КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

Виконав

ФБ-12 Сущенко Олександр

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.

Варіант: 14

Хід роботи

Знаходимо 5 найчастіших біграм шифртексту:

```
['аж', 'цп', 'шы', 'ки', 'тя']
```

Знаходимо можливі значення ключів:

```
[(858, 403), (452, 643), (418, 914), (521, 517), (232, 418), (624, 120), (458, 256),
```

Для автоматичного розпізнавача російської мови використаємо метод з забороненими біграмами, оскільки його доволі просто реалізувати, і в той же час він є ефективним для нашого випадку.

```
denied = ["аь", "ьь", "ээ", "ыь", "йь", "йй", "цщ", "уь", "оь", "иь"]
```

Шифрований текст:

```
ыенжийбжфзьеьжхфцрйишсвкрьзпцпьжэххжмжьрпймебжцыысзхяирхлыысчсс
```

Отримуємо розшифрований текст та ключ:

```
вскорепослесвоегоприемавбратствомасоновпьерсполнымнаписаннымимдлясебяруководс
(10, 52)
вскорепослесвоегоприемавбратствомасоновпьерсполнымнаписаннымимдлясебяруководс
(10, 52)
вскорепослесвоегоприемавбратствомасоновпьерсполнымнаписаннымимдлясебяруководс
(10, 52)
```

Висновок

Під час виконання цієї лабораторної роботи, я набув навичок частотного аналізу на прикладі розкриття моноалфавітноїм підстановки та опанував прийоми роботи в модулярній арифметиці. Завдяки тому, що афінний шифр зберігає статистичні властивості мови, пов’язані із частотами біграм, мені вдалося підібрати ключі розшифрування та автоматично визначити змістовний текст.