Криптографія

Лабораторна робота 2. Криптоаналіз шифру Віженера

ФБ-13 Ігнатенко Данило

Варіант 5

Мета роботи

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

Задача

0. Прочитати методичку. Тричі
1. Вибрати шматок тексту з першої лаби, щоб не шукати новий (з поправками на наявність літери "ъ")
2. Написати програму, що зашифровує та розшифровує текст шифром Віженера і зашифрувати текст обраними ключами довжини 2, 3, 4, 5 та 10-20 символів
3. Порівняти індекси відповідності для відкритого та зашифрованих текстів
4. З новими знаннями і силами розшифрувати наданий за варіантом шифротекст

Хід роботи

Для відкритого тексту довжини 2-3 кб був взятий відповідний шматок з трохи зміненого тексту, що використовувався у першій лабі, зокрема я просто підрізав два рядки у функції переформатування, що видаляли твердий знак, і пройшовся нею по тексту, після чого прибрав пробіли

Ключі обрані наступні: ио, осе, буер, зепар, рыбонуклеиновый. Імен довжини 2 в Гоетії не було, а довжини 10-20 починалися на "А", що для ключа так собі

Спершу були написані функції, що видають номер літери і літеру за номером, працює на основі рядка з алфавітом і безмежних приколів пітона. Далі функції шифрування/розшифрування, які потім об’єдналися в одну з додатковим параметром. Останніми були функції для підрахунку індексу відповідності

Труднощі

Написати нормально протокол. Лаба, як на мене, легша та цікавіша за попередню, тому сидіти і писати зараз протокол – найскладніша і найнудніша частина

