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 №1
«Атака на алгоритм шифрования RSA посредством метода Ферма»

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 метода Ферма.

Задание

Используя разложение модуля на простые числа методом Ферма и полученные исходные данные, определите следующие показатели:

- множители модуля (p и q);
- значение функции Эйлера для данного модуля $\phi(N)$;
- обратное значение экспоненты по модулю $\phi(N)$;
- дешифруйте зашифрованный текст, исходный текст должен быть фразой на русском языке;
- результаты и промежуточные вычисления оформите в виде отчета.

По варианту:

Вариант	Модуль, N	Экспонента, e	Блок зашифрованного текста, C
9	78908333904637	2821057	66488995800290 61829195949215 75187156530365 66944513684556 15641889286263 25273508344802 33011686981708 63079735408371 71989137480846 15936556748887 35940951317181 65389528900590

Ход работы

1) Вычисляем $n = \lceil \sqrt{N} \rceil + 1$
   D = 8883037, в первой строке таблицы [error], так как N – не квадрат целого числа.
2) $t_1 = n + 1$. Возводим t_1 в квадрат.
   $t_1^2 = 78908364109444$.
   Вычисляем $w_1 = t_1 - N$.
   $w_1 = 30204807$. Проверяем является ли w_1 квадратом целого числа. В первой строке таблицы появляется [error] → w_1 не является квадратом целого числа.
3) Необходимо повторять пункт 2 до тех пор, пока w_n не станет квадратом целого числа:

№	t	t^2	w	result
1	8883038	78908364109444	30204807	[error]
2	8883039	78908381875521	47970884	[error]
3	8883040	78908399641600	65736963	[error]
4	8883041	78908417407681	83503044	

w_4 – квадрат целого числа 9138

4) Вычисляем $p = t_4 + \sqrt{w_4}$ = 8892179
5) Вычисляем $q = t_4 - \sqrt{w_4}$ = 8873903
6) Вычисляем $\phi(N) = (p-1)(q-1) = 78908316138556$
7) Вычисляем $d = e^{-1} mod\ \phi(N) = 20249014412785$
8) Проводим дешифрацию блоков

Блок зашифрованного текста	Расшифрованный блок текста
66488995800290	Если
61829195949215	меж
75187156530365	ду к
66944513684556	ольц
15641889286263	ами
25273508344802	разм
33011686981708	ещен
63079735408371	о не
71989137480846	скол
15936556748887	ько
35940951317181	мост
65389528900590	ов,_

Полученный результат: «Если между кольцами размещено несколько мостов,_»

Вывод

В ходе выполнения лабораторной работы я ознакомился с методом Ферма для атаки на RSA-шифрование.