Міністерство освіти і науки України Національний технічний університет України “Київський політехнічний інститут ім. Ігоря Сікорського” Фізико-технічний інститут

**КРИПТОГРАФІЯ**

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3**

**Криптоаналіз афінної біграмної підстановки**

**Варіант 7**

Виконали студенти:

ФБ-23 Лишиленко Ангеліна

ФБ-23 Тіщенко Олександр

Київ-2024

**Мета роботи:**

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної

підстановки; опанування прийомами роботи в модулярній арифметиці.

**Порядок виконання 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 шифртексту

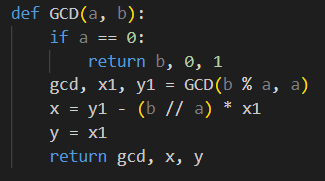
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п’яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв’язання системи

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

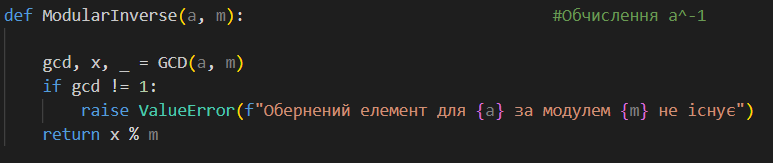
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

**Хід роботи:**

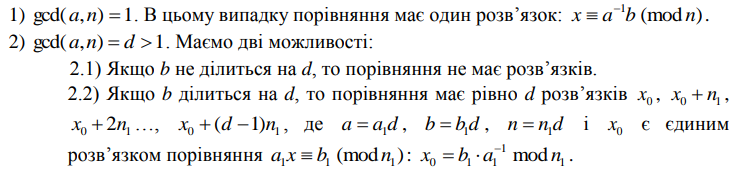
1. Спочатку зробили функцію GCD яка обчислює НСД за допомогою розширеного алгоритму Евкліда.

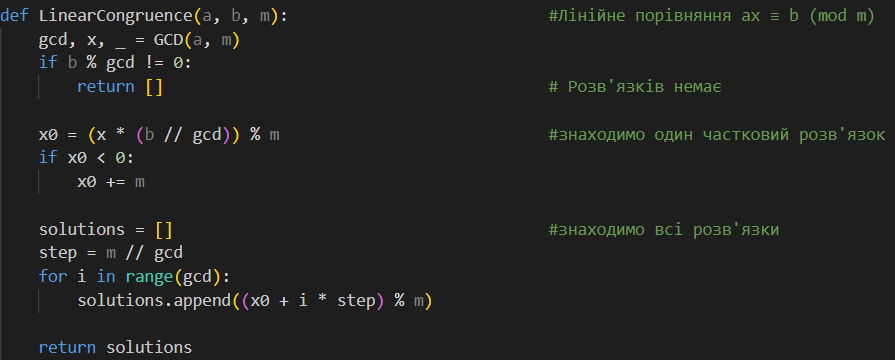


Потім написали функцію ModularInverse що обраховує обернений елемент. Обраховується НСД за допомогою функції GCD: якщо НСД(a,m)≠1, обернений елемент не існує (викидається помилка), в іншому випадку знаходимо обернений елемент за формулою a \* a^-1 = 1(mod m)

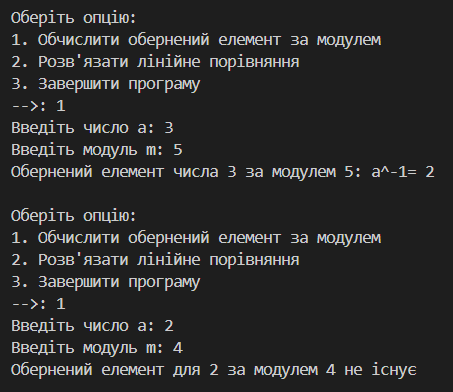


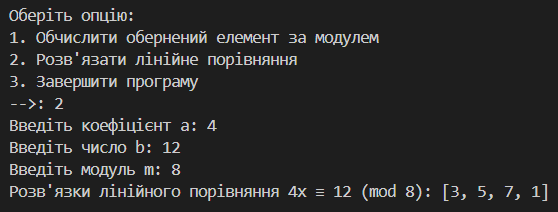
Також написали функцію для обчислення лінійних порівнянь LinearCongruence. В цій функції також обчислюємо НСД за допомогою функції GCD. А потім враховуємо три можливі випадки розв’язання:

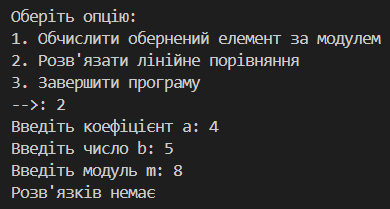




Що ми отримали:

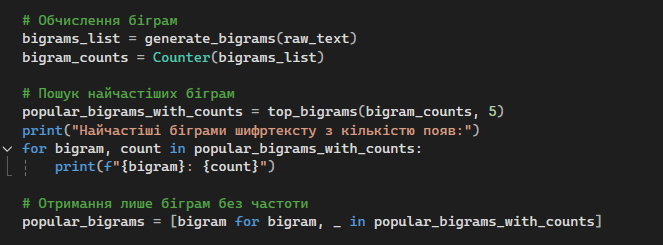






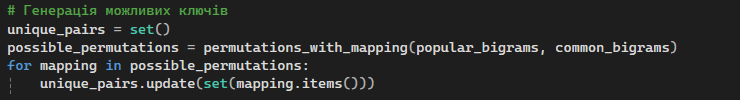
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп’ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту

