Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

Криптографія

Лабораторна робота №2

Варіант 1

Криптоаналіз шифру Віженера

Виконали:

студенти 3 курсу ФТІ

групи ФБ-05

Качур Ілля Ковальов Данііл

Перевірила:

Селюх П.В.

Київ – 2022

**Мета роботи**:

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

**Порядок виконання роботи**

0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

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 1)

**Хід роботи:**

1. Першим ділом створили функцію шифрування методом Віженера. Особих складнощів не було, нам у створені функцій давали деякі підказки, тож із цією частиною закінчили швидко. Расшифровка працює майже так саме, із маленькими змінами, але там вже віднімали від індексів літер індекс ключа.
2. Другий етап пройшов також швидко за допомогою формули з методички

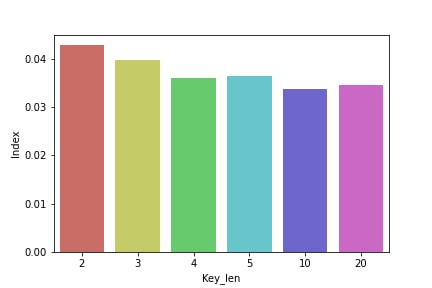
Изображение выглядит как текст

Автоматически созданное описание

З цієї формули зробив функцію



Після отримавши значення зробив діаграму для різного ключа



З цього можна бути впевненим що величина індексу залежить від довжини ключа (чим менший ключ, тим більший индекс), у звичайного тексту індекс був такий:

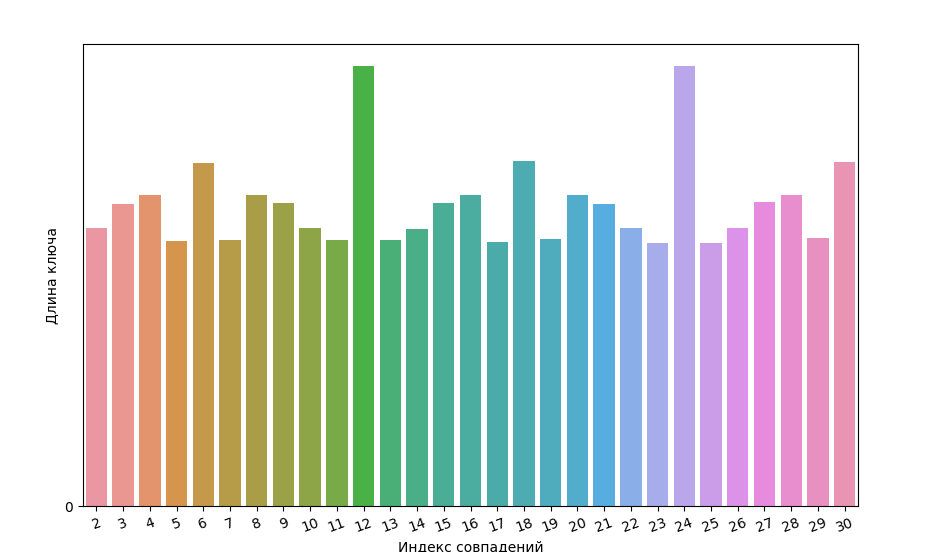


Що є приближеним до значення відповідності у рос.мови (десь 0.05, здається, я гуглив, але не пам’ятаю)

Изображение выглядит как стол

Автоматически созданное описание

1. Потім ми ділили текст на блоки (я назвав функцію Minecrafttext), розглядали проміжок с 2 до 30 та шукали індекси для кожного елементу, зробили графік



Він вийшов трохи дивний, пайчарм не дозволив поставити на х індекси відповідності (не знаю чому, бо на у запрацювало), та й довжина ключа не виводиться збоку (мабуть , бо вони не округлені чи щось таке), проте якщо навести на сам графік куди потрібно то довжину буде видно.

Далі виводив через функцію dovzhuna\_of\_key мої ключі, додав 2, бо починав рахувати з 2 елементу, отримав бажаний номерок (12).

1. Далі на довго застрягли по деяким причинам, проте завдяки підказці, додумали що від нас треба досить швидко (там була ще одна затримка, пізніше розкажу). Знайшли популярні у використанні букви алфавіту, використавши частотний аналіз знайшли можливі літери ключа, використали також найпопулярніші букви рос. алфавіту, використовували аналіз по блоку, звідси і дивне іменування Steve (я вирішив ще додати майнкрафту), після цього У ТЕОРІЇ ми мали знайти наші ключи та закінчити з кодом, але тіп-топ не вийшло, розповідаю чому, просиділи ми десь півтори години (4 якщо рахувати вбите в мене світло), нам виводило дивні ключи, які складувались в ну дуже стрьомні слова, які ну ніяк не можуть бути ключем, проте ми думали так і треба, шукали якісь слова у виводі розшифрованого тексту (використали функцію з першого пункту), чого ми тільки не знаходили, хліб, чорні коти і інші дивні речи, вирішили ще раз пройтися по файлу, (драматична пауза) помітили що забули видалити пробіли (ще одна драматична пауза), видалили їх та знайшли ключ одразу (треба було змінити одну літеру, але вона була друга у масиву ), отримали розшифрований текст та радісні закрили код.

Наш ключ: вшекспирбуря

Розшифрований текст вивели нижче:





Ну і там далі текст увесь не буду кріпити у документ.

**Висновок**

У ході роботи ми покращили наші навички праці з шифруванням, навчилися працювати з шифровкою за допомогою коду, стали більш уважними (сумне емодзі), також стали впевненими у деяких твердженях з методи, наприклад про індекс відповідності та його падіння дивлячись на довжину ключа. Трошки покращили навички праці з графіками у пітоні.