НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ  
імені Ігоря Сікорського»

Фізико-Технічний Інститут

Звіт

із лабораторної роботи №2

із дисципліни «Криптографія»

на тему

Криптоаналіз шифру Віженера

Виконав:  
студент групи ФБ-13

Берчук В.В.

Київ – 2023

**Мета роботи**

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

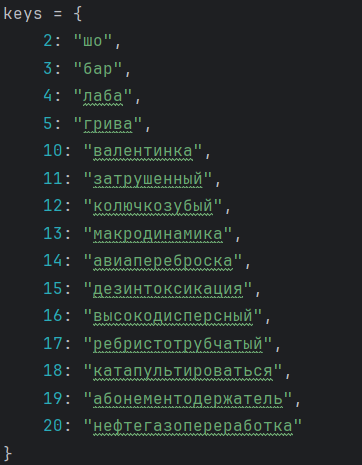
**Порядок виконання роботи**

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.

**Варіант 9**

**Хід роботи**

Підбираю ключі та пишу код (encryptor.py) який буде шифрувати текст (text.txt). Я вибрав такі ключі:



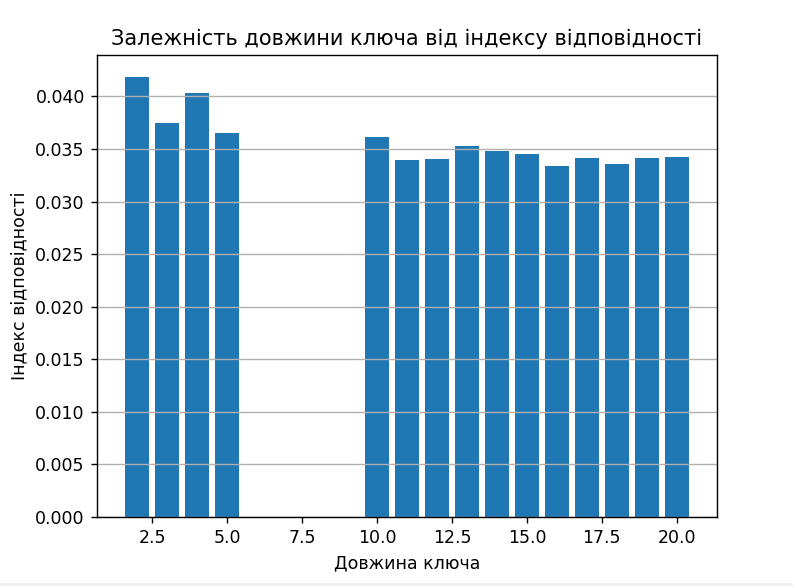
У результаті маю:



Для зручності запишу результати у таблицю:

|  |  |
| --- | --- |
| **Кількість символів ключа** | **Індекс відповідності** |
| 2 | 0.041849 |
| 3 | 0.037506 |
| 4 | 0.040354 |
| 5 | 0.036563 |
| 10 | 0.036161 |
| 11 | 0.033987 |
| 12 | 0.034017 |
| 13 | 0.035304 |
| 14 | 0.034769 |
| 15 | 0.034495 |
| 16 | 0.033389 |
| 17 | 0.034111 |
| 18 | 0.033603 |
| 19 | 0.034114 |
| 20 | 0.034258 |

Індекс для відкритого тексту: 0.057198

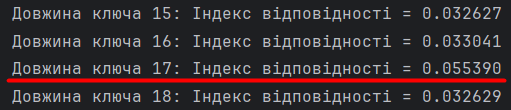
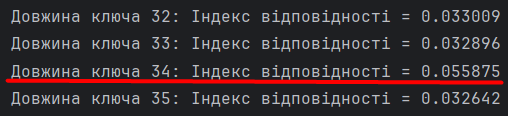


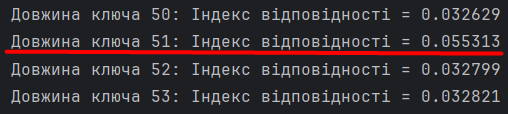
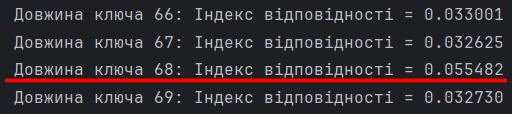
Перейдемо до завдання 3. Потрібно розшифрувати даний текст (9var.txt).

