

Санкт-Петербургский национальный исследовательский университет информационных
технологий, механики и оптики

Мегафакультет компьютерных технологий и управления

Факультет программной инженерии и компьютерной техники



Лабораторная работа 2.2

Информационная безопасность (Криптография)

Вариант 6

Группа: Р34151

Студент: Дау Конг Туан Ань

Преподаватель: [Маркина Татьяна Анатольевна](#)

г. Санкт-Петербург, 2024

Оглавление

1. Задачи	3
Цель работы:	3
Порядок выполнения работы:	3
2. Вариант	3
3. Выполнение	4
4. Рабочий код	4
5. Результат программы	6
6. Заключение	6

1. Задачи

Атака на алгоритм шифрования RSA методом повторного шифрования

Цель работы:

Изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

Порядок выполнения работы:

- ознакомьтесь с теорией в [3], рассмотренной в подразделе («Атака повторным шифрованием»);
- получите вариант задания у преподавателя;
- по полученным исходным данным, используя метод перешифрования, определите порядок числа e в конечном поле $Z_p() N$;
- используя значение порядка экспоненты, получите исходный текст методом перешифрования;
- результаты и промежуточные вычисления оформите в виде отчета.

Примечание. Для выполнения практического задания рекомендуется использовать программу PS.exe.

2. Вариант

Вариант = 6

Модуль, $N = 299547350633$

Экспонента, $e = 854929$

Блок зашифрованного текста, $C =$

273814931280
42731365375
226290712100
144895466043
54022172482
256403869247
20427366939
109560373874
17926624122
276548101136
138551457160
178721641850
153958773591

3. Выполнение

PS

Исходные данные: $N =$ $e =$ $Y =$ ☒ Show results

$Y_{i-1} =$ $Y_i =$

$X =$ $i =$

М

С

273814931280
42731365375
226290712100
144895466043
54022172482
256403869247
20427366939
109560373874
17926624122
276548101136
138551457160
178721641850
153958773591

станций кольца) в Token Ring. При возникшем у вас __

4. Рабочий код

[Link to github](#)

```
public class ModelreEnc implements Model{  
  
    private InputOnePair input;  
  
    private String result;
```

```

public ModelreEnc(InputOnePair inp) {

    this.result = "";

    this.input = inp;

}

@Override

public void solve() {

    try{

        for(String stri : input.getC()) {

            BigInteger y = BigInteger.valueOf(Long.parseLong(stri));

            BigInteger yi = y.modPow(input.getE(), input.getN());

            BigInteger res = BigInteger.ZERO;

            while(y.compareTo(yi) != 0) {

                res = yi;

                yi = yi.modPow(input.getE(), input.getN());

            }

            String temp = new String(res.toByteArray(), "windows-1251");

            if(temp.charAt(0) == 0) temp = temp.substring(1);

            this.result += temp.substring(0, temp.length());

        }

    } catch(UnsupportedEncodingException e) {}

}

public String getResult() {

    return this.result;

}

```

}

5. Результат программы

message = станций кольца) в Token Ring. При возникшем у вас __

6. Заключение

В ходе выполнения данной лабораторной работы я ознакомился с методом повторного шифрования для атаки на алгоритм шифрования RSA.