**Міністерство освіти і науки України  
 Національний технічний університет України  
 "Київський політехнічний інститут імені Ігоря Сікорського"  
 Фізико-технічний інститут**

Симетрична криптографія  
 Комп’ютерний практикум №3  
 Криптоаналіз афінної біграмної підстановки

Виконав:  
 студент групи ФІ-93  
 Папишев Олег

Перевірив:  
 Чорний О.М.

Київ 2022

**Мета роботи**

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

**Хід роботи**

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

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 шифротексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифротексту (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 шифротекст. Якщо шифротекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним. У разі необхідності змінити кодування алфавіту (див. методичні вказівки).

**Методичні вказівки**

Студентам надається текст, що є результатом шифрування за допомогою афінної підстановки біграм відкритого тексту, написаного російською мовою без пробілів, знаків пунктуації та великих літер. Буква «ё» заміщена буквою «е», а «ъ» – буквою «ь» (або навпаки). Таким чином, алфавіт відкритого тексту складається з 31 букви, що занумеровані в алфавітному порядку: а = 0 , б =1, …, я = 30 . Зауваження: у деяких варіантах літера «ь» стоїть у алфавіті після літери «ы» (що відповідає кодуванню ы = 26, ь = 27), а в деяких навпаки, «ь» ототожнюється із літерою «ъ» та стоїть перед літерою «ы» (що відповідає кодуванню ь = 26, ы = 27). Під час роботи вам необхідно встановити, яким саме способом закодовано алфавіт, для коректного дешифрування тексту. П’ятьма найчастішими біграмами російської мови (в порядку спадання частот) є біграми «ст», «но», «то», «на», «ен». Перевірте ці відомості за допомогою програми підрахунку частот біграм з комп’ютерного практикуму №1. Під час дешифрування виникне потреба відрізнити змістовний текст російською мовою від тексту-шуму, що виникає при неправильному дешифруванні. Вважаючи на доволі велику кількість можливих варіантів ключів, для цієї задачі необхідно побудувати автоматичний розпізнавач російської мови. Створення та принцип роботи такого розпізнавача залишається на ваш розсуд; традиційно використовують такі критерії змістовного тексту:

• перевірку частот частих літер («о», «а», «е», частоти можуть розглядатись окремо або в сукупності);

• перевірку частот рідкісних літер («ф», «щ», «ь», частоти також можуть розглядатись окремо або в сукупності);

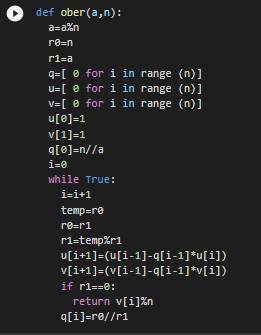
• перевірку частот біграм, підраховану для біграм «на перетині» (у вищенаведених позначеннях – біграм виду ( , ) 2i 2i+1 x x );

• перевірку частот триграм та довільних l-грам.

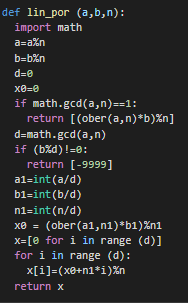
Зашифровані файли із варіантами завдань містяться в папці “variants”. Зашифровані файли, що містяться у папці “for\_test”, є більш простими для аналізу, ніж основні варіанти, їх можна використовувати для тестування або налаштування ваших програм.

ПРАКТИЧНА ЧАСТИНА

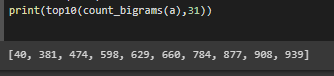
1.Обчислення оберненого:



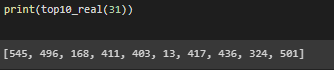
Обчислення порівнянь:



2. Найчастіші біграми у шифротексті: (з використанням функції X=x1\*n+x2)



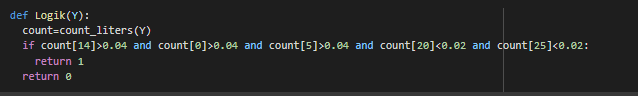
Найчастіші біграми у російській мові



3.Обчислюємо а з кожної пари біграм з топ10 біграм шифротексту, у відповідність яким поставлені пари біграм з топ10 реальних біграм.

Обчислюємо б для кожного а

Розшифровуємо текст та перевіряємо його на актуальність функцією Логик, яка рахує частоту букв о,а,е,ф,щ у тексті та порівнює з очікуванною частотою



Якщо текст схожий на російський то виводимо ключ а,б та текст.

