НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №2**

Криптоаналіз шифру Віженера

Виконали:

студенти групи ФБ-22

Мартинюк Артем

Шеїна Еліна

**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 шифротекстів і порівняти їх значення.

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

Хід роботи

Для першого завдання ми скористаємося текстом із попередньої роботи. Маємо список із ключів:



У коді ми проходимося по всім ключам із цього списку. Функція шифрування відкритого тексту за допомогою шифру Віженера:

A computer screen with text on it

Description automatically generated

Для кожної букви ключа послідовно визначається величина зсуву. Потім, використовуючи цей зсув, розраховується номер зашифрованої букви у відкритому тексті, а результат береться за модулем 32, щоб залишитися в межах алфавіту. Особливість у тому, що довжина ключа може не збігатися з довжиною відкритого тексту, і це враховується завдяки використанню індексу букви ключа за модулем.  
Функція дешифрування:

A computer screen with text on it

Description automatically generated

Виконуються ті ж дії, але зсув виконується в інший бік.

Індекс відповідності - метод криптоаналізу шифру Віженера. Обраховується за формулою:

A black and white math symbol

Description automatically generated

Якщо текст не зашифрований, то індекс відповідності набуватиме значень випадковим чином. Частота появи різних букв у тексті буде відповідати їхній загальній імовірності в появі у відкритому тексті. У такому випадку індекс відповідності дорівнюватиме:

A black and white math symbols

Description automatically generated

де t p – імовірність появи літери t в мові.

Обрахунок індексу відповідності реалізований наступним чином:

A black screen with colorful text

Description automatically generated

Виконується проходження по всіх буквах відкритого тексту з розрахунком їхніх індексів відповідності. Частота появи кожної букви ділиться на загальну кількість букв у тексті. Потім індекси відповідності всіх букв підсумовуються, утворюючи загальний індекс відповідності для всього тексту.  
Після застосування цієї функції до відкритого тексту отримано результат:

A screenshot of a computer

Description automatically generated

У наступному завданні нам надано шифротекст, і потрібно експериментально визначити ймовірну довжину ключа, використовуючи аналіз на основі індексів відповідності. З попереднього завдання відомо, що індекс відповідності для відкритого тексту російською мовою приблизно дорівнює 0.05628.

Оскільки ми розглядаємо шифр Віженера, де ключ повторюється до тих пір, поки його довжина не дорівнює довжині відкритого тексту, через певний період, рівний довжині ключа, можна помітити, що зсув букв відбувається на один і той самий індекс. Тому доцільно розбити шифротекст на блоки, що відповідають цьому періоду. Наприклад, якщо період дорівнює 2, слово "калейдоскоп" буде розбито на блоки "клйдскп" і "аеооо".

Обчисливши індекс відповідності для кожного блоку, можна визначити довжину ключа. Це стає можливим, оскільки для блоків, які містять букви, до яких застосовано однаковий зсув, індекс відповідності наближатиметься до нормального значення, тобто приблизно до 0.05628.

Такий принцип знаходження ключа було продемонстровано у трьох функціях нижче:

A computer screen shot of text

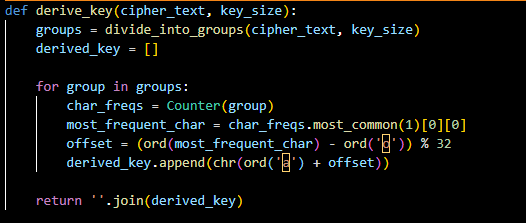
Description automatically generated

Таким чином, ми проаналізували ключі довжини від 2 до 30:

A screen shot of a computer

Description automatically generated

Тепер спробуємо знайти сам ключ:



Розбиваємо зашифрований текст на блоки відповідно до періоду, у цьому випадку для довжин 12 та 24. В кожному блоці визначаємо букву, яка з'являється найчастіше. Припускаємо, що ця буква відповідає найпоширенішій букві відкритого тексту, тобто "о". Потім обчислюємо зсув між найчастіше зустрічаючою буквою блоку шифротексту та буквою "о" у відкритому тексті, переводимо його в індекс і визначаємо відповідну букву ключа для кожного блоку. Таким чином, проходимо по всіх блоках. Спробуємо застосувати цей підхід для ключів довжиною 12 та 24:





Як бачимо, ключ довжиною 24 є просто подвоєним ключем довжиною 12, тому надалі ми будемо використовувати лише ключ 12. Ураховуючи, що ключ має бути змістовним, а також результат, який ми отримали при спробах знайти ключі довжиною 12 та 24, шебспир занадто сильно схоже на шекспир.  
Тому ключ буде "вшекспирбуря".

Спробуємо розшифрувати текст, використовуючи цей ключ:

Найденный ключ для длины 12: вшебспирбуря

Расшифрованный текст с ключом длиной 12:

действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконныйгерцогмиланскийантониоегобратнезаконнозахватившийвластьвмиланскомгерцогствефердинандсынкоролянеаполитанскогогонзалостарыйчестныйсоветниккоролянеаполитанскогоадрианфрансископридворныекалибанрабуродливыйдикарьтринкулошутстефанодворецкийпьяницакапитанкораблябоцманматросымирандадочьпроспероариэльдухвоздухаиридацерераюнонанимфыжнецыдухидругиедухипокорныепроспероместодействиякорабльвмореостровкорабльвморебурягромимолниявходяткапитанкорабляибоцманкапитанбоцманбоцманслушаюкапитанкапитанзовикомандунаверхживейзаделонетомыналетимнарифыскорейскорейкапитануходитпоявляютсяматросыбоцманэймолодцывеселейребятавеселейживоубратьмарсельслушайкапитанскийсвистокнутеперьветертебепросторнодуйпоканелопнешьвходяталонзосебастьянантониофердинандгонзалоидругиеалонзодобрыйбоцманмыполагаемсянатебяагдекапитанмужайтесьдрузьябоцмананукаотправляйтесьвнизантониобоцмангдекапитанбоцманавамегонеслышночтоливынаммешаетеотправляйтесьвкаютывидитештормразыгралсяатутещевыгонзалополегчелюбезныйусмирисьбоцманкогдаусмиритсямореубирайтесьэтимревущимваламнетделадокоролеймаршпокаютаммолчатьнемешайтегонзаловсетакипомнилюбезныйктоутебянабортубоцманаяпомнючтонетникогочьяшкура…

Текст вдалося розшифрувати.

**Висновки:**

У процесі цієї роботи ми ознайомилися з методами частотного криптоаналізу. Експериментально визначили індекс відповідності для відкритого тексту російською мовою, порівняли його з індексами відповідності зашифрованих текстів та виявили залежність цього індексу від довжини ключа.

Використовуючи отримані знання, ми змогли визначити довжину ключа для конкретного зашифрованого тексту, а також відновити сам ключ, що дозволило успішно дешифрувати текст.