КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконав
ФБ-12 Сущенко Олександр

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).

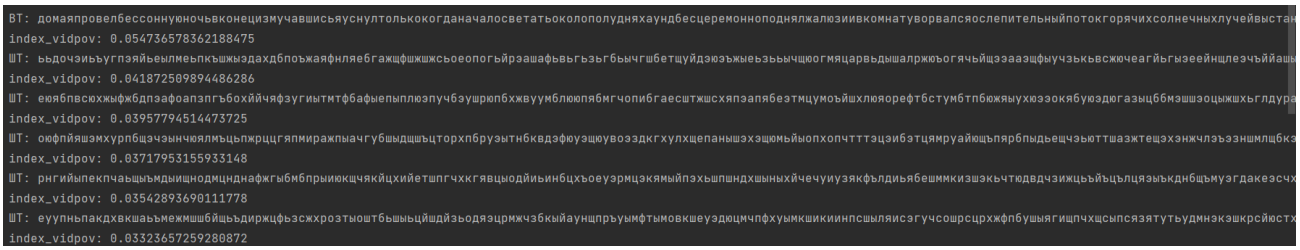
Варіант: 14

Хід роботи

Перш за все підберемо текст та ключі шифрування:

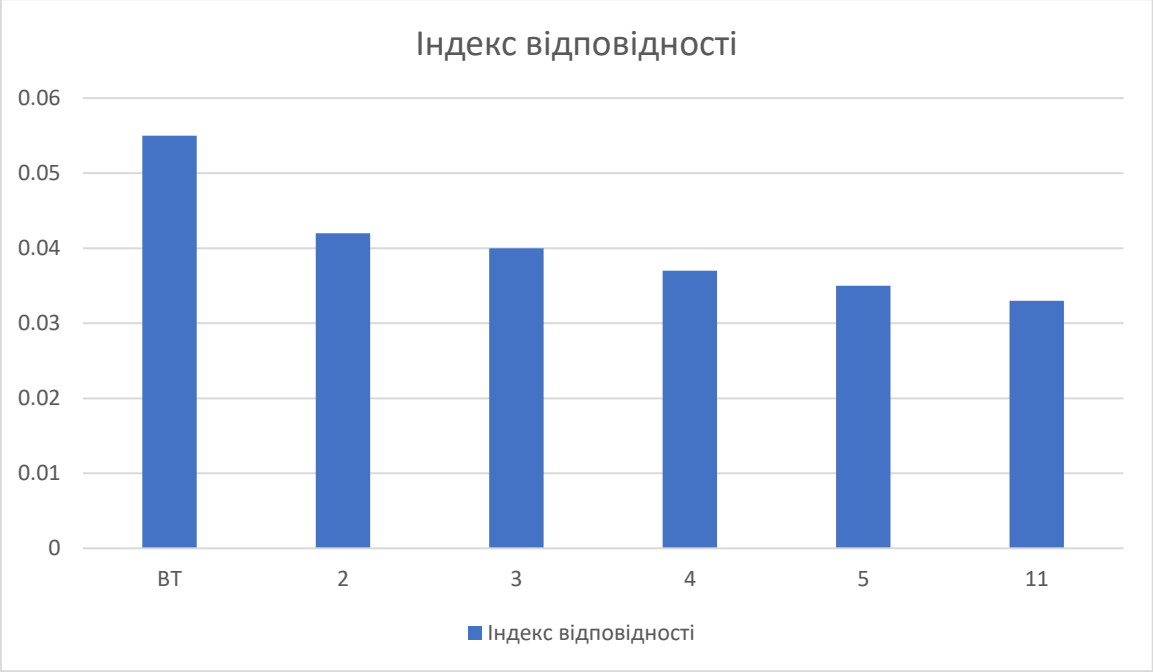
```
keys = ["шо", "бру", "крип", "мячик", "безпонятияк"]
```

Результати шифрування:



Значення індексів відповідності для вказаних значень r:

r	Індекс відповідності
ВТ	0.055
2	0.042
3	0.04
4	0.037
5	0.035
11	0.033



Індекси відповідності для тексту що треба розшифрувати:

Найбільше значення при 19, відповідно отримуємо можливі ключі:

```
key: ьоньисттцовыгермесч
key: ечцесъыыячлдмощхоъа
key: кьыкцяаадьрйсуюъуяе
key: вфувочшшьфибйлцтлчэ
key: эпоэйтуучпгьджснжтш
key: шкйшдноотккючябмибну
key: щлкщеоппуляшавнйвоф
key: ясрялфххщсеюжиупифъ
key: ъмлъжпррфмащбгокгпх
key: иъщифэююввъозпсьшсэг
```

Використаємо перший ключ:

```
ВТ: шроыштатаярляетсяноаолккоцуытюомстратосичускоськьмандовацця
```

Найбільша складність виникла саме при відновленні ключа, що потребувало деякий час.

Ключ – конкистадорыгермеса

```
ВТ: кронштадтявляетсянетолькоцентромстратегическогокомандования
```

Висновок

Під час виконання цієї лабораторної роботи, я набув навичок частотного криптоаналізу та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера. Також цікавою виявилася можливість застосування наведеної теорії для знаходження ключа та розшифрування за його допомогою шифрованого тексту. Незважаючи на деякі складнощі, в цілому процес виявився простим та повчальним.