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 13*

Студент

*Крюков А.Ю*

*P33101*

Преподаватель

*Маркина Т. А.*

Санкт-Петербург, 2022 г.

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

Исходные данные:

*N =* 518587807081

*e1 =* 293177

e2 = 1209781

C1 =

373852443734

447989059513

140756140384

207791711792

252160015422

151272799305

431450717984

252882800366

112417596471

301753741810

480461056512

334158277030

368394150653

C2 =

22286870422

343015689591

281801228231

360270382562

264253306719

128520421967

399665129411

448878989738

70913527757

295285211952

247990966487

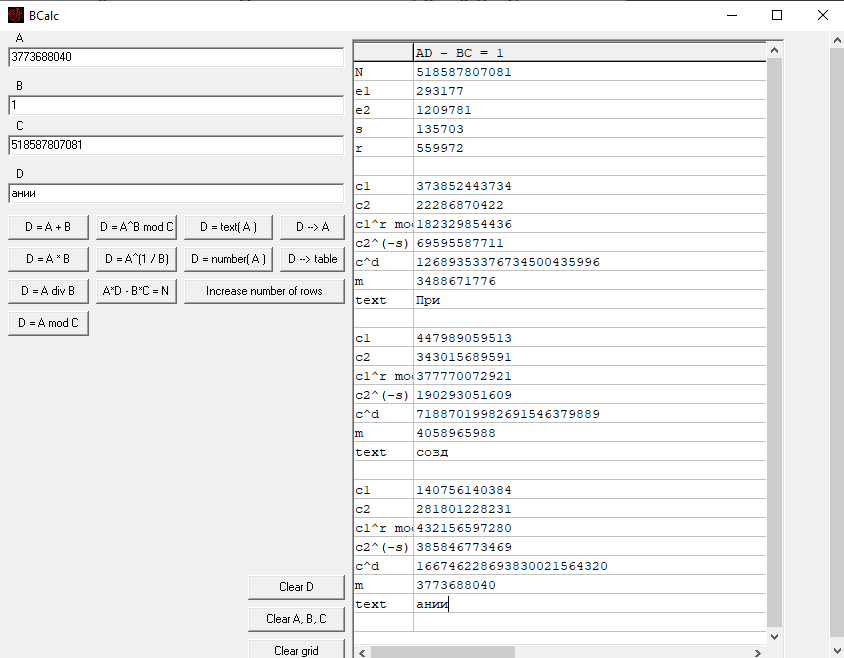
202711954425

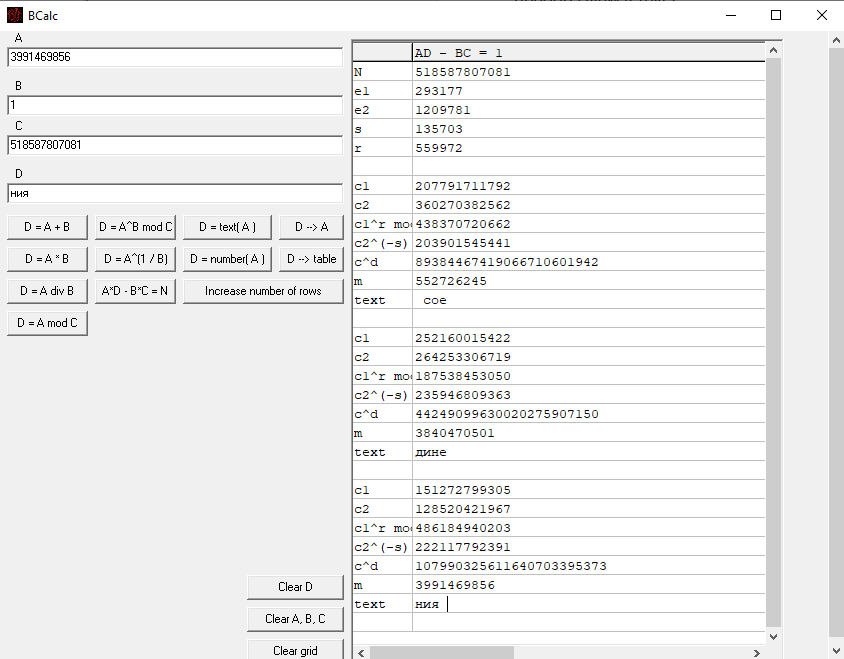
