Криптографія

Комп’ютерний практикум №2

Криптоаналіз шифру Віженера

Виконали

Студенти 3-го курсу

Групи ФБ-02

Замрій Денис,

Гнатюк Максим

Мета роботи:

Засвоєння методів часткового криптоаналізу. Здобуття навичок роботи та аналізу поточних шифрів гамування адитивного типу та прикладів 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.

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).

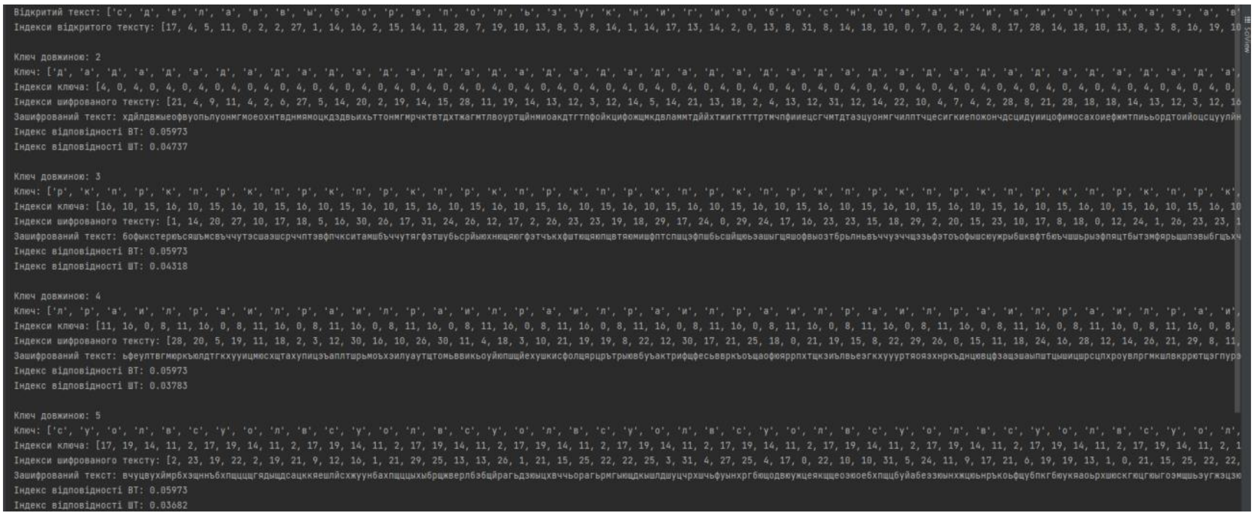
Використовували такі формули:

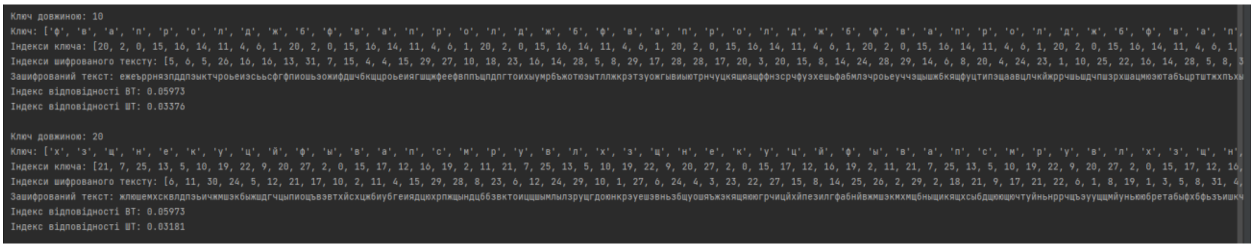
Формула індексу відповідності:

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

Шифр Віженера:

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





Індекс відповідності ВТ: 0.05973

Ключ довжиною: 2
Індекс відповідності ШТ: 0.04737

Ключ довжиною: 3
Індекс відповідності ШТ: 0.04318

Ключ довжиною: 4
Індекс відповідності ШТ: 0.03783

Ключ довжиною: 5
Індекс відповідності ШТ: 0.03682

Ключ довжиною: 10
Індекс відповідності ШТ: 0.03376

Ключ довжиною: 20
Індекс відповідності ШТ: 0.03181

Побачили, що чим довший ключ, тим менший індекс відповідності.

Висновок:
В ході лабораторної роботи навчилися використовувати шифр Віженера на практиці, Знайшли індекси відповідності для кожної довжини ключа.