Національний технічний університет України «КПІ» імені Ігоря Сікорського
Фізико-технічний інститут

Комп’ютерний практикум 3
Криптографія

Виконали:
студенти ФБ-21
Князян Кирило Андрійович
Новіцький Олександр Костянтинович

Криптоаналіз афінної біграмної підстановки

Мета роботи

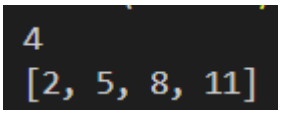
Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

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.

Хід роботи

1. Спочатку ми реалізували необхідні математичні операції, так як у коді не видно як воно працює і нічого не виводиться, ми взяли і окремо протестували 2 ці функції для демонстрації правильності їх роботи, також про коректність роботи свідчить безперебійна і якісна робота алгоритма при знаходженні ключа і дешифровці тексту:



Такі результати були отримані при подачі на вхід розширеного алгоритму евкліда значень 3 і 11, для яких 4 є дійсно оберненим до 3, а список із 2, 5, 8, 11 є результат подачі на вхід до функції обрахування

лінійних порівнянь значень 4, 8, 12, тобто якщо обрахувати самому, можна побачити, що знайдено всі 4 відповіді, тобто алгоритм повертає усі розв’язки, як і потрібно.

2. Тепер вивіли 5 найчастіших біграм, як і було необхідно, використано було функцію з першої лабораторної, але трохи модифіковано під потреби цієї:

```
PS D:\3> & D:/python/python.exe d:/3/crypto/3.py
5 найчастіших біграм ШТ:
Біграма: рн, частота: 0.0128913
Біграма: ыч, частота: 0.0090035
Біграма: нк, частота: 0.0087989
Біграма: цз, частота: 0.0075711
Біграма: тч, частота: 0.0067526
```

3. В кінці ми просто знайшли усі можливо правильні кандидати на ключ, використовуючи 5 найчастіших біграм, потім відсіяли повторювані ключі, подали їх на дешифрування і перевірили мову на змістовність за допомогою неможливих біграм мови, чого було достатньо, тому що ми отримали 1 правильний результат:

```
Знайдені ключі: a=13, b=151
Розшифрований текст: многограннуюличностьдостоевскогоможнорассматриватьсчетырехсторонкакписателякакневротикакакмыслителяэтикаикакгрешн
икакакжеразобратьсявэтойневольносмущающейнассложностинаименееспоренонкакписательместоеговодномрядусшекспиромбратьякарамазовывеличайший
романизвсехкогдалибонаписанныхалегендаовеликоминквизитореодноизвысочайшихдостиженийимировойлитературыпереоценитькотороеневозможноксожал
ениюпередпроблемойписательскоготворчествапсихоанализдолженсложитьоружиедостоевскийскореевсегоуязвимкакморалистпредставляяегочеловекомв
```

Тобто ми отримали ключ a=13, b=151 і по тексту зрозуміло, що він змістовний.

Висновки:

У результаті виконання третьої лабораторної роботи ми засвоїли частотний криптоаналіз на прикладі афінної біграмної підстановки. Ми навчились його розшифровувати, враховуючи 5 найчастіших біграми самої мови та ШТ та використовуючи повністю автоматизований алгоритм, який крім знаходження можливих ключів за допомоги виведеного у методичці рівняння і дешифрування тексту на основі знайдених ключів також перевіряє текст на змістовність (тут нам вистачило тільки 1 з методів для відсіювання зайвого)