201121363025

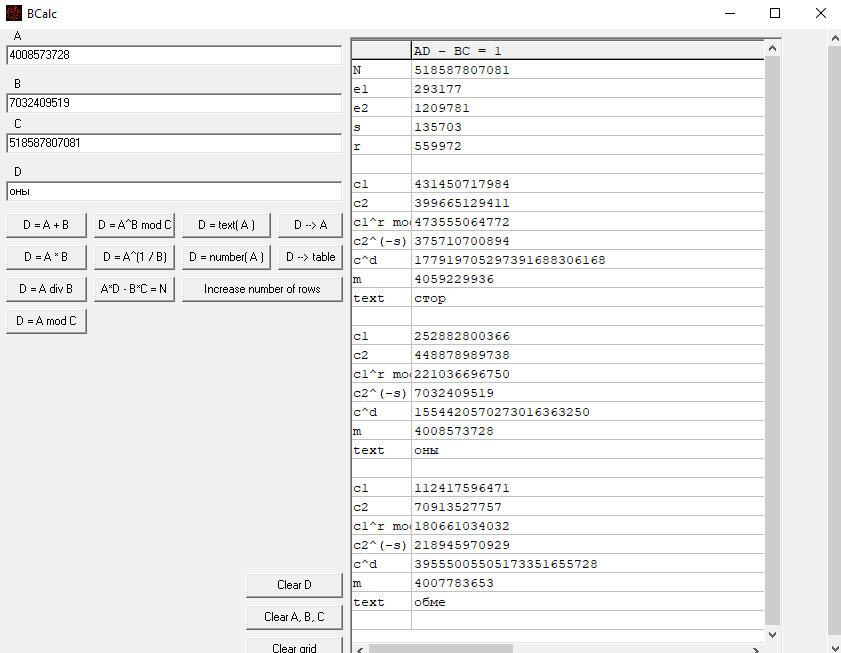
Алгоритм выполнения

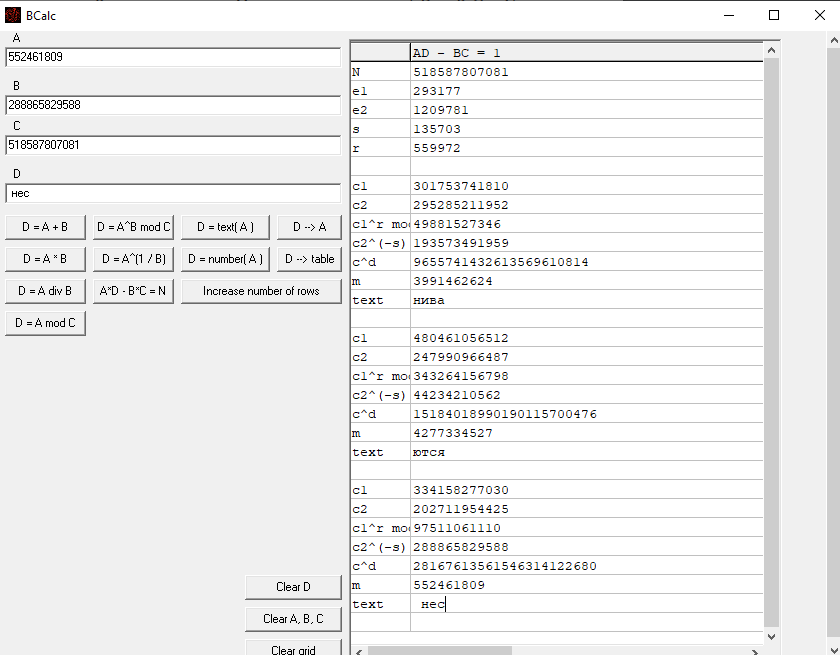
1. Решаем уравнение (e1∙r – e2∙s = ±1). В поле A помещаем значение e1, в поле B – значение e2. В поле C появляется значение s; В поле D значение r .
2. c1 возводим в степень r, а c2 – в степень (–s). После этого результаты перемножаем. Получаем m^(e1∙r – e2∙s).
3. Берем модуль от полученного значения: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

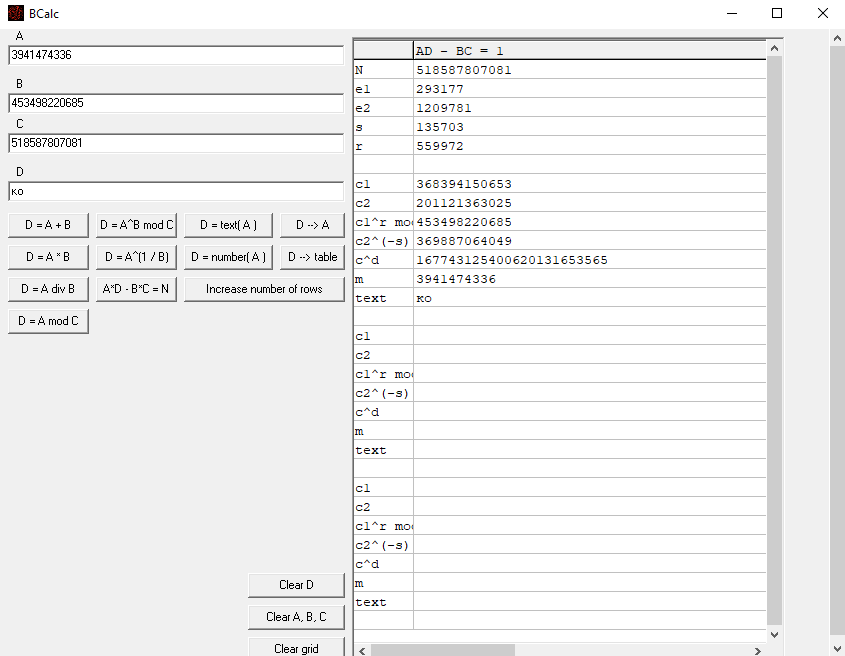
Выполнение работы











Итоговый текст:

При создании соединения стороны обмениваются неско

Выводы

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