МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3
Криптоаналіз афінної біграмної підстановки

Виконав:
ФБ-14 Фролов Павло

Перевірила:
Селюх П. В.

Київ 2023

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

Порядок виконання:
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),(ba 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:

Використовував частину коду з минулих лабораторних робіт.

1. Отримав найчастіші біграми з шифротексту.

```
/home/netrunner/PycharmProjects/labs/venv/bin/python /home/netrunner/PycharmProjects/l
Топ 5 біграм в тексті: [('нк', 56), ('юж', 52), ('шь', 49), ('х6', 49), ('6й', 47)]
```

2. Знайшов можливі кандидати на ключ.

```
Можливі ключі:: {(224, 714), (182, 589), (154, 582), (919, 629), (549, 437), (59, 192)
```

3. Перевірив текст на змістовність через неможливі біграми і отримав ключ.

```
Ключ: (703, 956)
```

Розшифрував текст в окремий файл. В моєму випадку це текст Рея Бредбері "Кульбабове вино"

Висновки:
Виконавши комп’ютерний практикум я отримав практичні навички криптоаналізу афінного шифру.