Информационная безопасность

Лабораторная работа №7

Матюшкин Денис Владимирович (НПИбд-02-21)

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 Теоретическое введение

VirtualBox (Oracle VM VirtualBox) — программный продукт виртуализации для операционных систем Windows, Linux, FreeBSD, macOS, Solaris/OpenSolaris, ReactOS, DOS и других [1].

Rocky Linux — дистрибутив Linux, разработанный Rocky Enterprise Software Foundation. Предполагается, что это будет полный бинарно-совместимый выпуск, использующий исходный код операционной системы Red Hat Enterprise Linux (RHEL) [2].

# 3 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.

# 4 Программа

Написанная программа на Java:

import java.util.Random;  
  
/\*\*  
 \* @author Денис on 19.10.2024  
 \*/  
  
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();  
 }  
  
 public static String generateKey(int length) {  
 String chars = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789";  
 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);  
 }  
}

Вывод программы (рис. 1).

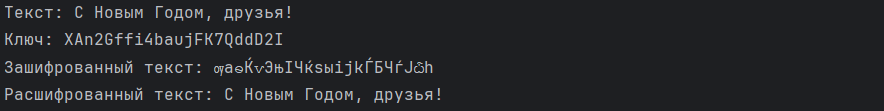


Рис. 1: Вывод программы

# 5 Выводы

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

# Список литературы

1. VirtualBox Documentation [Электронный ресурс]. Oracle, 2024. URL: <https://www.virtualbox.org/wiki/Documentation>.

2. Rocky Documentation [Электронный ресурс]. Rocky Enterprise Software Foundation, 2024. URL: <https://docs.rockylinux.org/ru/>.