Национальный исследовательский университет ИТМО

Факультет Программной Инженерии и Компьютерной Техники

Вариант №26

Лабораторная работа №2.3

«Атака на алгоритм шифрования RSA методом бесключевого чтения»

По дисциплине:

«Информационная безопасность»

Работу выполнила:

Студентка группы P34102

Никонова Наталья Игоревна

Преподаватель:

Рыбаков Степан Дмитриевич

Санкт-Петербург

2023

Цель работы

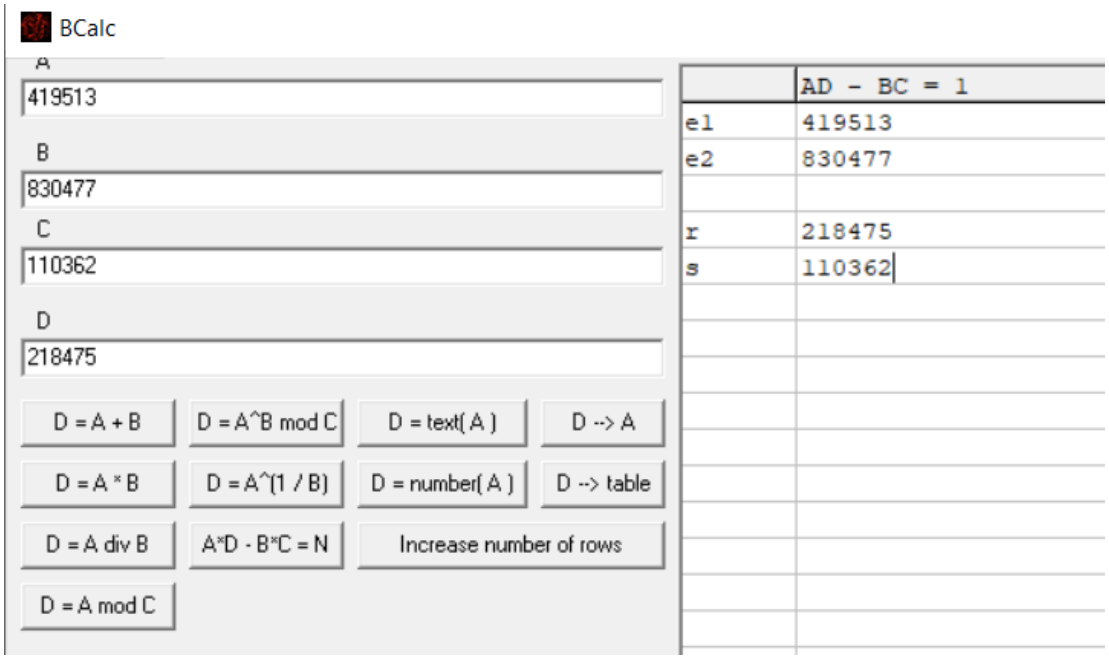
Изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

Вариант

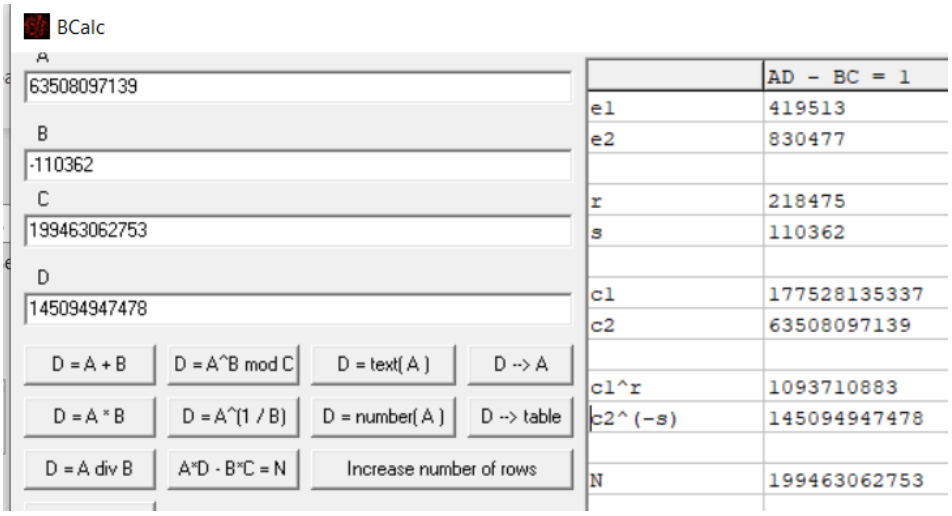
№	N	E1	E2	C1	C2
26	199463062753	419513	830477	177528135337 131197957980 181321285074 96738779356 127632416974 161779284378 148599198368 2033602084 141914496373 105405878640 120038779975 7139491789	63508097139 142467940607 131649552179 182684157712 22912524157 94825501208 189716623763 86236434624 94875774697 120252092430 26215384541 53782670605

