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

Криптографія

Комп’ютерний практикум №3

Варіант 1

Виконав
студент гр. ФБ-03 Антіпов Данило
Перевірив
Чорний Олег Миколайович

Київ — 2022

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 усіх.
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. Спочатку реалізував підпрограми із необхідними математичними операціями: знаходження НСД, обчислення оберненого елементу за модулем з використанням розширеного алгоритму Евкліда, а також розв'язування лінійних порівнянь, функції:

extended_gcd(),

inverse(),

solve_equation().

2. Далі за допомогою функції find_top_bigrams() знайшов 5 біграм, що зустрічаються в нашому зашифрованому тексті найчастіше. Їх перелік:

```
['рн', 'ыч', 'нк', 'цз', 'иа']
```

Також біграми переводимо у числовий формат:

```
['рн', 'ыч', 'нк', 'цз', 'иа']
[509, 860, 413, 689, 248]
```

Труднощі, що виникли при виконанні комп'ютерного практикуму:

На жаль не вдалося в повному обсязі реалізувати функції останніх двох пунктів в першу чергу через обмеження по часу, в яких я сам винний). А практичні проблеми виникли при спробі співставити біграми між собою.

Висновки:

При виконанні комп’ютерного практикуму мною були отримані навички частотного аналізу, опановані прийоми роботи в модулярній арифметиці. Були написані математичні підпрограми, які необхідні для подальшої реалізації алгоритму дешифрування афінного шифру методом криптоаналізу афінної біграмної підстановки. На жаль дешифрувати сам текст не вийшло, про що було написано у пункті про труднощі, але, прочитавши уважно методичні вказівки, я отримав теоретичні знання, зокрема по критеріях автоматичного визначення змістовного тексту, по тому як працює афінний шифр біграмної заміни, а також як проводиться атака на нього. Також були отримані навички роботи з біграмами.