Шляхи розв’язання

Завжди є

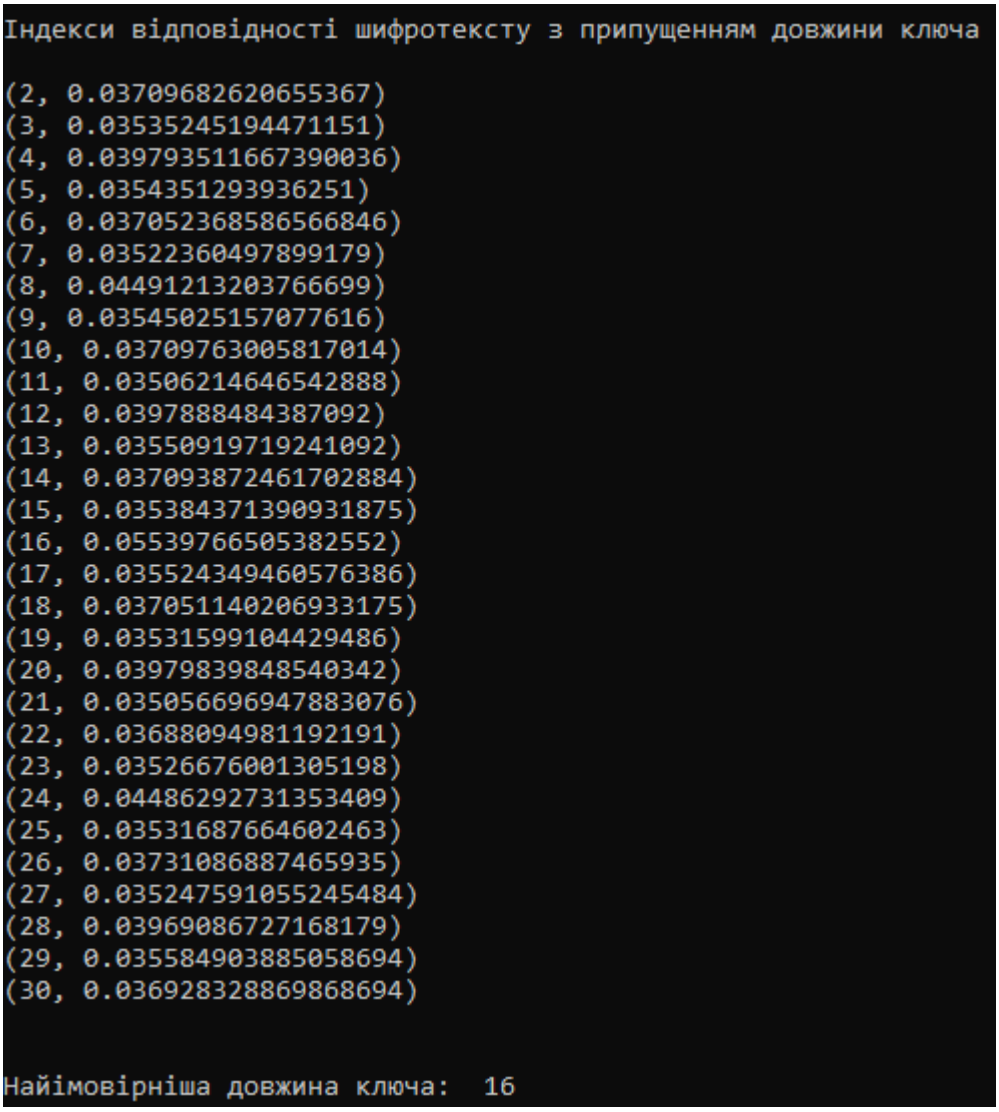
Результати

Повний відкритий текст збережений у файлі fulltext.txt (щоб порахувати частоти літер), його частинка на 3 кб – у файлі sample.txt, результати шифрування – у файлах key2.txt, key3.txt, key4.txt, key5.txt та keylong.txt відповідно, шифротекст за варіантом – у файлі ciphertext5.txt, проміжні та остаточний результати розшифрування збережені у файлах ct1.txt, ct2.txt та ct3.txt відповідно. Пробіли між частинами розставлялися руками для легкості читання

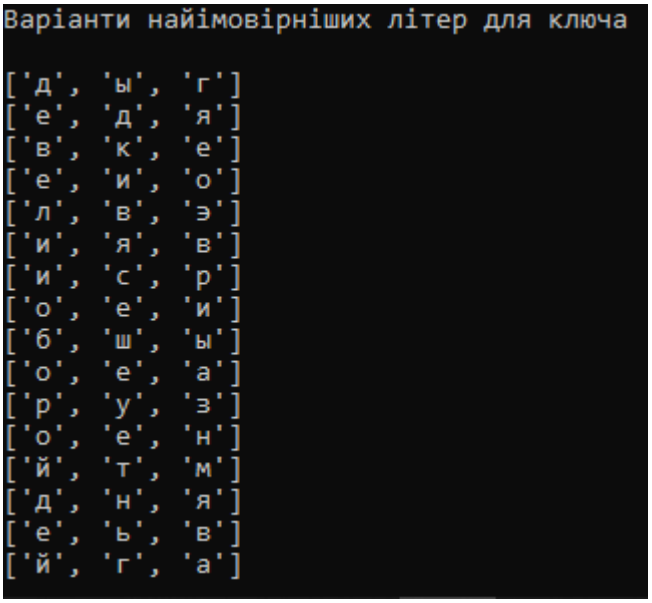
Отримали теоретичне значення індексу відповідності 0.056, а практично порахували 0.058, що доволі близько. При порівнянні індексів видно стрімкий спад, проте його швидкість спадання зменшується теж дуже швидко

```
(base) C:\Users\uranus\Desktop\Crypt\ihnatenko_fb-13_cp2>python lab2.py
Теоретичне значення індексу відповідності повного тексту:  0.05586932290323541
Практичне значення індексу відповідності зразка:  0.05776291402132586
Індекс відповідності шифротексту з ключем "ио": 0.044934767142034975
Індекс відповідності шифротексту з ключем "осе": 0.03972338911773636
Індекс відповідності шифротексту з ключем "буер": 0.03924666131933965
Індекс відповідності шифротексту з ключем "зепар": 0.03589869081120763
Індекс відповідності шифротексту з ключем "рыбонуклеиновый": 0.033746165105519074
```

