НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
Фізико-Технічний Інститут

Звіт
із лабораторної роботи №3
із дисципліни «Криптографія»
на тему
Криптоаналіз афінної біграмної підстановки

Виконав:
студент групи ФБ-13
Берчук В.В.

Київ – 2023

Мета роботи

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

Порядок виконання роботи

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 9
Хід роботи

1. Реалізував підпрограми з математичними операціями (весь код у файлі code_cp3.py):
   - Обчислення НСД розширеним алгоритмом Евкліда

```
def egcd(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, x, y = egcd(b % a, a)
        return (g, y - (b // a) * x, x)
```

```
Приклад для чисел 371 та 791: (7, 32, -15)
Результат подається у вигляді (g, x, y),
де g - найбільший спільний дільник, a x та y - коефіцієнти Безу, такі, що g = a*x + b*y.
```

   - Обчислення оберненого за модулем числа

```
def inverted(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
        return None
    else:
        return x % m
```

```
Приклад для числа 51 за модулем 71: 39
```

– Розв’язування лінійних порівнянь

```
def solve_equation(a, b, m):
    g = egcd(a, m)[0]
    if b % g != 0:
        return None
    else:
        a = a // g
        b = b // g
        m = m // g
        return (inverted(a, m) * b) % m
```

```
Приклад для конгруенції 7x ≡ 6 mod 129 : 93
```

2. За допомогою коду з практикуму №1 знайшов 5 найчастіших біграм у шифртексті:

```
Топ 5 біграм за частотами:
Біграма: ээ, частота: 0.00827
Біграма: вд, частота: 0.00637
Біграма: чф, частота: 0.00626
Біграма: цг, частота: 0.00626
Біграма: гн, частота: 0.00626
```

3. Кожній біграмі, яку отримав та 5 найчастішим біграмам рос. мови співставив числа по формулі:

$$(x_{2i-1}, x_{2i}) \leftrightarrow X_i = x_{2i-1}m + x_{2i}.$$

```
Біграми в числовому значенні:
ст, но, то, на, ен : 545, 417, 572, 403, 168.
ээ, вд, чф, цг, гн : 896, 66, 733, 685, 106.
```

Знайшов кандидатів на ключ (a, b) розв’язуючи систему рівнянь:

$$\begin{cases} Y^* \equiv aX^* + b \pmod{m^2} \\ Y^{**} \equiv aX^{**} + b \pmod{m^2} \end{cases}.$$

4. Для кожного можливого ключа спробував дешифрувати текст (09.txt), при цьому якщо текст після дешифрування має біграми, які неможливо зустріти у рос. мові (критерій заборонених l-грам), а саме:

```
forbidden_bigrams = \
    ['аь', 'бй', 'бф', 'гщ', 'еь', 'жй', 'жц', 'жщ', 'жы', 'уь', 'фщ', 'хы', 'хь', 'цщ', 'цю', 'чф','чц',
    'чщ', 'чы', 'чю', 'шщ', 'шы', 'шю', 'щг', 'щж', 'щл', 'щх', 'щц', 'щч', 'щш', 'щы', 'щю','щя', 'ыь',
    'ьы', 'эа', 'эж', 'эи', 'эо', 'эу', 'эщ', 'эы', "эь", 'эю', 'эя', 'юы', 'юь', 'яы','яь', 'ьь']
```

або якщо текст не має зовсім символів, то я відкинув такий текст. Цікаво, що з усього списку таких біграм, більшість беззмістовних дешифрованих текстів не пройшли перевірку вже на першій біграмі, лише декілька дійшли до другої, і жоден до третьої.

5. В результаті один з дешифрованих текстів підійшов за критеріями:

```
Key: 378 711
Forbidden: аь
Key: 18 867
Forbidden: аь
Key: 314 34
Decrypted text:
мамапошламытьпосудуитомотправилсязанейкаждыйзвукзвонложкиилитарелкигулкораздавалсявзнойномвечернемв
Key: 568 949
Forbidden: аь
Key: 130 370
Forbidden: аь
```

Бачу, що текст має зміст (повний текст у файлі decrypted_text.txt), можна зробити висновок, що текст був зашифрований ключем (314, 34)

Висновок

У ході виконання даного практикуму я застосував частотний аналіз до шифртексту та побачив його ефективність для розкриття афінних шифрів підстановки. Також за результатом практикуму можна підтвердити, що статистичні властивості природної мови (а саме частоти біграм) зберігаються після шифрування і можуть бути використані для визначення ключа.