Выполнение

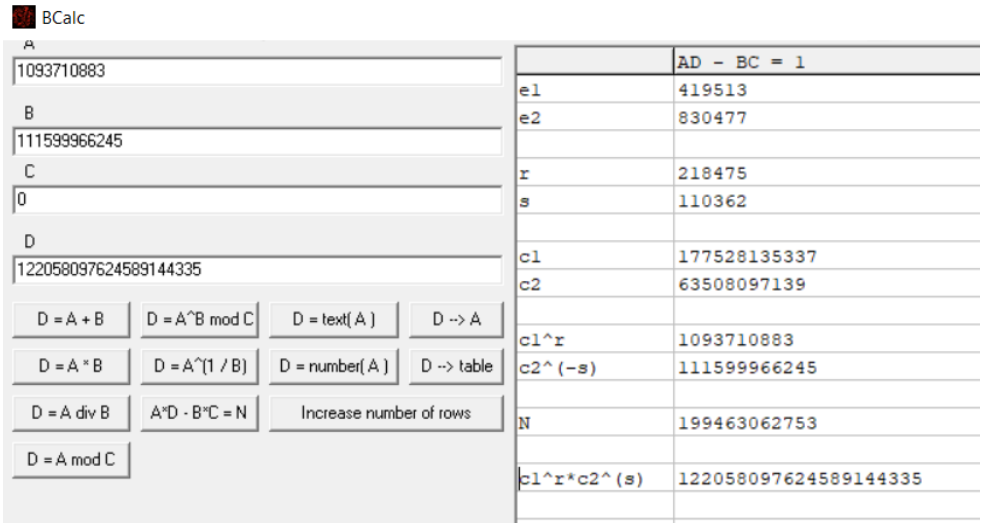
1. Решение уравнения $e_1 * r - e_2 * s = \pm 1$



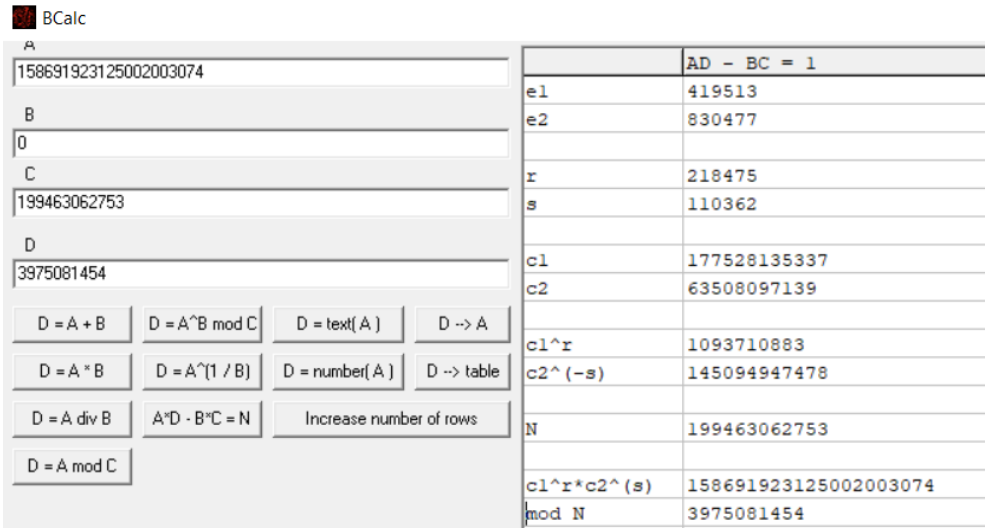
2. Возводим c1[0] в степень r по модулю N, а c2[0] – в степень (-s) по модулю N.



