**КРИПТОГРАФІЯ**

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3**

**Криптоаналіз афінної біграмної підстановки**

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

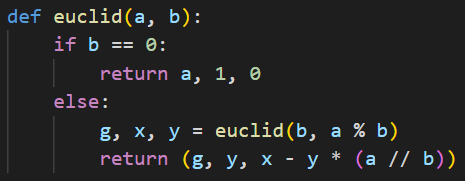
**Порядок виконання роботи:**

1. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.
2. 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.
3. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп’ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
4. 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).
5. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
6. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

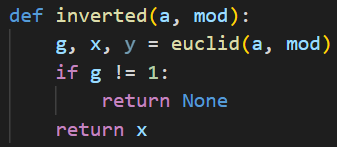
**Хід роботи:**

1. Реалізуємо функції з необхідними математичними операціями:

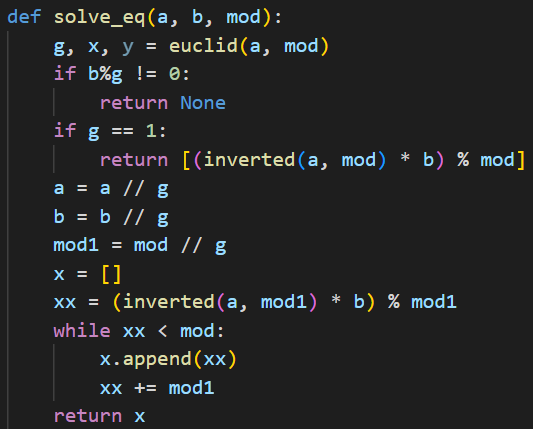
розширений алгоритм Евкліда



обчислення оберненого елементу за модулем



розв’язання лінійних порівнянь



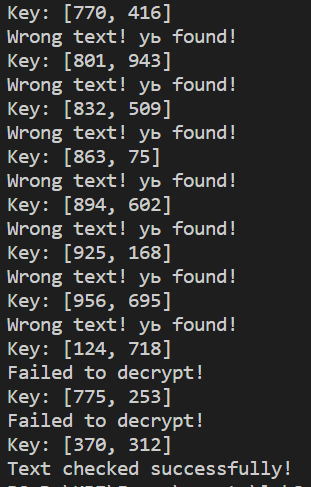
2. знайдемо 5 найчастіших біграм запропонованого шифртексту (варіант 16):



3-5. Переберемо всі комбінації найчастіших біграм відкритого та зашифрованого тексту, порахуємо ключ для кожної з них, спробуємо розшифрувати текст отриманими ключами та перевіримо кожен з отриманих текстів на змістовність.

Будемо відкидати тексти, які ми не змогли розшифрувати та тексти які містять біграму, яка не існує в російскій мові:





Ми отримали ключ – 370, 312

Розшифрований текст у файлі 16\_decrypted.txt

**Висновок:**

В ході цієї лабораторної я навчився використовувати частотний аналіз для розшифрування афінної біграмної підстановки.