НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ  
імені Ігоря Сікорського»

Фізико-Технічний Інститут

Звіт

із лабораторної роботи №3

із дисципліни «Криптографія»

на тему

Криптоаналіз афінної біграмної підстановки

Виконав:  
студент групи ФБ-13

Берчук В.В.

Київ – 2023

**Мета роботи**

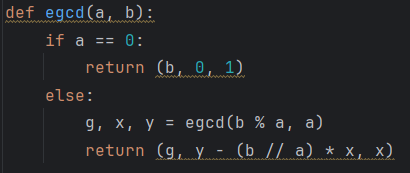
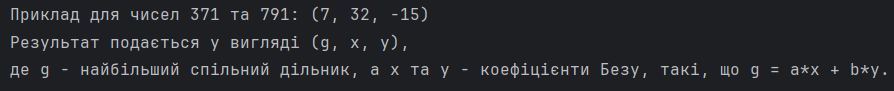
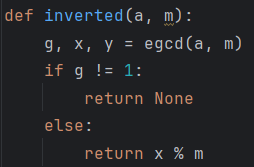
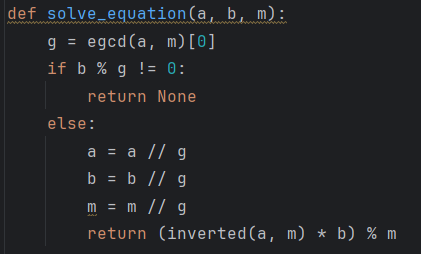
Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

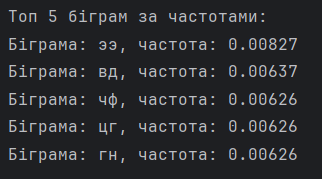
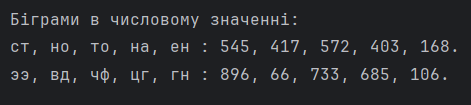
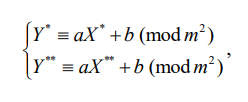
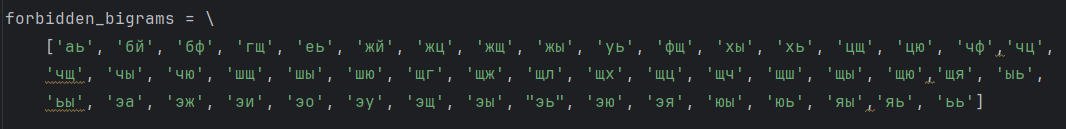
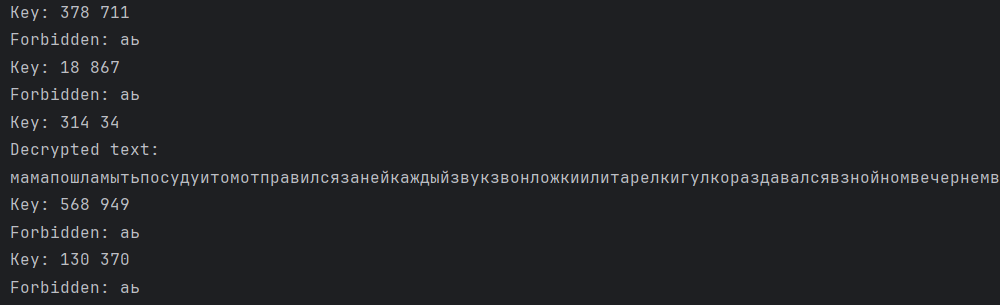
**Порядок виконання роботи**

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв’язуванням лінійних порівнянь. При розв’язуванні порівнянь потрібно коректно обробляти випадок із декількома розв’язками, повертаючи їх усі.
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп’ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п’яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв’язання системи (1).
4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

**Варіант 9  
Хід роботи**

1. Реалізував підпрограми з математичними операціями (весь код у файлі code\_cp3.py):

* Обчислення НСД розширеним алгоритмом Евкліда  
    
  
* Обчислення оберненого за модулем числа  
    
  
* Розв’язування лінійних порівнянь   
    
  

1. За допомогою коду з практикуму №1 знайшов 5 найчастіших біграм у шифртексті:  
   
2. Кожній біграмі, яку отримав та 5 найчастішим біграмам рос. мови співставив числа  
   по формулі:  
     
     
   Знайшов кандидатів на ключ (a, b) розв’язуючи систему рівнянь:  
   
3. Для кожного можливого ключа спробував дешифрувати текст (09.txt), при цьому якщо текст після дешифрування має біграми, які неможливо зустріти у рос. мові (критерій заборонених l-грам), а саме:  
      
   або якщо текст не має зовсім символів, то я відкинув такий текст. Цікаво, що з усього списку таких біграм, більшість беззмістовних дешифрованих текстів не пройшли перевірку вже на першій біграмі, лише декілька дійшли до другої, і жоден до третьої.
4. В результаті один з дешифрованих текстів підійшов за критеріями:  
      
   Бачу, що текст має зміст (повний текст у файлі decrypted\_text.txt), можна зробити висновок, що текст був зашифрований ключем (314, 34)

**Висновок**

У ході виконання даного практикуму я застосував частотний аналіз до шифртексту та побачив його ефективність для розкриття афінних шифрів підстановки. Також за результатом практикуму можна підтвердити, що статистичні властивості природної мови (а саме частоти біграм) зберігаються після шифрування і можуть бути використані для визначення ключа.