КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

(Варіант 2)

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 (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

Роботу виконали: ФБ-13 Летюка, Мірошніков

Хід Роботи

1. Реалізували програму, що обчислює обернений елемент за модулем (за допомогою розширеного алгоритму Евкліда) та розв’язує лінійні порівняння.
2. Далі ми використовуємо код з ЛР1, який обчислює найпоширеніші біграми в заданому шифртексті. Отримали такий результат:
   ['йа', 'юа', 'чш', 'юд', 'рщ']
   Як найчастіші біграми в мові використовуємо: **['ст','но','то','на','ен']**

Для заміни біграми числовим значенням користувалися такою формулою:

$$(x_{2i-1}, x_{2i}) \leftrightarrow X_i = x_{2i-1}m + x_{2i}.$$

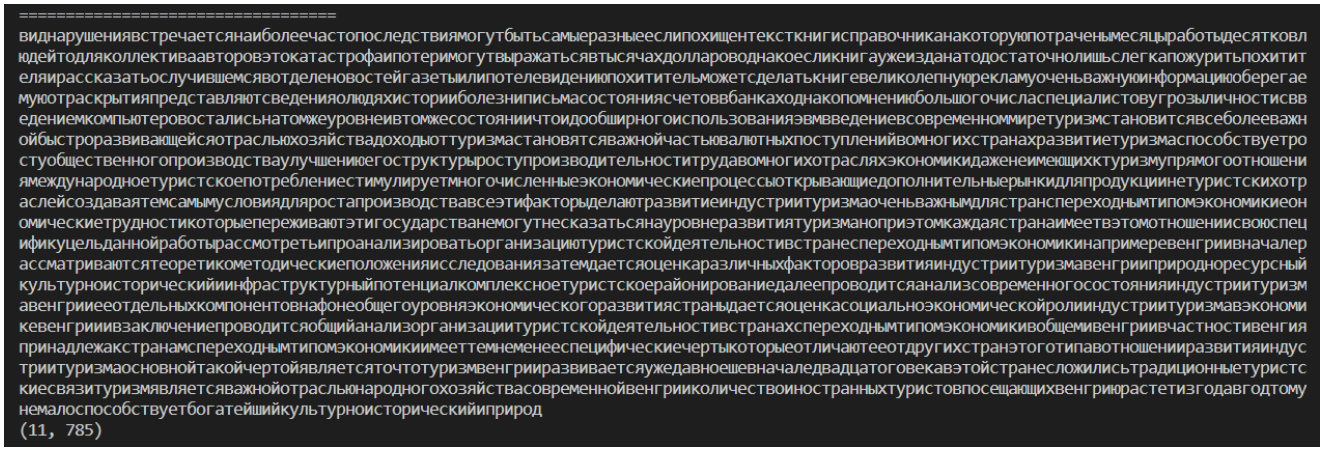
3. Перебравши можливі варіанти співставлення найчастіших біграм в шифртексті нашого варіанту та біграм в мові, реалізована програма виконує пошук можливого ключа для кожного співставлення. Ключ шукаємо за допомогою розв’язання такої системи рівнянь:

$$\begin{cases} Y^{*} \equiv aX^{*} + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases},$$

4. Далі розшифровуємо текст використовуючи надані можливі ключі.
   Для покращення ефективності використовуємо алгоритм перевірки отриманого тексту на читабельність за допомогою “розпізнавача”, в основі якого лежить перевірка наявності неіснуючих в мові біграм (перевіряємо чи отримали біграми типу голосна літера + “ъ”)
5. В результаті отримали такий відкритий текст:

Ключ шифрування = (27, 211)

6. Перевіряємо ще раз нашу програму для наданого тестового тексту:



Труднощі

Під час реалізації програми виникли незначні труднощі з використанням модульної арифметики в програмуванні для підрахунку оберненого елементу за модулем. Бо незначні помилки приводили до неправильних результатів підрахунку.

Висновок

В результаті виконання даної лабораторної роботи ми ближче ознайомилися з шифром афінної підстановки та виконали криптоаналіз афінної біграмної підстановки. Окрім цього, опанували принцип роботи з модулярною арифметикою. Також реалізували програму “розпізнавач” що допомагає відфільтрувати читабельний текст та пропускати “текст - шум”, що виникає після неправильного розшифрування.