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

Лабораторна робота №3

Криптоаналіз афінної біграмної підстановки

Виконали:
студентки ФБ-06
Товкач К.В.
Вєрнікова Л.Г.

Київ – 2022

Варіант 10

Мета роботи

Ознайомлення з тестами перевірки чисел на простоту і методами генерації ключів для асиметричної криптосистеми типу RSA; практичне ознайомлення з системою захисту інформації на основі криптосхеми RSA, організація з використанням цієї системи засекреченого зв'язку й електронного підпису, вивчення протоколу розсилання ключів.

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 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:

За допомогою функції top5_bigr ми пройшлись по тексту та знайшли 5 найчастіших біграм шифртексту:

1. **“сг”**
2. **“жэ”**
3. **“ям”**
4. **“нг”**
5. **“тм”**

Розпізнавач російської мови ми будували за певними критеріями змістовності тексту. Спочатку ми використали критерій по частоті вживання літер “о” та “е” - найчастіших літер російського алфавіту. Потім перевіряли можливість неіснуючих біграм, припущення яких вказали на початку програмного коду.

В даній функції ми відразу розшифровуємо текст нашими ключами (перебором), рахуємо літери які найчастіше зустрічаються. Записуємо їх в масив, при чому по спаданню. Тобто першою в нас стоїть літера, яка найчастіше зустрічається в тексті.

Потім беремо перший елемент масиву і перевіряємо його на співпадіння з найчастіше вживаними літерами в російській мові. Якщо перевірка пройдена, то ми переходимо до наступного критерію, де ми використовуємо функцію пошуку неіснуючих біграм з

нашого масиву. Якщо ми знаходимо неіснуючі біграми в розшифрованому тексті - то даний ключ нам не підходить, і ми переходимо на початок циклу для перевірки наступної пари ключа. І так відбувається до того моменту поки кількість неіснуючих біграм в тексті розшифрованому певним ключем не буде дорівнювати 0. В такому випадку ключ знайдено.

В ході виконання лабораторної роботи та за допомогою вищеописаного методу нами було знайдено невідомі параметри ключа **a,b**, шо дорівнюють **(300, 400)** відповідно.

Висновки:

В результаті виконання лабораторної роботи ми здобули навички частотного аналізу на прикладі моноалфавітної підстановки, попрацювали на практиці написання коду з модулярною арифметикою, і в результаті застосування знань з теорії реалізували код, за допомогою якого знайшли ключ для розшифрування афінного шифру за допомогою криптоаналізу біграмної підстановки.