Лабораторна робота №3

Криптоаналіз афінної біграмної підстановки

Виконала Годлевська Аліса ФБ-11

**Мета роботи**

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

**Порядок виконання**

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)

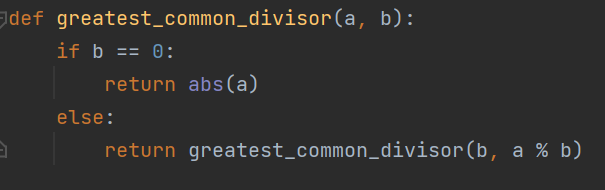
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п’яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв’язання системи

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

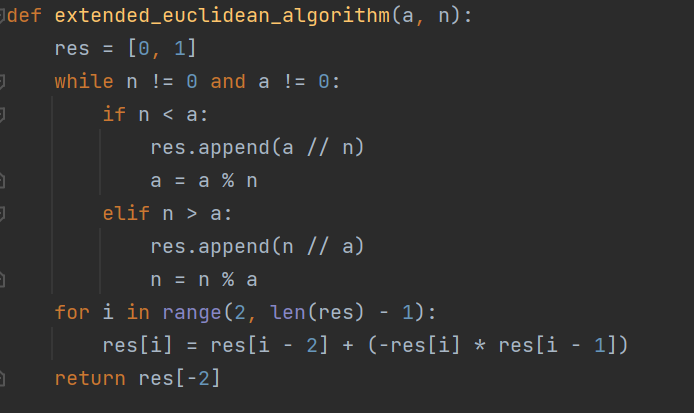
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

**Хід роботи**

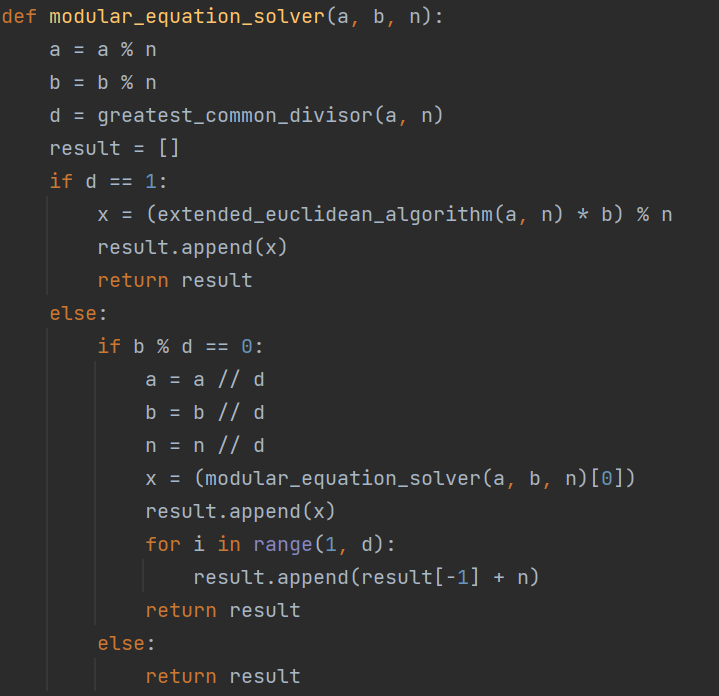
1. Реалізую усі необіхідні функції для математичних операцій:



