

Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет информатики и
радиоэлектроники»

Факультет компьютерного проектирования

Кафедра инженерной психологии и эргономики

Дисциплина: Криптографические технологии

Отчет
по Практическому заданию №3
на тему: «Шифрование, дешифрование информации с применением
криптографических алгоритмов гаммирования»

Студент: гр. 910902

Шарупич К. А.

Руководитель:

Давыдович К.И.

Минск 2022

Цель работы: написать программу шифрования и дешифрования шифром XOR.

Ход работы

В ходе лабораторной работы была написана программа для шифрования и дешифрования шифром XOR на языке Java с записью результата в .txt файл. Листинг кода представлен ниже.

```
package org.example.lab3;

import java.io.*;
import java.util.Scanner;

public class Lab3 {
    private static final Scanner SCANNER = new Scanner(System.in);

    public static void main(String[] args) throws IOException {
        String message = scan("Message");
        String gammaKey = scan("Gamma key");
        String encodeResult = encodeMessage(message, gammaKey);
        String decodeResult = encodeMessage(encodeResult, gammaKey);
        System.out.println(encodeResult+" "+decodeResult);
        try (Writer writer = new BufferedWriter(new OutputStreamWriter(
            new FileOutputStream("filename.txt")))) {
            writer.write("Encoded: " + encodeResult+"\n");
            writer.write("Decoded: " + decodeResult);
        }
    }

    public static String encodeMessage(String message, String key) {
        byte[] messageBytes = message.getBytes();
        byte[] keyBytes = key.getBytes();
        byte[] result = new byte[messageBytes.length];
        for (int i = 0, j = 0; i < messageBytes.length; i++, j++) {
            if (j == keyBytes.length) {
                j = 0;
            }
            result[i] = (byte) (messageBytes[i] ^ keyBytes[j]);
        }
        return new String(result);
    }

    public static String scan(String variableName) {
        System.out.print(variableName + ": ");
        return SCANNER.nextLine();
    }
}
```

Результат выполнения представлен на рисунке ниже.

```
Message: it works!  
Gamma key: or not?  
Encoded:       T S  
Decoded: it works!
```

```
filename.txt x  
1 Message: it works!  
2 Gamma key: or not?  
3 Encoded: ACKACKNUL      ACKT  S  
4 Decoded: it works!  
5
```

Вывод. В ходе выполнения лабораторной работы была написана программа шифрования и дешифрования шифром XOR.