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

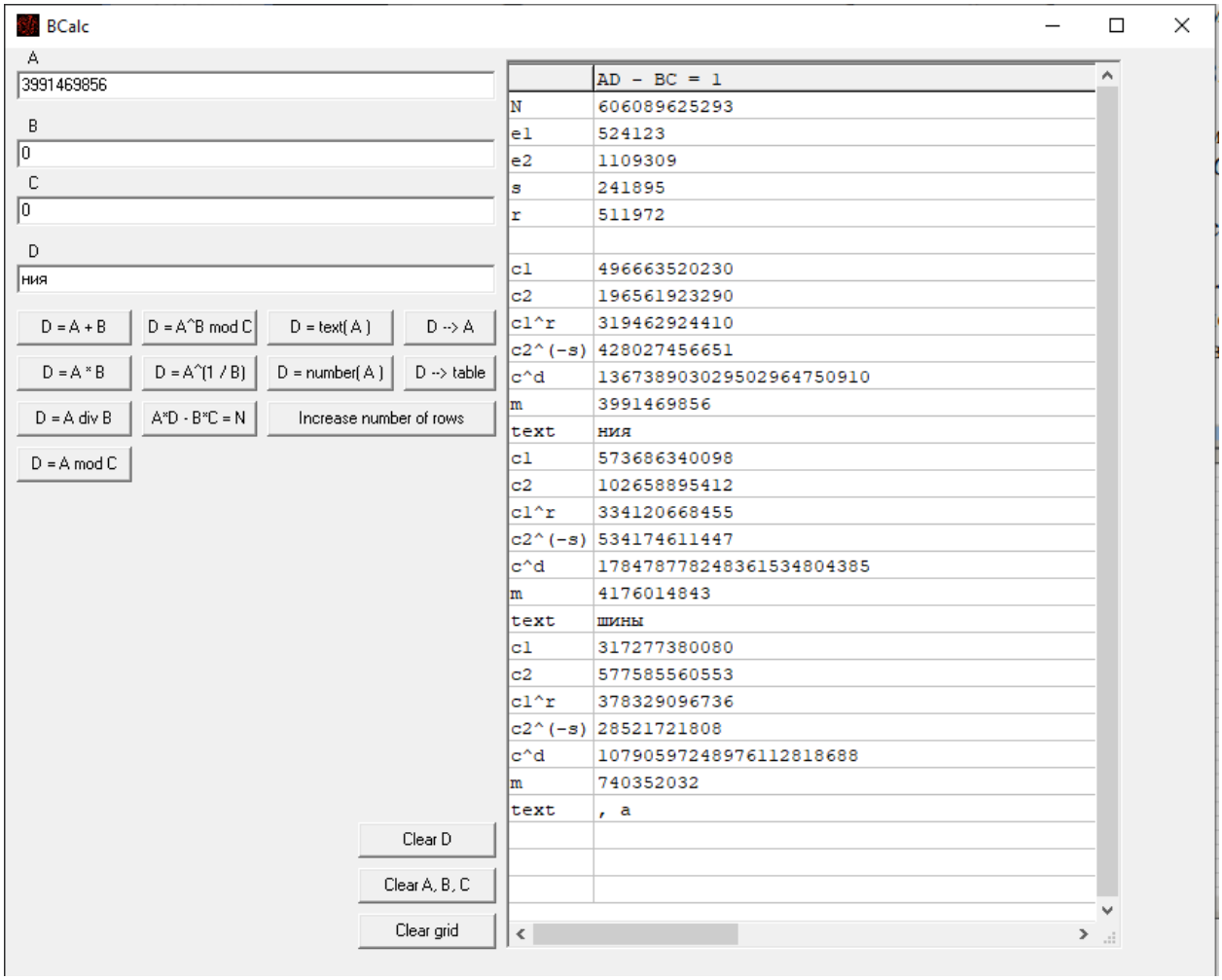
C_2 =

196561923290
102658895412
577585560553
44037449636
508496748333
278687486043
261550581766
487843663934
314450235982
345028986924
104569551730
486557652833
337080661180

Алгоритм выполнения

1. Решаем уравнение (e1·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



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.