ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет Программной Инженерии и Компьютерной Техники

Дисциплина:
«*Информационная безопасность*»
(Криптографические системы с открытым ключом)

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4
«Атака на алгоритм шифрования RSA, основанная на Китайской теореме об остатках»

Вариант 9

Выполнил:
Студент гр. P34151
Соловьев Артемий Александрович

Преподаватель:
Маркина Татьяна Анатольевна

Санкт-Петербург
2024г.

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством Китайской теоремы об остатках.

Задание

- Используя Китайскую теорему об остатках, получите исходный текст;
- Результаты и промежуточные вычисления значений для любых трех блоков шифрованного текста оформите в виде отчета.

Для всех вариантов экспонента $e = 3$

По варианту:

Вариант	Модуль, N			Блок зашифрованного текста		
	N_1	N_2	N_3	C_1	C_2	C_3
9	441716293693	442258294987	444399387571	324500796659	364411844182	57065247639
				324547036186	137247785047	130359065508
				367901833181	389030356498	391859459727
				38558700097	293766643714	128196485994
				401956144715	259139396276	412050631244
				260421328704	429702138150	367300386309
				356041474179	17968702271	83703862830
				113539876955	84037113464	218100297714
				304515179769	91988591941	10243576841
				302662240842	425057692992	232358719915
				282367185538	391906969363	412546535924
				432213853716	244207991747	398872645339

Ход работы

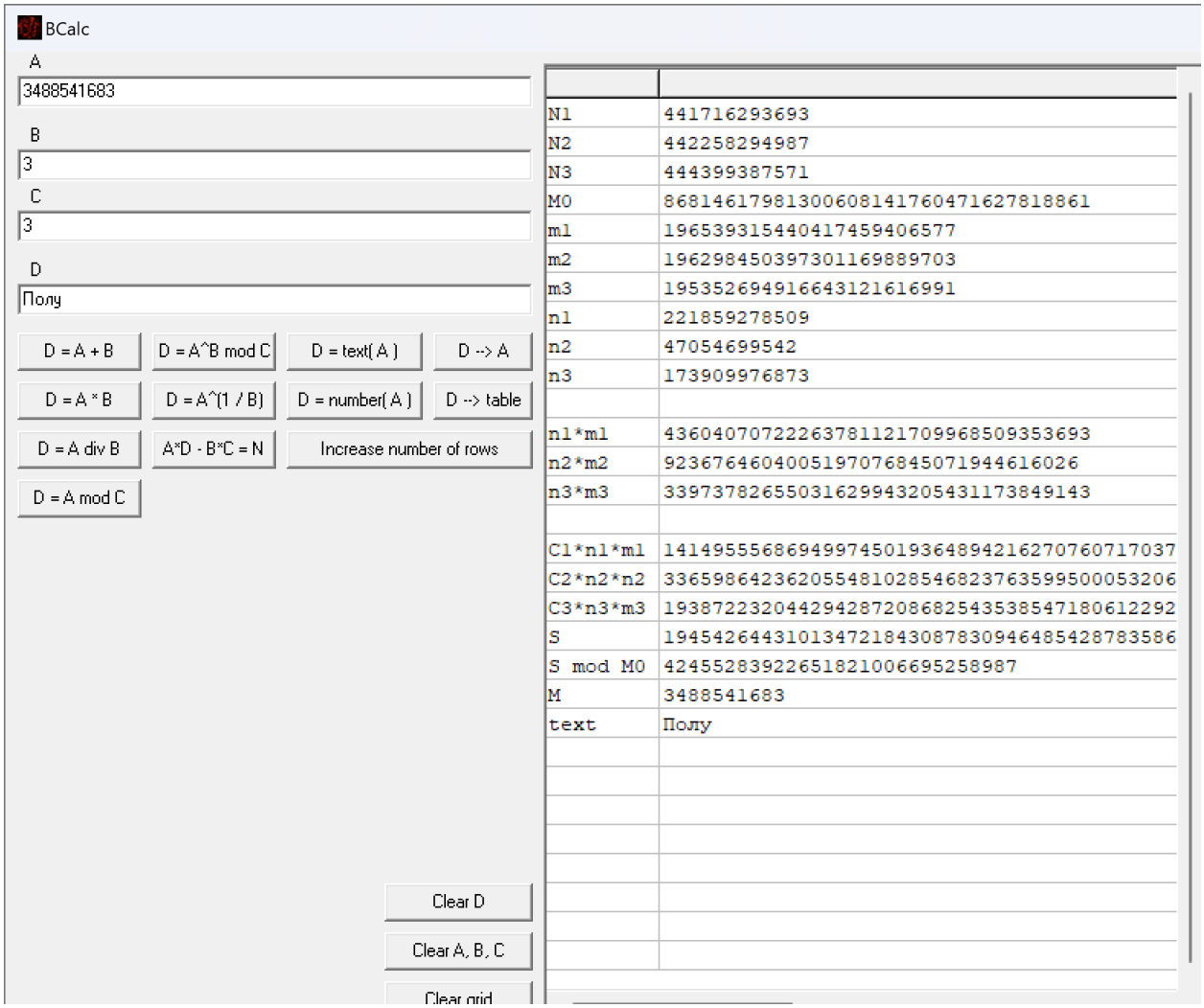
1. Последовательно вычисляем параметры:
   a. $M_0 = N_! \cdot N_2 \cdot N_3 =$
   b. $m_1 = N_2 \cdot N_3 =$
   c. $m_2 = N_1 \cdot N_3 =$
   d. $m_3 = N_1 \cdot N_2 =$
   e. $n_1 = m_1^{-1} mod\ N_1 =$
   f. $n_2 = m_2^{-1} mod\ N_2 =$
   g. $n_3 = m_3^{-1} mod\ N_3 =$
2. Вычисляем значение для блока зашифрованного текста
$$S = \mathrm{C}_1 \cdot n_1 \cdot m_1 + \mathrm{C}_2 \cdot n_2 \cdot m_2 + \mathrm{C}_3 \cdot n_3 \cdot m_3 =$$
3. Вычисляем значение $M = (S\ mod\ M_0)^{\frac{1}{3}}$
4. Преобразуем результат в текст
5. Повторяем шаги 2–4 для каждой строки

№	M	Текст
1	3488541683	Полу
2	4158714597	чате
3	3959169258	ль к
4	3773100256	адра
5	552595170	пов
6	4075745517	торн

7	3995132667	о вы
8	4159238635	числ
9	4293259808	яет
10	1129464608	CRC
11	3940607216	кадр
12	3760227630	а…

Расшифрованное сообщение: «Получатель кадра повторно вычисляет CRC кадра…»

Скриншот работы программы



Вывод

В ходе выполнения лабораторной работы я ознакомился с методом, основанным на китайской теореме об остатках, для атаки на RSA-шифрование.