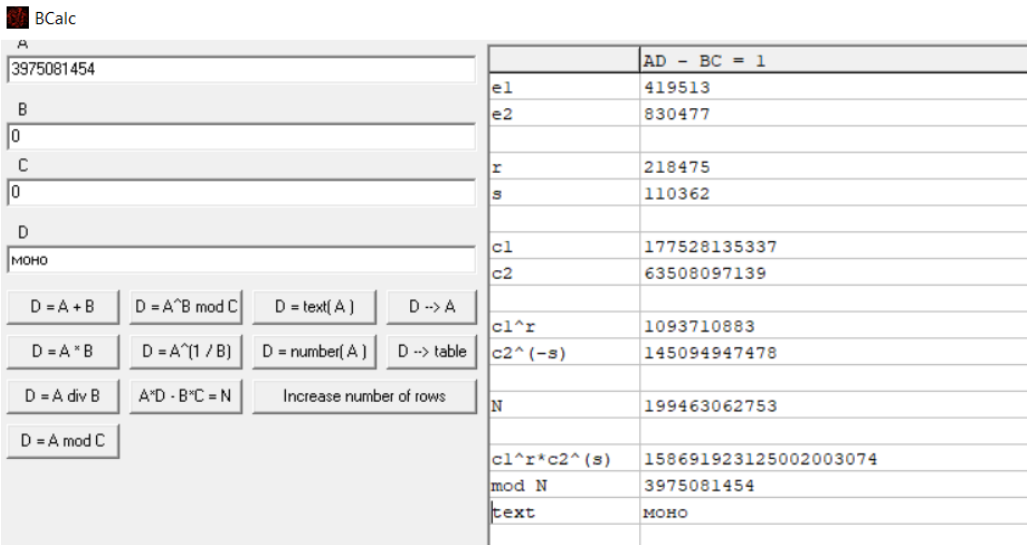
Перемножаем полученные значения



Берем модуль



Расшифровываем значение



3. Текст получился не битый – все высчитано верно и можно продолжать расшифровывать текст

c1	131197957980
c2	142467940607
c1^r	53544889324
c2^(-s)	9162749179
*	490618390693126864996
mod N	4025412604
text	поль
c1	181321285074
c2	131649552179
c1^r	125925619509
c2^(-s)	91326209934
*	115003095633479400024 06
mod N	3991806183
text	но з
c1	96738779356
c2	182684157712
c1^r	194343675467
c2^(-s)	55328911260
*	107528239738558820584 20
mod N	3774210784
text	ахва
c1	127632416974
c2	22912524157
c1^r	124029759789
c2^(-s)	149794311078
*	185789524207630816425 42
mod N	4075352828
text	тить

c1	161779284378
c2	94825501208
c1^r	134488296193
c2^(-s)	146399457422
*	196890135922644281944 46
mod N	552527085
text	одн
c1	148599198368
c2	189716623763
c1^r	84685337907
c2^(-s)	40162803630
*	340120059669903620241 0
mod N	3760253159
text	а из
c1	2033602084
c2	86236434624
c1^r	75916506396
c2^(-s)	179642871635
*	136378592134742844774 60
mod N	552727264
text	ста
c1	141914496373
c2	94875774697
c1^r	116443442636
c2^(-s)	61777863558
*	719362711139060785888 8
mod N	3992381673
text	нций

c1	105405878640
c2	120252092430
c1^r	18429026961
c2^(-s)	57260719857
*	1055259350050921064577
mod N	740356078
text	, по
c1	120038779975
c2	26215384541
c1^r	121704007889
c2^(-s)	44117095228
*	5369227305668276253692
mod N	4059229951
text	стоя
c1	7139491789
c2	53782670605
c1^r	66208570704
c2^(-s)	84135096222
*	5570464466902130280288
mod N	3991793184
text	нно

Итоговая расшифрованная фраза: монопольно захватить одна из станций, постоянно

Вывод

В ходе выполнения лабораторной работы я познакомилась с очередным методом атаки на шрифт RSA. Этот экземпляр показался достаточно простым, без неизвестно заранее количества возведений в степень как во втором способе и без подбора значений. Но вначале необходимо решить уравнение через расширенный алгоритм Евклида для двух взаимно простых числе (поэтому из НОД = 1), а его реализация рекурсивна и неизвестна сложность.