Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

КРИПТОГРАФІЯ

Комп’ютерний практикум №3

Варіант 7

Криптоаналіз афінної біграмної підстановки

Роботу виконав:
Студент 3 курсу
Групи ФБ-06
Кононець В. М.

Київ – 2022

Мета роботи

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

Постановка задачі

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). **Варіант №7**

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. Для написання функції пошуку оберненого елемента я використав розширений алгоритм Евкліда, та знання з теорії чисел. Для написання розв'язування порівнянь, я скористався додатковими відомостями у методичці

знаходиться за такою процедурою:

Нехай $ax \equiv b \pmod{n}$ і треба встановити значення x за відомими a та b. Маємо такі випадки:

1) $\gcd(a,n) = 1$. В цьому випадку порівняння має один розв'язок: $x \equiv a^{-1}b \pmod{n}$.
2) $\gcd(a,n) = d > 1$. Маємо дві можливості:
   2.1) Якщо b не ділиться на d, то порівняння не має розв'язків.
   2.2) Якщо b ділиться на d, то порівняння має рівно d розв'язків x_0, $x_0 + n_1$, $x_0 + 2n_1 \ldots$, $x_0 + (d-1)n_1$, де $a = a_1 d$, $b = b_1 d$, $n = n_1 d$ і x_0 є єдиним розв'язком порівняння $a_1 x \equiv b_1 \pmod{n_1}$: $x_0 = b_1 \cdot a_1^{-1} \bmod n_1$.

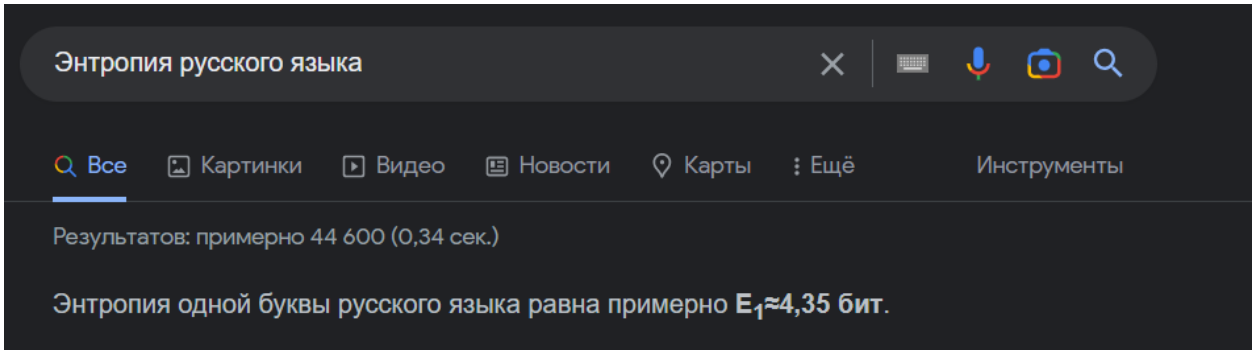
2. Для знаходження частот біграм бувло взято функцію із лаб1 та трохи її змінено.

Найчастіші біграми шифртексту варіанта 7 (5 штук):

['цл', 'ял', 'ае', 'ле', 'чо']

3. Третій крок видався найскладнішим для мене, бо було дуже багато виключень, наприклад біграма переходить сама у себе, чи дві найчастіші біграми мови не можуть переходити у одну й ту ж саму біграму ШТ, і навпаки. Тому на цьому кроці я возився довго. Але помізкувавши, усі виключення вдалося реалізувати.
   Щоб не пхати все у 3-4 функції, я вирішив розбити задачу на підфункції, і таким чином об'єднав усе до купи та отримав результат.
4. Напевно найпростішим кроком для мене видався розпізнавач змістовності тексту. Із набутих знань з перших двох практикумів, та довідки з методички, я обрав такий метод:

1) Кожен отриманий розшифруванням текст був перевірений на частоту зустрічаємості літер, зокрема на те, що найчастішою літерою тексту повинна бути «о» або «е». Якщо це не «о» або «е», то цей текст не змістовний.
2) Другим критерієм змістовності тексту було перевірити, чи є у тексті неможливі біграми, такі як: оь аь гь і т.д. Якщо такі біграми були знайдені, то текст не змістовний.
3) І останній критерій, який я використав – ентропія.



Тому текст перевірявся на ентропію в межах від 4.2 до 4.5.

5. Таким чином, за допомогою цих критеріїв, мені вдалося отримати одну єдину пару ключа :

```
(200, 900)
```

Висновки

У ході даної лабораторної роботи я набув навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанував прийоми роботи в модулярній арифметиці Написав програму, яка розшифровує афінний шифр методом криптоаналізу афінної біграмної підстановки. Закріпив знання з теорії чисел.