КРИПТОГРАФІЯ КОМП’ЮТЕРНИЙ ПРАКТИКУМ №3

Криптоаналіз афінної біграмної підстановки

ФБ-14 Гавриленко Давид, ФБ-14 Земляний Олександр

Варіант 6

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

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).

```
{'ще': 46, 'хе': 44, 'чв': 42, 'ле': 40, 'цв': 38, 'ощ': 37, 'сд': 36, 'же': 36, 'де': 36, 'гд': 34, 'ню': 33, 'нв': 33}
```

У нас виникла проблема, коли ми розшифровували текс кандидатами в ключі, що були отримані комбінаціями з двох рівнянь, отриманих з комбінацій відомих найчастіших 5 біграм російської мови зі знайденими 5 біграмами: змістовного тексту не існувало (вручну переглянули усі розшифровані тексти). Після довгих мук з переписуванням фунцій першого пункту, коли ми вибрали 20 найчастіших біграм у нашому зашифрованому тексті, змістовний розшифрований текст з'явився. Поступово зменшуючи цю кількість прийшли до того, що потрібно 12 найчастіших біграм для того щоб утворилася така система рівнянь, результат якої успішно розшифровував шифротекст.

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).

Комбінацій рівнянь вийшло 3600:

```
Потеціальні ключі:
[None, None, None, None, None, None, None, None, None, None, None, None, [0, 780], [31, 222], [954, 751],
3600
```

Коли відкинули системи рівнянь, що не мали розв'язків, залишилось 1069 кандидатів:

```
Потеціальні ключі:
[[0, 780], [31, 222], [954, 751], [589, 749], [241, 131], [956, 622], [535, 388],
1069
Ключ [441,310]: утробылотихоегородокутанныйтьмоймирнонежилсявпостелипришлолетоивет
```

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.

Отримані розшифровані тексти перевіряли на відповідність мові методом заборонених біграм.

Вибрали найочевидніший набір таких біграм: ['аь','эь','ыь','иь','юь','оь','уь','еь','яь','ьь','йь']

```
Ключ [441,310]: утробылотихоегородокутанныйтьмоймирнонежилсявпостелипришлолето
```