

УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

Направление подготовки 09.03.04 Программная инженерия

Дисциплина «Информационная безопасность»

### **Лабораторная работа №2.3**

Атака на алгоритм шифрования RSA методом бесключевого чтения

*Вариант 22*

Студент

*Патутин В. М.*

*P33101*

Преподаватель

*Маркина Т. А.*

Санкт-Петербург, 2022 г.

## Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

Исходные данные:

$N = 606089625293$

$e_1 = 524123$

$e_2 = 1109309$

$C_1 =$

496663520230

573686340098

317277380080

311062242263

87966670626

156120202050

517816376872

255107405391

70642465288

390229374493

333422604916

2671384922

509131255766

$C_2 =$

196561923290

102658895412

577585560553

44037449636

508496748333

278687486043

261550581766

487843663934

314450235982

345028986924

104569551730

486557652833

337080661180

## Алгоритм выполнения

1. Решаем уравнение ( $e1 \cdot r - e2 \cdot s = \pm 1$ ). В поле A помещаем значение  $e1$ , в поле B – значение  $e2$ . В поле C появляется значение  $s$ ; В поле D значение  $r$ .
2.  $c1$  возводим в степень  $r$ , а  $c2$  – в степень  $(-s)$ . После этого результаты перемножаем. Получаем  $m^{(e1 \cdot r - e2 \cdot s)}$ .
3. Берем модуль от полученного значения:  $(m^{(e1 \cdot r - e2 \cdot s)} \bmod N)$  и преобразуем в текст.

## Выполнение работы

The screenshot shows the BCalc application window. On the left, there is a grid with fields A, B, C, and D. Field A contains the value 3991469856. Below the grid are several buttons for operations:  $D = A + B$ ,  $D = A^B \bmod C$ ,  $D = \text{text}(A)$ ,  $D \rightarrow A$ ,  $D = A * B$ ,  $D = A^{(1/B)}$ ,  $D = \text{number}(A)$ ,  $D \rightarrow \text{table}$ ,  $D = A \div B$ ,  $A * D - B * C = N$ , Increase number of rows, and  $D = A \bmod C$ . At the bottom of the grid are buttons for 'Clear D', 'Clear A, B, C', and 'Clear grid'. On the right, there is a table with the following data:

|             | AD - BC = 1              |
|-------------|--------------------------|
| N           | 606089625293             |
| e1          | 524123                   |
| e2          | 1109309                  |
| s           | 241895                   |
| r           | 511972                   |
| c1          | 496663520230             |
| c2          | 196561923290             |
| $c1^r$      | 319462924410             |
| $c2^{(-s)}$ | 428027456651             |
| $c^d$       | 136738903029502964750910 |
| m           | 3991469856               |
| text        | ния                      |
| c1          | 573686340098             |
| c2          | 102658895412             |
| $c1^r$      | 334120668455             |
| $c2^{(-s)}$ | 534174611447             |
| $c^d$       | 178478778248361534804385 |
| m           | 4176014843               |
| text        | шины                     |
| c1          | 317277380080             |
| c2          | 577585560553             |
| $c1^r$      | 378329096736             |
| $c2^{(-s)}$ | 28521721808              |
| $c^d$       | 10790597248976112818688  |
| m           | 740352032                |
| text        | , a                      |

Вывод программы:

3991469856  
4176014843  
740352032  
4159041765  
3877694949  
3790531580

4176406816  
3907908325  
4041400555  
551743717  
3974491624  
773902320  
3894419488

### Итоговый текст:

ния шины, а через небольшой интервал времени. При

### Выводы

В данной лабораторной работе я изучил атаку на алгоритм шифрования RSA методом бесключевого чтения.