Информационная безопасность

Лабораторная работа №7

Матюшкин Д. В.

19 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Матюшкин Денис Владимирович
- студент 4-го курса
- группа НПИбд-02-21
- Российский университет дружбы народов
- 1032212279@pfur.ru
- https://stifell.github.io/ru/

Цель работы

Цель работы

- Освоить на практике применение режима однократного гаммирования.

Задача

Задача

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

Программа

```java
public class Main {
    public static String xorText(String text, String key) {
        if (text.length() != key.length()) {
            return "Ошибка: Ключ и текст разной длины";
        }
        StringBuilder xorText = new StringBuilder();
        for (int i = 0; i < text.length(); i++) {
            char xorChar = (char) (text.charAt(i) ^ key.charAt(i));
            xorText.append(xorChar);
        }
        return xorText.toString();
    }
```

Продолжение кода

```
public static String generateKey(int length) {
    String chars = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0
    StringBuilder key = new StringBuilder();
    Random random = new Random();
    for (int i = 0; i < length; i++) {
        key.append(chars.charAt(random.nextInt(chars.length())));
    }
    return key.toString();
}
```

```
    public static void main(String[] args) {
        String text = "С Новым Годом, друзья!";
        System.out.println("Текст: " + text);
        String key = generateKey(text.length());
        System.out.println("Ключ: " + key);
        String encryptedText = xorText(text, key);
        System.out.println("Зашифрованный текст: " + encryptedText);
        String decryptedText = xorText(encryptedText, key);
        System.out.println("Расшифрованный текст: " + decryptedText);
    }
}
```

```
Текст: С Новым Годом, друзья!
Ключ: XAn2Gffi4baujFK7QddD2I
Зашифрованный текст: ογaөḰѵЭњIЧḱsыijkЃБЧѓJѽh
Расшифрованный текст: С Новым Годом, друзья!
```

Рис. 1: Вывод программы

Выводы

Выводы

- В ходе данной лабораторной работы мы освоили на практике применение режима однократного гаммирования.