МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ
КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2
Криптоаналіз шифру Віженера

Виконав:
ФБ-14 Фролов Павло

Перевірила:
Селюх П. В.

Київ 2023

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

Порядок виконання роботи
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
1. Взяв уривок з “Приключения Гулливера” як текст для шифрування.
Ключі: “он", "два", "пять", "полет", "самолетнебовысоко”

2. Підраховані індекси

```
Індекс відповідності для відкритого тексту: 0.057347093316871794
0.047348481705627284 - Індекс відповідності для тексту зашифровакого ключем "он"
0.042852535966736195 - Індекс відповідності для тексту зашифровакого ключем "два"
0.03779957529685798 - Індекс відповідності для тексту зашифровакого ключем "пять"
0.03745441410824232 - Індекс відповідності для тексту зашифровакого ключем "полет"
0.03529826296525543 - Індекс відповідності для тексту зашифровакого ключем "самолетнебовысоко"
```

Як можна побачити значення індексу відповідності дорівнює близько 0.057 і зменьшується при збільшенні ключа бо короткий ключ дає більш регулярний розподіл.

3. Результат роботи коду:

```
Вірогідна довжина ключа: 17
Вірогідний ключ: венецианскийкужец
```

Також можна побачити що є невелика помилка в відгаданому ключі, правильний ключ це “веницианскийкупец”. Розшифрований текст це п’єса Вільяма Шекспіра “Венеційській купець”. Зберіг цей текст в окремому файлі.

Висновки:
Виконавши комп’ютерний практикум я зрозумів роботу шифру Віженера. Я отримав практичні навички використання його для шифрування і проведення криптоаналізу цього шифру.