ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

ЛАБОРАТОРНАЯ РАБОТА № 2.1 ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Атака на алгоритм шифрования RSA посредством метода Ферма

Выполнил: Давыдов Иван Денисович

Группа: Р3400

Вариант 5

Санкт-Петербург 2020/2021

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

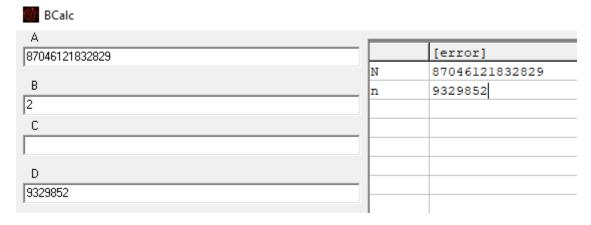
Задание

Вариант	Модуль, N	Экспонента, е	Блок зашифрованного
			текста, С
5	8704612183282	2342047	38288567928461
	9		32933111631628
			3796990272007
			14526017018271
			6637183116942
			46455894660145
			17024410119252
			49991104309343
			20967672129390
			3377231740209
			37201047739579
			56818318686813

Выполнение

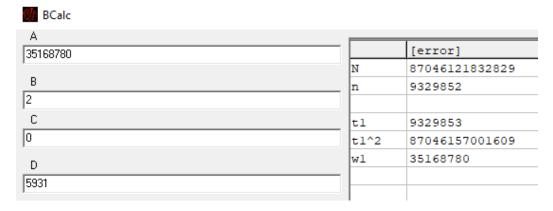
Для выполнения лабораторной работы использовалась программа BCalc.exe.

Найдем n = [sqrt(N)]:



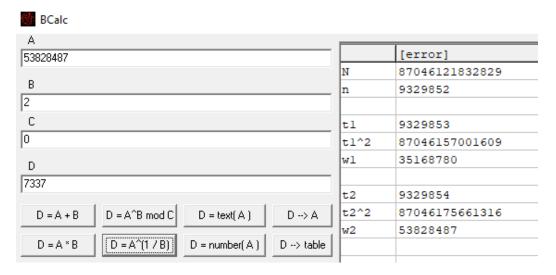
N не является квадратом целого числа, т.к. вверху таблицы высветилось сообщение об ошибке.

Проверим $w = (n + k)^2 - N, k = 1$:



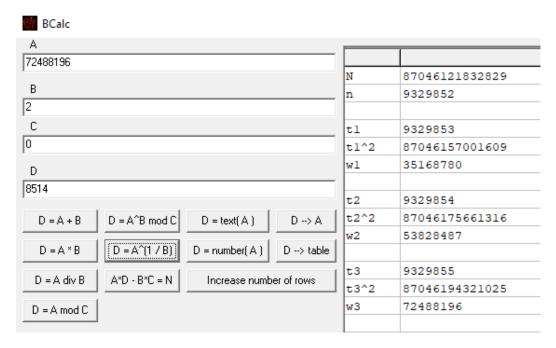
w не является квадратом целого числа

Проверим $w = (n + k)^2 - N, k = 2$:



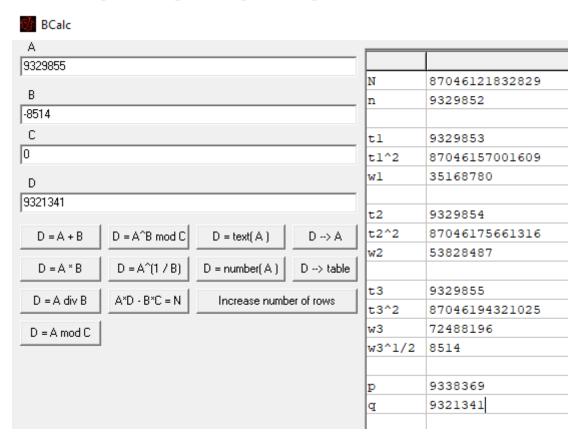
w не является квадратом целого числа

Проверим $w = (n + k)^2 - N, k = 3$:

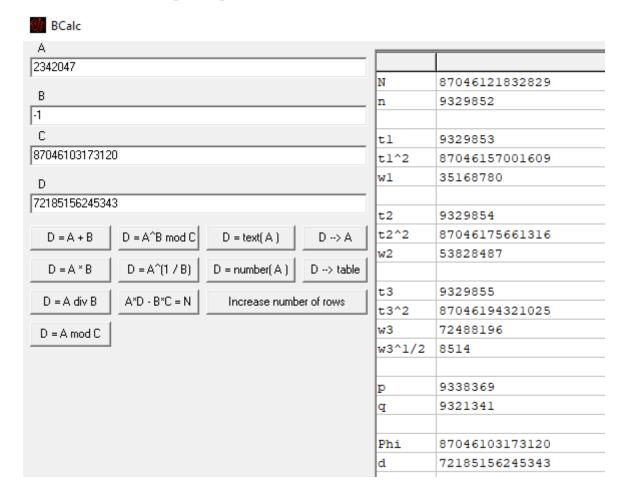


w является квадратом целого числа

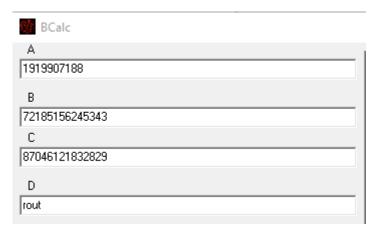
Вычислим p = t3 - sqrt(w) и q = t3 + sqrt(w):



Найдем Phi(n) и параметр d:



Далее, расшифруем сообщение:



Криптограмма	Сообщение	Текст
38288567928461	1919907188	rout
32933111631628	1702045998	es).
3796990272007	550429933	Одн
14526017018271	3995987168	о-ма
6637183116942	4042846451	ршру
46455894660145	4075682793	тный
17024410119252	552591594	пак
49991104309343	3857850607	ет п
20967672129390	4009747179	оявл
3377231740209	4293260017	яетс
37201047739579	4280349422	я то
56818318686813	3959220974	лько

Итоговое сообщение: «routes). Одно-маршрутный пакет появляется только»

Вывод

В ходе выполнения данной лабораторной работы была успешно произведена атака на алгоритм RSA методом Ферма.