Ми генеруємо всі біграми в тексті, рахуємо кількість появ кожної біграми, обираємо 5 найпоширеніших біграм та виводимо на екран

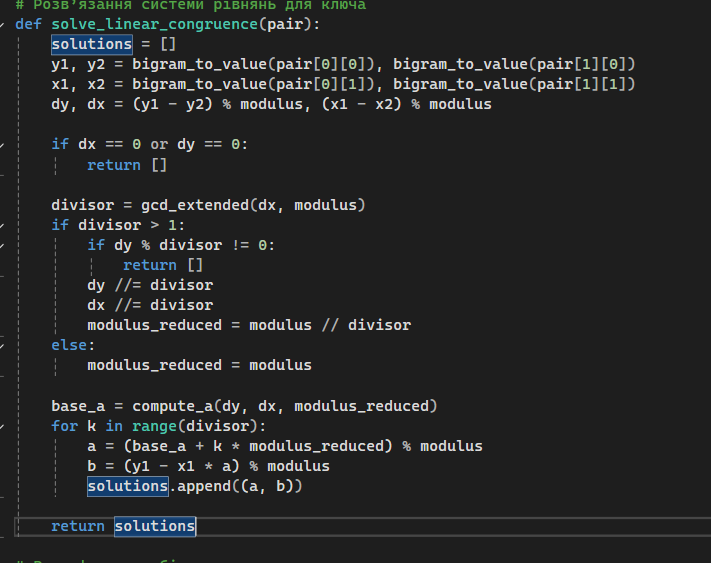


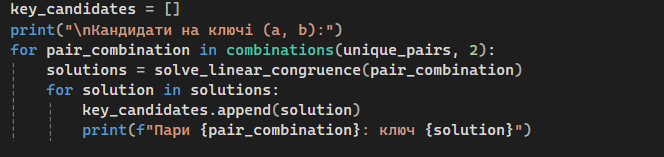
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п’яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв’язання системи

Створюємо всі можливі відповідності між п’ятьма найчастішими біграмами шифртексту та частими біграмами мови(common\_bigrams = ['ст', 'но', 'то', 'на', 'ен'])



Ця частина коду розв’язує систему рівнянь для кожної пари біграм:

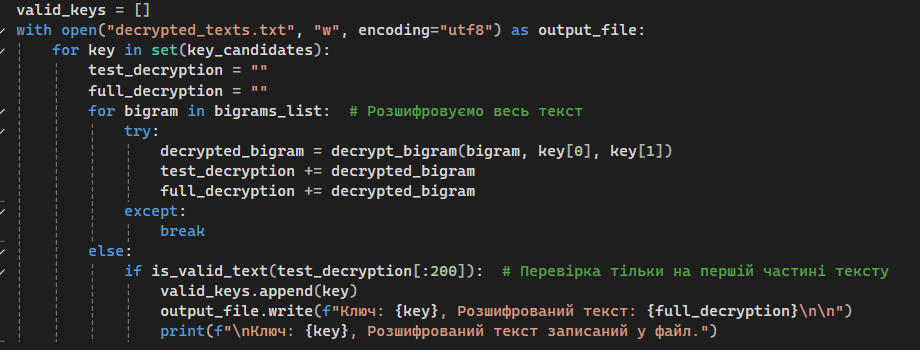
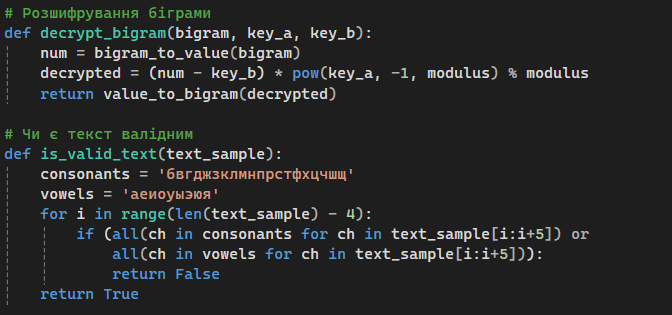




Генерує всі пари з унікальних відповідностей біграм та для кожної пари біграм розв’язує систему рівнянь виду:

Де , — біграми шифртексту, а , — біграми мови. Повертає можливі значення a і b

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



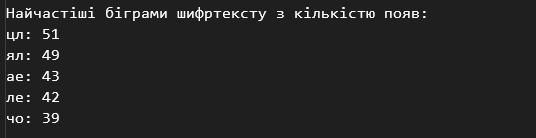
Дешифруємо біграму за формулою:

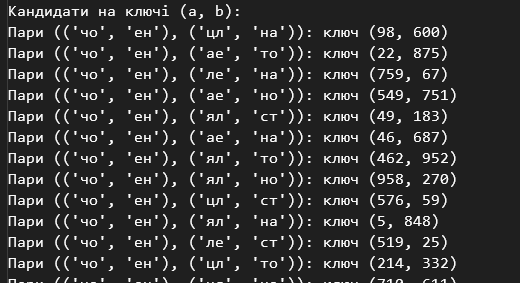
де — обернене до a за модулем.

Та перевіряємо, чи є розшифрований текст змістовним.

Наприклад, текст відкидається, якщо 5 поспіль букв — голосні або приголосні. А результат розшифрованого тексту записується у файл

Й в результаті ми отримаємо:





Ключ: (200, 900), Розшифрований текст: атызнаешьсколькоразмывэтомгодуиграливбейсболавпрошломавпозапрошломнистогониссегоспросилтомгубыегодвигалисьбыстробыстроявсезаписалтысячпятьсотшестьдесятвосемьразасколькоразячистилзубызадесятьлетжизнишестьтысячразарукимылпятнадцатьтысячразспалчетыресл…