

Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерного проектирования

Кафедра инженерной психологии и эргономики

КРИПТОГРАФИЧЕСКИЕ ТЕХНОЛОГИИ
Практическая работа №3
Шифрование, дешифрование информации с применением
криптографических алгоритмов гаммирования

Проверил:
Давыдович К. И.

Выполнили:
Мисевич А. С.

Минск 2023

Цель работы

Изучение и криптоанализ криптографического алгоритма гаммирования.

Задача

Написать программу, используя любой известный нам язык программирования, которая будет шифровать и дешифровать текст алгоритмом гаммирования. В качестве гаммы использовать слово или фразу.

Листинг кода

```
import java.io.File;
import java.io.IOException;
import java.io.PrintWriter;
import java.nio.file.Files;
import java.nio.file.Paths;

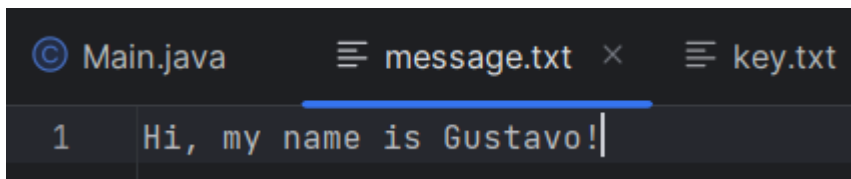
public class Main {
    public static void main(String[] args) throws
IOException {
        byte[] message =
Files.readAllBytes(Paths.get("message.txt"));

        byte[] key =
Files.readAllBytes(Paths.get("key.txt"));

        for(int i = 0, j = 0; i < message.length; i++,
j++) {
            if(j == key.length) j = 0;
            message[i] = (byte)(message[i] ^ key[j]);
        }

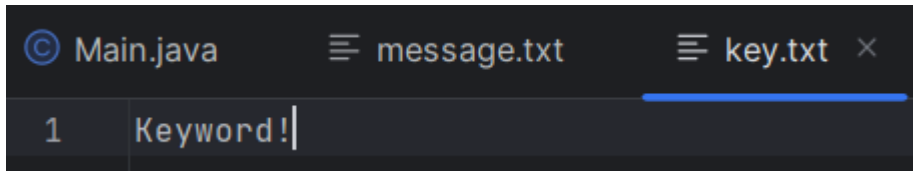
        PrintWriter pw = new PrintWriter(new
File("message.txt"));
        pw.print(new String(message));
        pw.close();
    }
}
```

Результат работы программы



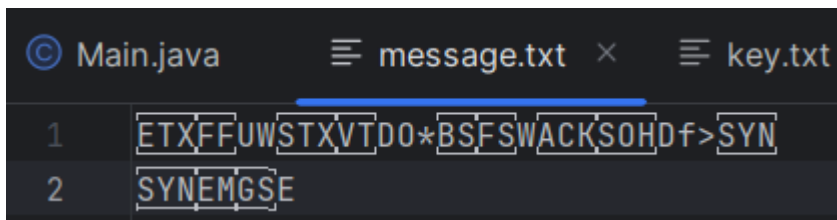
© Main.java message.txt × key.txt

```
1 Hi, my name is Gustavo!
```



© Main.java message.txt key.txt ×

```
1 Keyword!
```



© Main.java message.txt × key.txt

```
1 ETXFFUWSTXVTDO*BSFSWACKSOHDf>SYN
2 SYNEMGSE
```

Вывод

Был изучен криптографический алгоритм гаммирования.