Національний технічний університет України «КПІ» імені Ігоря Сікорського
Фізико-технічний інститут

Лабораторна робота 3

Криптографія

Виконали:

студенти ФБ-14

Кот Микита Сергійович

Чавалах Артем Дмитрович

Перевірила:

Селюх П. В.

Мета роботи

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

Порядок виконання роботи

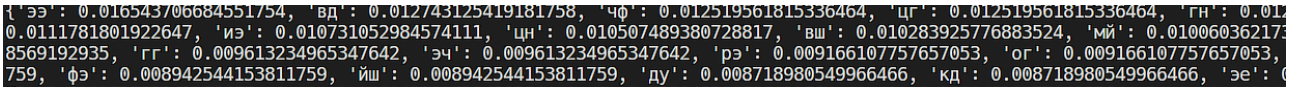
0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

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 (варіант 9).

Знайшли біграми, які частіше усього повторюються в нашому запропонованому варіанті:




```
most_freq_bigr = ['ээ', 'вд', 'чф', 'цг', 'гн']
```

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.

Також обрали неможливі біграми, які не можуть існувати в російській мові (за критерієм заборонених біграм):

```
['дй', 'юь', 'юы', 'эь', 'эы', 'фй']
```+

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

Знайшли наш ключ – (314, 34) та отримали дешифрований текст:

Труднощі

Зіткнулися зі труднощами: у алфавіті були переплутані місцями букви ы та ь. Довго думали над функцією для знаходження a, b у афінному шифрі.

Висновки

У ході виконання лабораторної роботи, ми набули практичних навичків щодо розшифрування афінного шифру за допомогою частотного аналіза. Опанували прийоми в модулярній арифметиці, а точніше лінійні порівняння. Пригадали розширений алгоритм Евкліда. Закріпили свої знання щодо того, які є способи виявлення змістовного тексту.