

**Національний технічний університет України «КПІ» імені  
Ігоря Сікорського  
Фізико-технічний інститут**

**Комп'ютерний практикум 2  
Криптографія**

Виконали:  
студенти ФБ-21  
Князян Кирило Андрійович  
Новіцький Олександр Костянтинович

# Криптоаналіз шифру Віженера

## Мета роботи

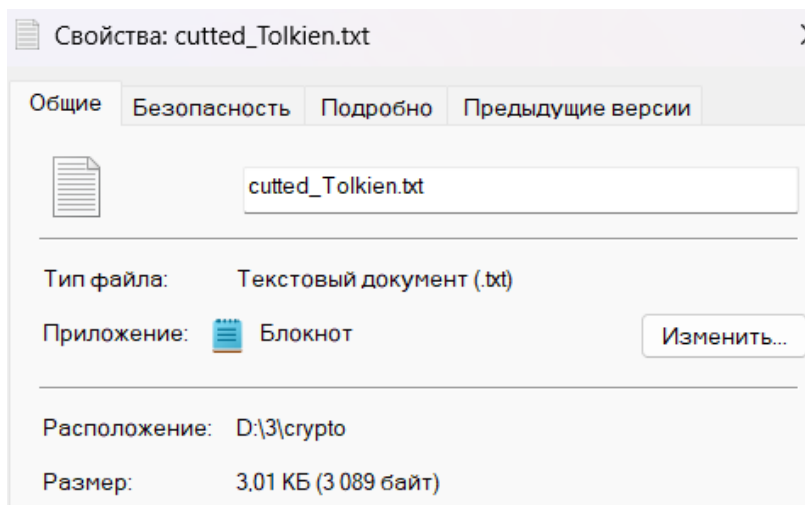
Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових шифрів гамування адитивного типу на прикладі шифру Віженера.

## 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. Ми підібрали фрагмент тексту з першої лабораторної роботи:



та ось такі ключі:

```
KEYS = ["да", "нет", "танк", "омлет", "олександрвеликий"]
```

2. Після шифрування текстів з допомогою різних ключів, маємо такий результат:

[illegible][illegible]

Також вивели індекси відповідності для відкритого тексту та шифрованих, обраховані за формулою:

$$I(Y) = \frac{1}{n(n-1)} \sum N_i(Y)(N_i(Y)-1)$$

```

Індекс відповідності ВТ: 0.054951194808953
Індекс відповідності ШТ з ключем да: 0.046290916780749494
Індекс відповідності ШТ з ключем нет: 0.03880597014925373
Індекс відповідності ШТ з ключем танк: 0.03847874720357942
Індекс відповідності ШТ з ключем омлет: 0.036699055060269124
Індекс відповідності ШТ з ключем олександрвеликий: 0.035490333567064006

```

Можна побачити, що зі збільшенням розміру ключа, індекс відповідності зменшується.

Для розшифровки наданого тексту потрібно спочатку знайти можливі довжини ключів, після чого вже можна буде підібрати сам ключ. Щоб знайти його довжину, ми рухались за першим алгоритмом пошуку значення  $r$  за індексом відповідності. Для  $r = 2, 3, \dots, 30$  розбили ШТ на блоки. Обчислили індекс відповідності для кожного з них і підраховували середній, потім виокремили 3 найімовірніші довжини ключа - ті, у яких різниця за модулем із

індексом відповідності російської мови найменша. Після того, як ми знаємо можливі довжини ключа, потрібно знайти сам ключ. Для цього знадобляться частоти символів з першої лабораторної, які ми для цієї цілі захардкодили на початку скрипта. Тепер, ми беремо, та дістаємо фрагменти тексту, які є зашифровані кожним символом ключа. Тобто кожен перший символ тексту по модулю, кожен другий символ тексту по модулю, і так, поки не виберемо по набору символів тексту для кожного символу ключа. Після цього, ми беремо ці фрагменти тексту, та для кожного з них перебираємо всі можливі зсуви по алфавіту, та шукаємо частоту символів. Тут і знадобиться частота символів з першої лаби, адже ми порівнюємо ці частоти з тими, що отримали ми. І там, де вони найкраще співпадають - правильний символ ключа. Ось результати підбору:

```
Найвірогідніші ключі:  
Довжина ключа: 12, ключ: вшекспирбуря, відхилення індексу відповідності від стандартного: 0.0006304432641336469  
Довжина ключа: 24, ключ: вшекспирбурявшекспирбуря, відхилення індексу відповідності від стандартного: 0.0006458335008186836  
Довжина ключа: 18, ключ: ирбкрявреусяврекп, відхилення індексу відповідності від стандартного: 0.012380760218599754
```

```
Ключ: вшекспирбуря, Початок розшифрованого тексту:  
действиущицаалонзокорольнеаполитанскийсебастьянегобратпрсперозаконныйгерцогмиланскийантониоегобратнезаконнозахватившийвластьвмиланскомгерцогствевфе  
Ключ: вшекспирбурявшекспирбуря, Початок розшифрованого тексту:  
действиущицаалонзокорольнеаполитанскийсебастьянегобратпрсперозаконныйгерцогмиланскийантониоегобратнезаконнозахватившийвластьвмиланскомгерцогствевфе  
Ключ: ирбкрявреусяврекп, Початок розшифрованого тексту:  
кннсутщюхидливаамоноуороуьдержозстрэцикблбсьссяхегпбратшросчезоаккццлгльрчюймдлнстийбнтонсоегцбзавуегйккзхтзбеаоибшисвлбствхилахсбоьйемоульхехх
```

Можна зробити висновок, що ключ - “вшекспирбуря” - тобто В. Шекспір і його п'єса Буря, можна побачити з фрагменту розшифрованого тексту початок цієї п'єси.

## Висновки:

У ході виконання лабораторної роботи ми навчилися працювати з шифром Віженера. Ми розробили код для шифрування тексту різними ключами. Також навчилися аналізувати зашифрований шифром Віженера текст, знаходити можливу довжину ключа, та, на основі цієї інформації, розшифровувати сам текст після отримання самого ключа. Тобто, здобули навички частотного криптоаналізу.