Лабораторная работа №3

Математические основы защиты информации и информационной безопасности

Минов К.В., НПМмд-02-23

9 октября 2023

Российский университет дружбы народов

Москва, Россия

Цель лабораторной работы

1) Реализовать на языке программирования шифрование гаммированием конечной гаммой

Задачи лабораторной работы

1) Изучить теоретическую часть лабораторной работы по методичке
2) Написать соответствующую программу

Теоретическое введение

Гаммирование - процедура наложения при помощи некоторой функции F на исходный текст гаммы шифра, то есть псевдослучайной последовательности (ПСП) с выходов генератора G. Чаще всего в качестве функции F берется операция поразрядного сложения по модулю два или по модулю N (N - число букв алфавита открытого текста).

Ход выполнения лабораторной работы

- Реализуем шифрование гаммированием с конечной гаммой

```
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];
        }
```

-

Figure 1: Рис.1: Шифрование гаммированием

Реализуем шифрование гаммированием с конечной гаммой

```
    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;
}
```

Figure 2: Рис.2: Шифрование гаммированием

Вывод

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