Лабораторная работа №3

Математические основы защиты информации и информационной безопасности

Минов Кирилл Вячеславович | НПМмд-02-23

Содержание

1 Цель работы

Реализовать на языке программирования шифрование гаммированием конечной гаммой.

2 Теоретическое введение

Гаммирование - процедура наложения при помощи некоторой функции F на исходный текст гаммы шифра, то есть псевдослучайной последовательности (ПСП) с выходов генератора G. ПСП по своим статистическим свойствам неотличима от случайной последовательности, но является детерминированной, то есть известен алгоритм ее формирования. Чаще всего в качестве функции F берется операция поразрядного сложения по модулю два или по модулю N (N - число букв алфавита открытого текста).

Стойкость шифров, основанных на процедуре гаммирования, зависит от характеристик гаммы - длины и равномерности распределения вероятностей появления знаков гаммы.

3 Выполнение лабораторной работы

1)Импорт библиотек и объявление переменных: В этом шаге мы начинаем программу, импортируем необходимые библиотеки и объявляем переменные для открытого текста и ключа.

2)Преобразование строк в массивы символов: Мы преобразуем строки с открытым текстом и ключом в массивы символов (char arrays) для удобной работы с отдельными символами.

3)Создание алфавита: Мы создаем массив символов, представляющий собой русский алфавит, включающий буквы от 'а' до 'я'.

4)Создание нового ключа: Мы создаем новый ключ (gammaNew), который будет использоваться для шифрования. Этот ключ повторяет символы из исходного ключа (gamma) так, чтобы его длина совпадала с длиной открытого текста (word).

5)Шифрование открытого текста: на этом этапе каждый символ открытого текста преобразуется в шифрованный символ. Для этого: находим позиции символов в алфавите. Добавляем 1 к этим позициям (позиции начинаются с 0). Складываем позиции символов открытого текста и соответствующего символа из ключа. Результат делится по модулю на 32 (размер алфавита). Результат вычитается 1, чтобы получить шифрованный символ. Зашифрованные символы добавляются в массив cipher.

6)Вывод зашифрованного текста: Зашифрованные символы объединяются в строку, и эта строка выводится на экран.

```java
public class GammaEncryption {
    public static void main(String[] args) {
        String word = "приказ";
        String gamma = "гамма";
        word = word.replace( target: " ",  replacement: "");

        char[] wordChars = word.toCharArray();
        char[] gammaChars = gamma.toCharArray();

        char[] alphabet = new char[32];
        for (char c = 'а'; c <= 'я'; c++) {
            alphabet[c - 'а'] = c;
        }

        char[] gammaNew = new char[wordChars.length];
        for (int i = 0; i < wordChars.length; i++) {
            gammaNew[i] = gammaChars[i % gammaChars.length];
        }

        char[] cipher = new char[wordChars.length];
        for (int i = 0; i < wordChars.length; i++) {
            int numberWord = findCharIndex(alphabet, wordChars[i]) + 1;
            int numberGammaNew = findCharIndex(alphabet, gammaNew[i]) + 1;
            int k = (numberWord + numberGammaNew) % 32;
            cipher[i] = alphabet[k - 1];
        }

        String cipherText = new String(cipher);
        System.out.println(cipherText);
    }

    public static int findCharIndex(char[] arr, char c) {
        for (int i = 0; i < arr.length; i++) {
            if (arr[i] == c) {
                return i;
            }
        }
        return -1;
    }
```

Рис. 1: Реализация шифрования гаммированием

4 Выводы

В ходе выполнения данной лабораторной работы было реализовано шифрование гаммированием конечной гаммой на языке программирования Java.