НТУУ "КПІ ім Ігоря Сікорського"

Фізико-технічний інститут

КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шрифту Віженера

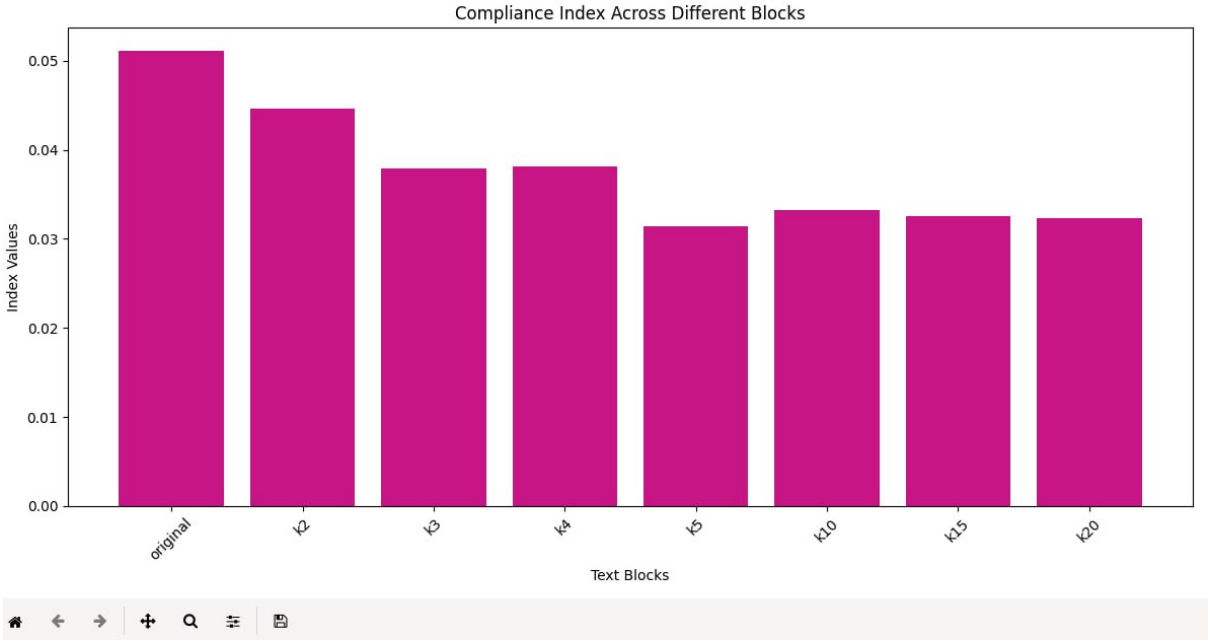
Виконав:

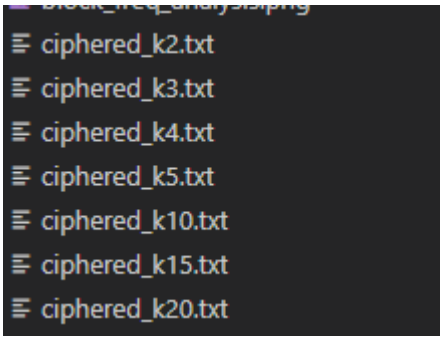
студент групи ФБ-14 Хаща Іван

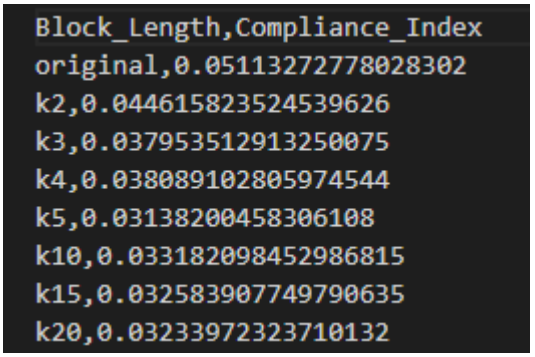
Київ 2023

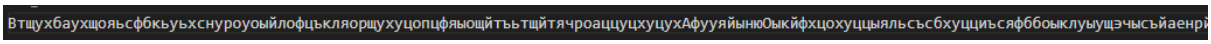
Порядок виконання роботи:

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







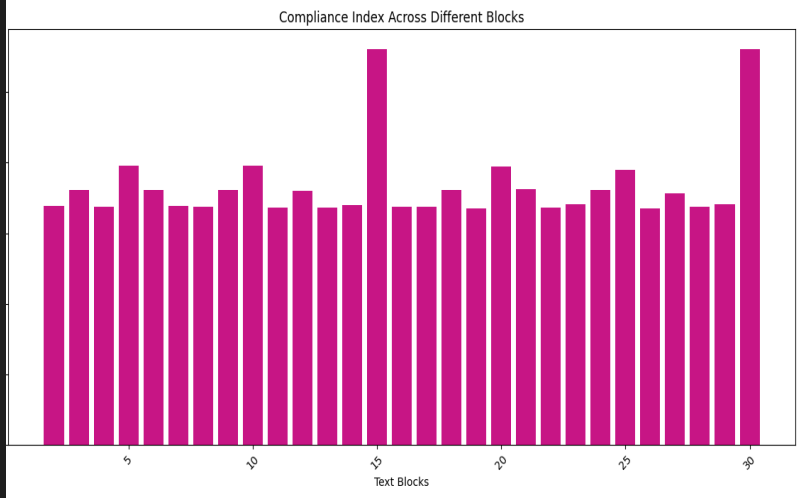


3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Спочатку знайдемо значення індексів відповідності для різних періодів. Той індекс, який буде найбільш близьким до теоретичного значення індексу відповідності російської мови і буде шуканим ключем (Індекс відповідності рос. мови - 0.0553)

Отже ключ довжини 15 символів

```
Block_Length,Compliance_Index
2,0.03385388813744475
3,0.03615187096897406
4,0.03374293361807624
5,0.03952084806368013
6,0.036125055880893396
7,0.033821792020889335
8,0.03374094496535136
9,0.03608280586815857
10,0.03952252784858045
11,0.033676545852495285
12,0.03604485666071514
13,0.03357519915761071
14,0.03392455396612265
15,0.05605177331202787
16,0.033683288319021676
17,0.03368867351961501
18,0.03608986458957075
19,0.0335364228338296
20,0.03938936497846169
21,0.03619388229715766
22,0.033594664277906146
23,0.03408654267171319
24,0.03608759248034322
25,0.03901716563504428
26,0.03346893581656819
27,0.03564037880738555
28,0.033727646862663656
29,0.03404426010285956
30,0.056003131569729775
```



Починаємо розшифровку

`арудазевархимаг` - найадекватніший ключ

`прошлопятнадцатьднейистарыйдомпостепенноначаложиватьсор`

Висновки з лабораторної роботи:

Зашифрування Тексту: Успішно зашифрував текст, використовуючи ключі різної довжини.

. **Процес Дешифрування:** Ми виконали наступні кроки для дешифрування шифру Віженера:

- Розділили текст на періоди.

- Обчислили індекси відповідності для кожного періоду.

- Визначили періоди з індексами відповідності, що наближаються до теоретичного значення для даної мови.

- Аналізували отримані індекси відповідності.

- Застосували частотний аналіз для розшифровки ключа.

- Перевірили ключ на тексті, коригуючи помилки за допомогою формули Віженера або умовної ентропії.

- Підтвердили правильність ключа математично та логічно, що засвідчило успішне дешифрування тексту.

. **Формула Шифрування:** Для шифрування тексту шифром Віженера використовували формулу y = (x + k) mod m, де x - символ відкритого тексту, k - ключ, m - розмір алфавіту.