Після виконання коду (index.py) маємо таблицю із значеннями індексів відповідності для цього тексту:

|  |  |
| --- | --- |
| **Кількість символів ключа** | **Індекс відповідності** |
| 2 | 0.032889 |
| 3 | 0.032803 |
| 4 | 0.032777 |
| 5 | 0.032811 |
| 6 | 0.032805 |
| 7 | 0.032728 |
| 8 | 0.032834 |
| 9 | 0.032699 |
| 10 | 0.032853 |
| 11 | 0.032767 |
| 12 | 0.032617 |
| 13 | 0.032877 |
| 14 | 0.032780 |
| 15 | 0.032627 |
| 16 | 0.033041 |
| **17** | **0.055390** |
| 18 | 0.032629 |
| 19 | 0.032884 |
| 20 | 0.032559 |
| 21 | 0.032814 |
| 22 | 0.032870 |
| 23 | 0.032783 |
| 24 | 0.032638 |
| 25 | 0.032717 |
| 26 | 0.033028 |
| 27 | 0.032470 |
| 28 | 0.032565 |
| 29 | 0.032944 |
| 30 | 0.032497 |

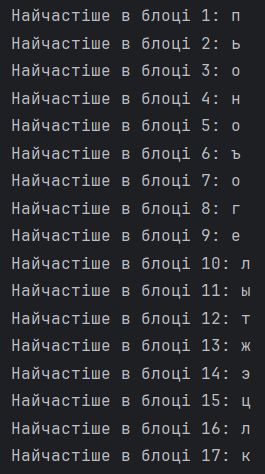
Бачимо що при r =17 значення індексу помітно відрізняється. Збільшимо кількість символів до 70:

Бачимо такий же результат для r кратних 17, тому можемо припустити, що довжина ключа = 17 символів.

Тепер розіб’ємо текст на блоки (block\_count.py) та порахуємо яка літера найчастіше зустрічається в кожному блоці.

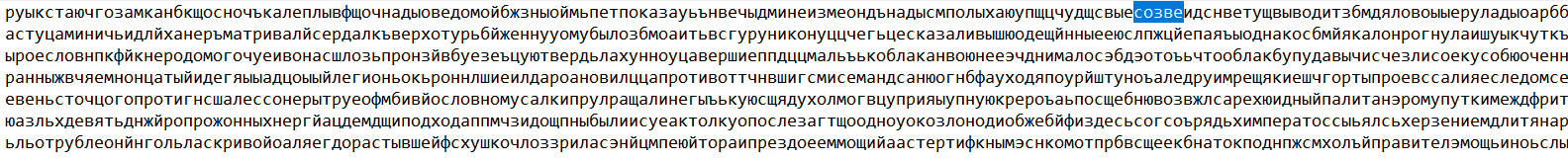


Маємо: **пьоноъогелытжэцлк**

Припустимо, що це зашифровані літери “о” шифром Цезаря у кожному блоці. Розшифровуєм по формулі , де *x* – літера відкритого тексту, *y* – літера шифрованого тексту, *k* – ключ, у мому випадку – 14, *m* – кількість літер в алфавіті (32).

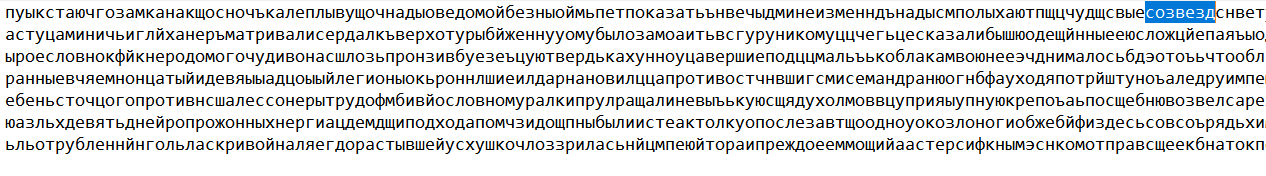
Після розшифровки маю ключ: **боаяамахчэндшпиэь**.