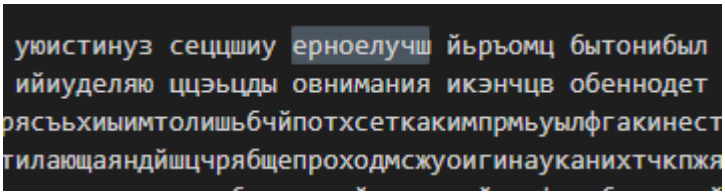
Було розраховано індекси відповідності шифротексту з припущенням довжин ключів від 2 до 30. Стрімкий спад значення при неправильній довжині швидко дає зрозуміти, що був використаний ключ довжини 16



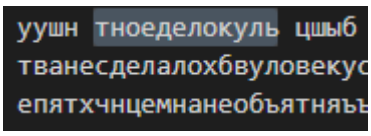
Літери для ключа підбиралися доволі просто: рахували топ-3 літери у блоці по частоті і припускали, що це "о". Від порядкового значення літери блоку віднімалося порядкове значення літери "о" і отримувалося припущення для літери ключа



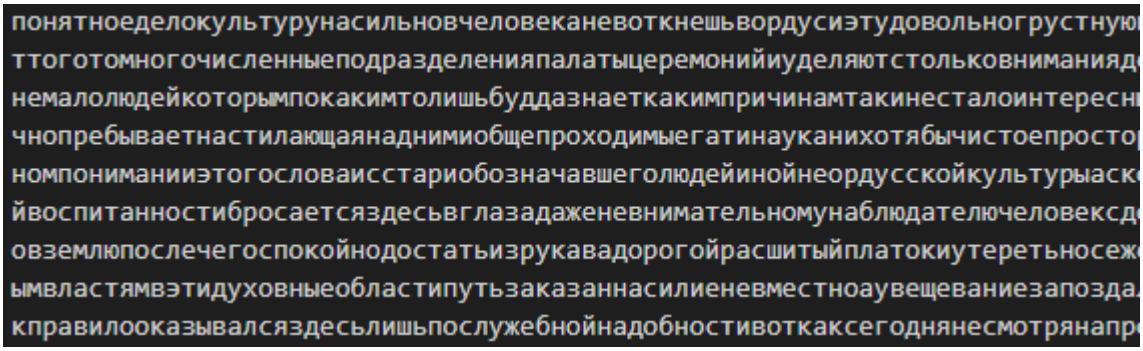
Саме розшифрування вже проводиться руками з використанням функцій скрипта. Із даних літер (більше спираючись на перший стовпець) чітко видно слово "оборотней" в кінці ключа. Спробуємо розшифрувати текст ключем "ааааааоборотней" і проаналізувати



При огляді помічено фрагмент, в якому пізнається слово "наверное". Робимо припущення, що частинка "нав" стала частинкою "шиу". Від порядкових значень останніх віднімаємо порядкові значення перших і пробуємо розшифрувати з новим ключем "аааалисоборотней"



Текст став більш змістовним, припущення виявилося правильним. Крім того, одразу пізнається шматочок фрази "понятное дело", тому припускаємо, що частинка "уушн" була в оригіналі "поня" і пробуємо розшифрувати текст отриманим ключем "делолисоборотней"



Отримали зрозумілий російський текст, а отже, ключ знайдено. До речі, дякую, це вдруге, коли у нас замість sampletext чи аналогів в завданнях використовується щось змістовне, типу назв музики або, як цього разу, назв і тексту книг, і від цього робити їх стає якось приємніше

Висновки

Протягом роботи ми розібралися з поняттям індексу відповідності, а також дізналися, як його можна застосувати на практиці, зокрема розшифрувати текст, зашифрований шифром Віженера. Також звернули увагу на кілька ознак самого шифру, наприклад на факт частого повторення літер на відстанях, рівних довжині ключа