Знаходимо НСД

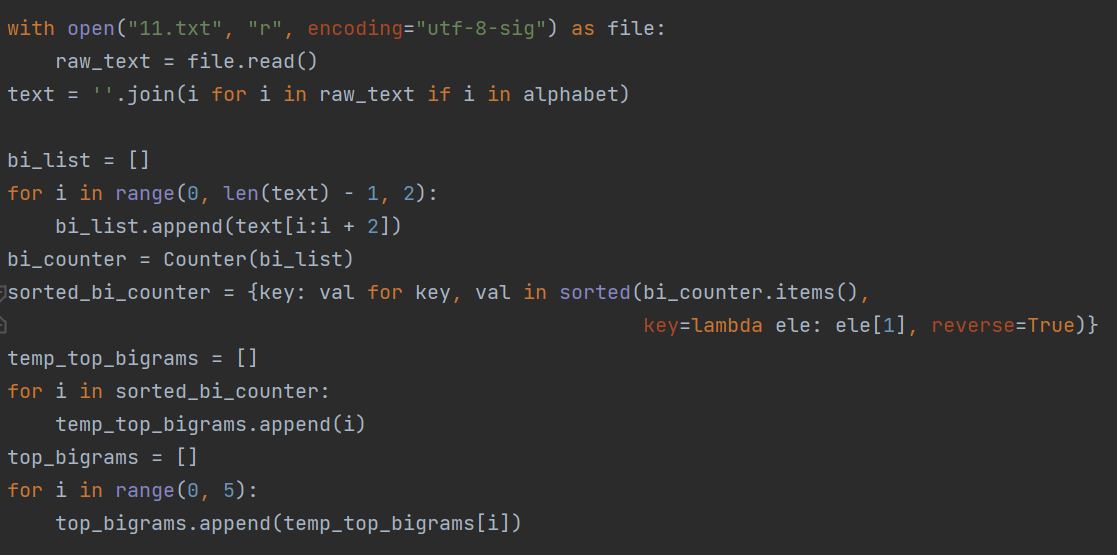


Розширений алгоритм Евкліда



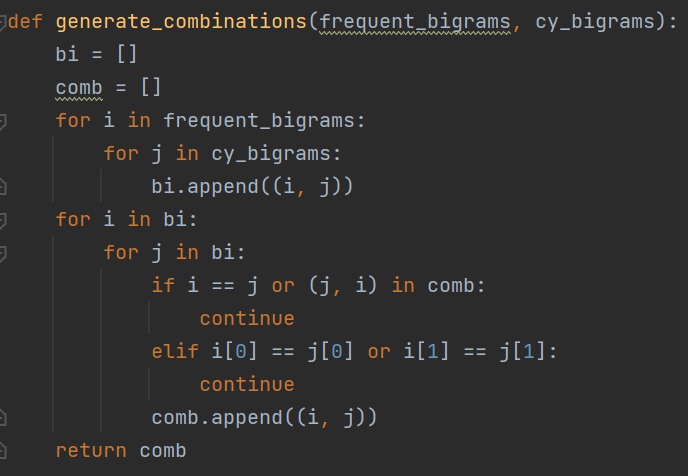
Розв’язання лінійних порівнянь

2.

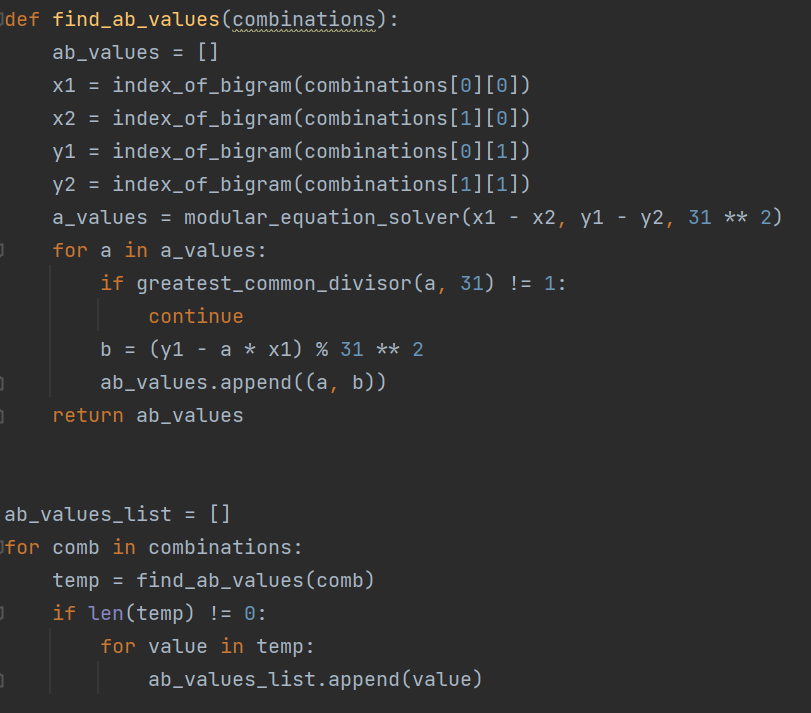


Найчастіші біграми

3.

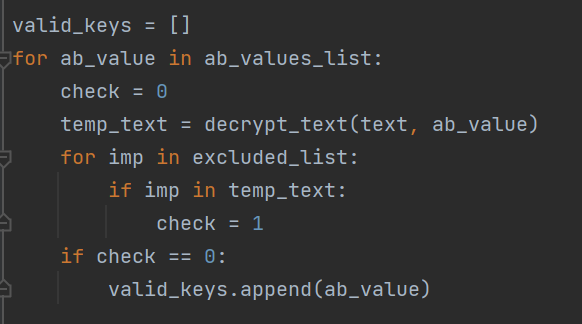


Співставляємо

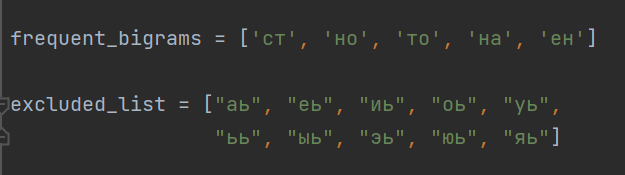


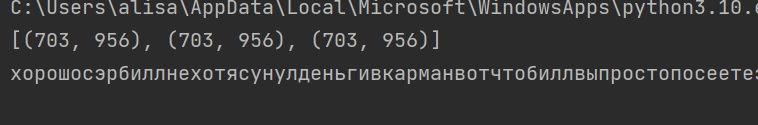
Знаходимо кандидатів на ключ

4.



Використаю відбракування неможливих біграм (excluded\_list):





Текст є фрагментом книги «Кульбабове вино» Рея Бредбері

**Висновки**: мені вдалося проаналізувати шифр афінної підстановки та дешифрувати текст; також я отримала практичні навички із використанням модульної арифметики.