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

Лабораторна робота № 3

з предмету «Криптографія»

«Криптоаналіз афінної біграмної підстановки»
Варіант 3

Виконали:
Студенти 3 курсу,
ФТІ, груп ФБ-02, ФБ-05
Кодак Єгор,
Нікітський Іван

Київ - 2022

Мета: 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 (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: 3

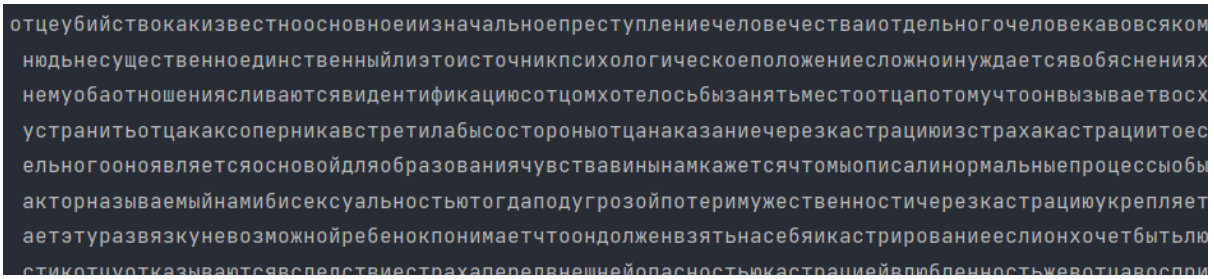
Хід роботи:

1. Реалізовані функції:
    a. gcd - звичайний розрахунок gcd
    b. expanded_gcd - обчислення gcd за розширеним алгоритмом Евкліда
    c. my_mod_equation - Обчислити рівняння моди
    d. top_bgrams - Отримати топ 5 біграм з цільового файлу
    e. bigram_to_num - Конвертувати біграму в число
    f. num_to_bgram - Конвертувати число в біграму
    g. _bgram_frequency - Обчислити частоту bgram. Алгоритм з 1 лабораторної роботи
2. 5 найчастіших біграм запропонованого шифртексту

```
['тд', 'рб', 'во', 'щю', 'ет']
```

3. Реалізовані функції:
    a. create_system - Формуємо систему біграм за формулою
    $\{Y * \equiv aX *+ b(mod\, m^2), Y * \equiv aX **+ b(mod\, m^2)\}$
    b. roots - Отримуємо корені для кожної пари біграм за формулою
    $Y *- Y **= a(X *- X **)(mod\, m\text{^}2)$
4. Реалізовані функції:
    a. get_keys - Перебираємо системи біграм і знайти корінь кожної пари
    b. decrypt - розшифрувуємо текст на основі пари ключів використовуючи наступне рівняння:
    $X_i = a^{-1}(Y_i - b) mod\, m^2$
    c. _validate - Після того, як отримаємо найбільш коректний текст, валідуємо розшифрований текст, використовуючи біграми за перевіркою частоти символів

5. Як результат роботи програми отримали змістовний дешифрований текст:



Висновки

Під час виконання лабораторної роботи ми набули навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки, опанували прийоми роботи в модулярній арифметиці.