НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра Інформаційної Безпеки

Лабораторна робота №3 дисципліни

’’КРИПТОГРАФІЯ’’

Підготували:

студенти групи ФБ-03

Борох Іван

Жигун Анастасія

Київ 2022

Тема роботи: Криптоаналіз афінної біграмної підстановки.

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.

Хід роботи

1. Пропишемо необхідні математичні підпрограми в окремому файлику та імпортуємо до основного виконуваного файлу:

```
import euclidean
```

Обчислюємо обернений елемент за модулем із використанням розширеного алгоритму Евкліда, розв'язуємо лінійні рівняння.

2. Знайдемо 5 найчастіших біграм запропонованого шифртексту за допомогою програми обчислення частот біграм, написаної в ході виконання першого практикуму:

```
[('тд', 77), ('рб', 53), ('во', 52), ('щю', 45), ('кд', 42)]
```

3. Пропаруємо найбільш повторювані біграми в мові, знайдені в результаті виконання першого практикуму, з найбільш повторюваними біграмами запропонованого шифртексту '03.txt' (всього 25):

Найбільш повторювані біграми в результаті 1 практикуму:

```
top_5 = ['ст', 'но', 'то', 'на', 'ен']
```

Пропаровані біграми:

```
[(('ст', 'тд'), ('но', 'рб')), (('ст', 'тд'), ('то', 'рб')), (('ст', 'тд'), ('на', 'рб')),
```

Знайдемо можливі значення ключів для кожної пари (x1,y1) (x2,y2).

```
[(954, 533), (38, 33), (305, 590), (199, 700), (199, 700), (18, 362), (802, 727), (246, 71), (854, 256), (169, 713),
```

4. Для кожного ключа пробуємо розшифрувати текст цим ключем і перевіряємо його на наявність неіснуючих біграм мови:

```
errors = ['еь', 'юы', 'яы', 'аы', 'оы', 'иы' 'аь', 'оь', 'ыь', 'уь', 'эы', 'ыы', 'уы', 'еы', 'юь', 'яь', 'эь',
          'ць']
```

5. Результат:

```
Our key: (199, 700)
Decrypted text: отцеубийствокакизвестноосновноеиизначальноепреступлениечеловечестваиотдельногочеловекав
```

Розшифрований текст збережено в файлі ‘answer.txt’.

Труднощі, що виникали

Виникла проблемка з перебором усіх можливих пар ключів, не вдавалось віднайти правильний ключ через те, що не були перебрані всі існуючі варіанти.

Висновки

В ході виконання даної лабораторної роботи ми набули навички частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанували прийомами роботи в модулярній арифметиці, прописавши системи для пошуку можливих кандидатів на ключ за допомогою розширеного алгоритму Евкліда та лінійних рівнянь, перебрали всі варіанти ключів та, віднайшовши правильний, розшифрували запропонований шифртекст 03 варіанту.