Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Лабораторна робота №2

Криптоаналіз шифру Віженера

Виконали:
студентки ФБ-06
Товкач К.В.
Вєрнікова Л.Г.

Київ – 2022

Варіант 10

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.
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).

Хід роботи:

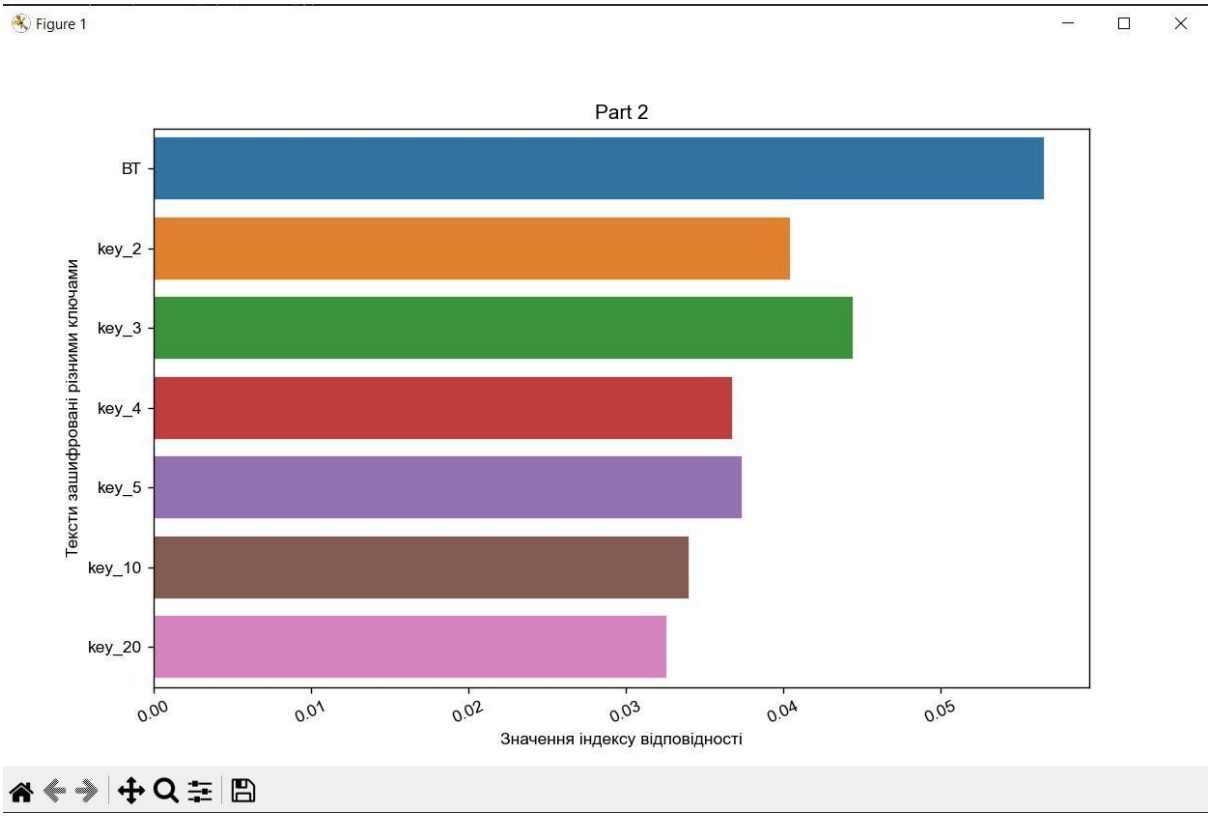
Порахували індекси відповідності для різних значень r шифротексту, отримали наступні значення:

r	Індекс
2	0.040480824102661656
3	0.04449478617254916
4	0.03684642033510209
5	0.03740422914857003
10	0.034044960809275056
20	0.032670392191031336

Індекс відкритого тексту: 0.05664286889320178

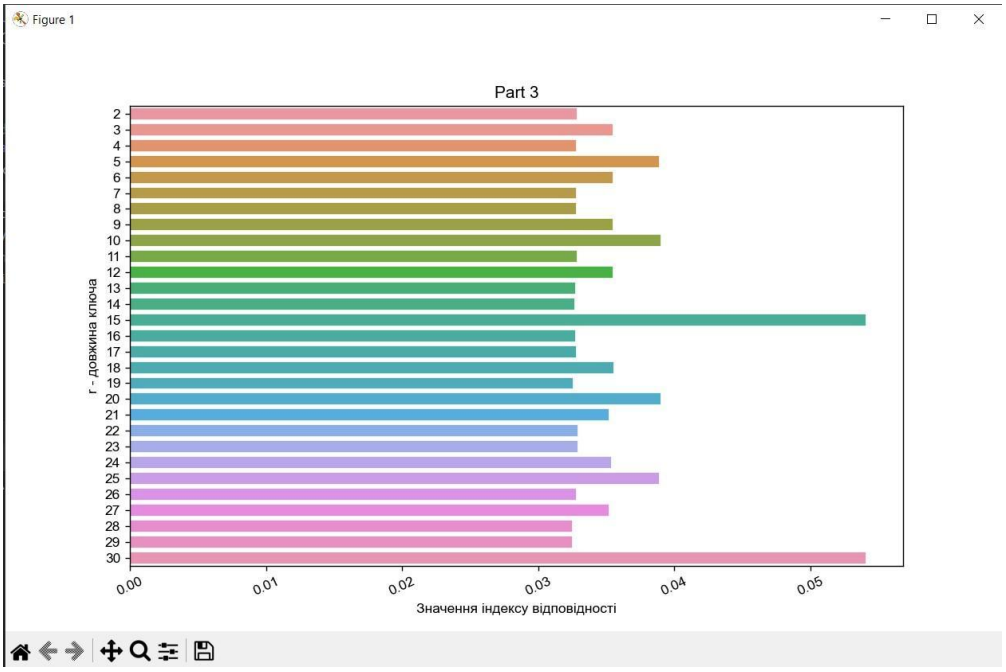
```
Індекс для шифр тексту1: 0.040480824102661656
Індекс для шифр тексту2: 0.04449478617254916
Індекс для шифр тексту3: 0.03684642033510209
Індекс для шифр тексту4: 0.03740422914857003
Індекс для шифр тексту5: 0.034044960809275056
Індекс для шифр тексту6: 0.032670392191031336
Індекс відкритого тексту: 0.05664286889320178
```

У нашому випадку індекс відповідності у відкритому тексті більше, тому що літери у такому випадку наш текст має сенс, на відміну від зашифрованого.



Згідно цього графіку ми бачимо тенденцію, що із збільшенням довжини ключа падає індекс відповідності. Проте, це відбувається не постійно, тому що існує межа після якої ця властивість не виконується.

Для третього пункту, ми скористались методом із теоретичних відомостей, ми виставили потрібні нам границі для ключа та шукали індекси відповідності для кожного блоку:



Графік показує, що у нашому випадку ключ може бути довжиною 15 або 30 літер.
Ми почали перевірку з 15 і ця довжина ключа виявилась підходящою.

Далі, методом частотного аналізу ми визначили ключ, з яким і отримали відкритий текст.

Висновки:

В результаті виконання лабораторної роботи, ми засвоїли метод частоного криптоаналізу, здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера, розібрались з індексами відповідності та математичними очікуваннями.