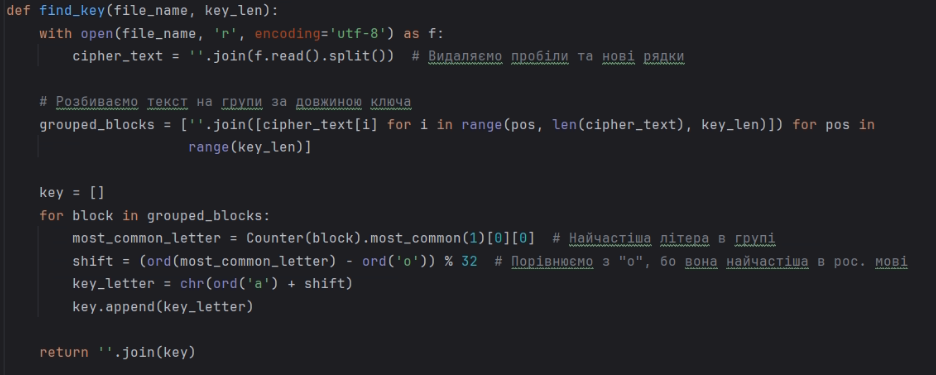


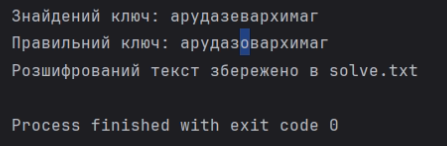
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).



З графіка стає очевидно, що довжина ключа – 15 символів.

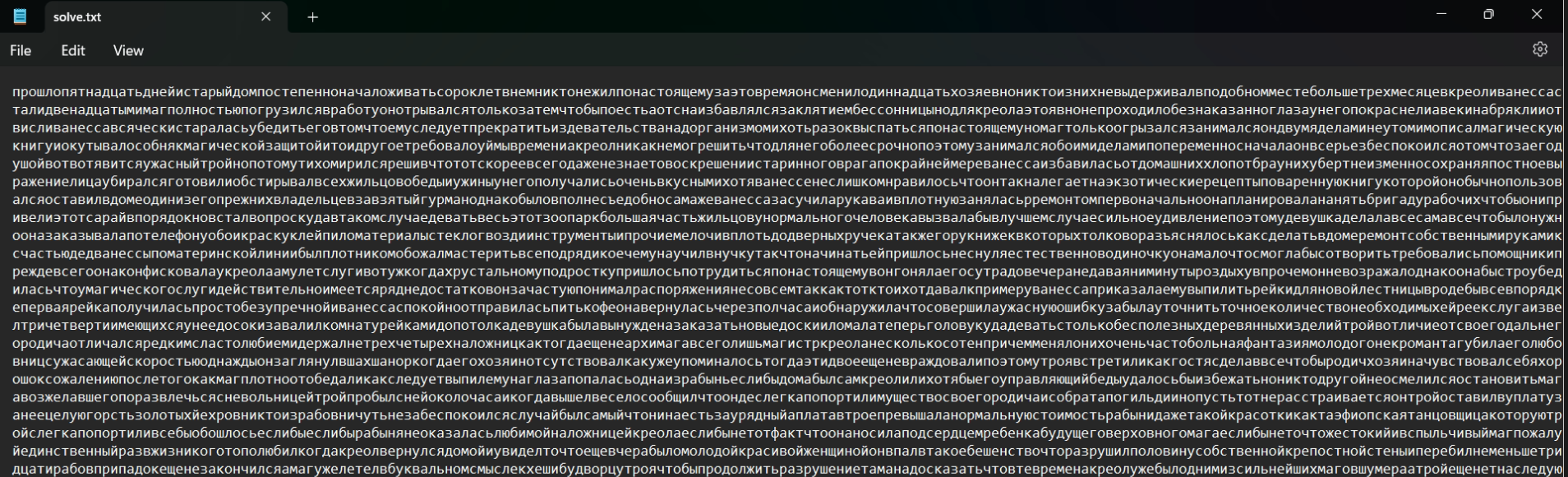
Знайдемо сам ключ:





**арудазевархимаг**

**арудазовархимаг**



Висновки:

У процесі виконання лабораторної роботи було розглянуто шифр Віженера і методи частотного аналізу для його криптоаналізу. Ми ознайомилися з індексом відповідності, що є важливим інструментом для визначення довжини ключа при криптоаналізі шифрів. На основі графіка зміни індексу відповідності встановлено, що довжина ключа становить 15 символів. Це є важливим кроком у криптоаналізі шифру Віженера, що дозволяє значно звузити коло можливих ключів для подальшого розшифрування. Використовуючи отримані знання та проведений аналіз, вдалося відновити оригінальний ключ для шифру Віженера та розшифрувати зашифрований текст. Це підтверджує ефективність методу частотного аналізу для цього типу шифрів.