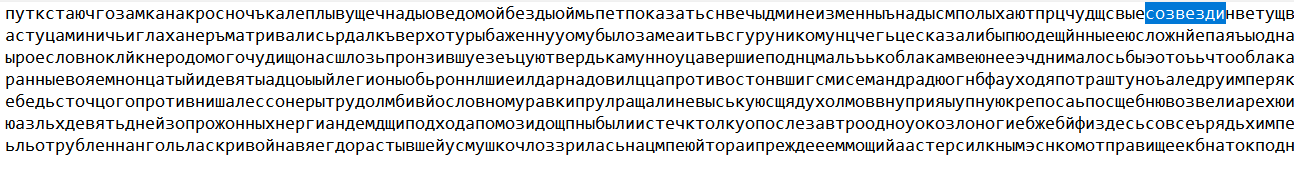
З цього моменту починаються складності. Зразу у ключі видно слово *эндшпиль*, якщо замінити *э* на *л.* Припустимо, що так і є. Спробуємо дешифрувати (decryptor.py) таким поки перехідним ключем:



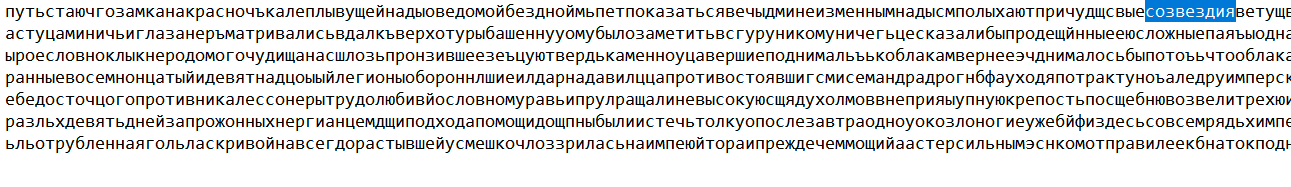
У тексті вже видно деякі слова, які можна розрізнити. Візьмемо наприклад частину *созве.* Ймовірно, що це слово *созвездие.* Спробуємо далі підібрати правильний ключ.   
Розшифруємо **пьоноъогелытжэцлк** відносно інших літер, які трапляються в тексті найчастіше (їх я визначав у 1 лабораторній роботі).  
Відносно е: кчйийхйюажцнбшсже  
Відносно а: оынмнщнвдкъсеьхкй  
Відносно и: зфжежтжыэгукюхогв  
Відносно н: впбабнбцшюоещрйюэ

Перебравши в нашому ключі на першій позиції літери, позитивний результат маю при літері *в*, тобто ключ: **воаяамахчэндшпиль**.

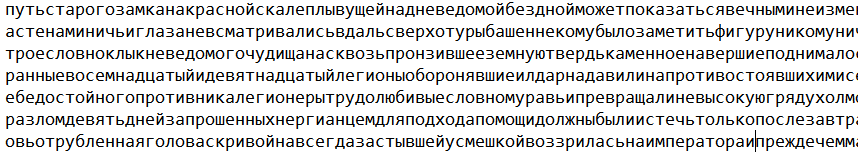


Вже ближче, наступна літера о виглядає найкращим варіантом після *в*, залишимо її. На 3 місце є кандидати *й, н, ж, б*. Спробуємо *й*: **войяамахчэндшпиль**  


Підходить, залишаємо. Можна припустити, що перше слово в ключі це *война,* спробуєм його:



Маємо прогрес і ключ **война махч эндшпиль**. На цьому етапі я вирішив загуглити чи є щось в інтернеті, що містить ці слова і знаходжу книгу “Война мага. Эндшпиль”. Спробуєм дешифрувати:



Текст розшифровано (decrypted\_9var.txt), отже ключ **войнамагаэндшпиль**.

**Висновок**

У ході виконання лабораторної роботи я засвоїв методи частотного криптоаналізу. Я досліджував шифр Віженера, на прикладі якого я набув практичні навички аналізу та розшифрування криптографічних шифрів.