Отчет по лабораторной работе по предмету Математические основы защиты информации и информационной безопасности

Лабораторная работа №3. Шифрование гаммированием

Никита Андреевич Топонен

Содержание

# 1 Цель работы

Цель работы — познакомиться с шифрованием гаммированием.

# 2 Задание

1. Реализовать шифрование гаммированием.

# 3 Теоретическое введение

Гаммирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле.

# 4 Выполнение лабораторной работы

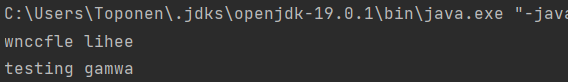
## 4.1 Шифрование гаммировнием

В рамках данной лабораторной работы я реализовал шифрование гаммированием на языке Java. Ниже приведен код:

import java.util.ArrayList;  
  
public class Gamma {  
 private final ArrayList<Character> alphabet = new ArrayList<>();  
 private final int alphabetSize;  
  
 public Gamma() {  
 for (char symbol = 'a'; symbol <= 'z'; symbol++) {  
 alphabet.add(symbol);  
 }  
 alphabetSize = alphabet.size();  
 }  
  
 public String encrypt(String text, int key) {  
 StringBuilder cryptogram = new StringBuilder();  
  
 key = key % alphabetSize;  
 for (int i = 0; i < text.length(); i++) {  
 char symbol = text.charAt(i);  
 if (symbol == ' ') {  
 cryptogram.append(" ");  
 } else {  
 int index = alphabet.indexOf(symbol);  
 index = xor(index, random(key, i)) % alphabetSize;  
 cryptogram.append(alphabet.get(index));  
 }  
 }  
 return cryptogram.toString();  
 }  
  
 public String decrypt(String text, int key) {  
 return encrypt(text, key);  
 }  
  
 private int random(int number, int count) {  
 int[] numbers = new int[]{5, 67, 21, 76, 13, 86, 32, 87, 3, 98, 21,  
 9, 11, 54, 94, 1, 4, 7, 55, 44, 32, 95, 33, 22, 64, 87, 30, 39,  
 65};  
 return numbers[(number \* count) % numbers.length] % alphabet.size();  
 }  
  
 private int xor(int a, int b) {  
 return a ^ b;  
 }  
}

public class Main {  
 public static void main(String[] args) {  
 Gamma gamma = new Gamma();  
 String message = "testing gamma";  
  
 String encryptedMessage = gamma.encrypt(message, 33);  
 System.out.println(encryptedMessage);  
  
 String decryptedMessage = gamma.decrypt(encryptedMessage, 33);  
 System.out.println(decryptedMessage);  
 }  
}

Результаты выполнения программы на иллюстрации (рис. ??).



Шифрование гаммированием

# 5 Выводы

В рамках данной лабораторной работы я познакомился с шифрованием гаммированием или XOR шифром. Также реализовал данный шифр на языке Java.

# Список литературы