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 методом бесключевого чтения»

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 бесключевого чтения.

Задание

- По полученным данным определить r и s при условии чтобы $e_1 \cdot r - e_2 \cdot s = \pm 1$. Для этого необходимо использовать расширенный алгоритм Евклида
- Используя полученные выше значения r и s, записать исходный текст
- Результаты и промежуточные вычисления значений для любых трех блоков шифрованного текста оформить в виде отчета.

По варианту:

Вариант	Модуль, N	Экспоненты		Блок зашифрованного текста	
		e_1	e_2	C_1	C_2
9	319418480417	602087	523639	52405618926 216147098445 216743861265 66972942908 191820297330 190353918873 110095200781 90183965366 296876615222 154988611456 166443759664 9906682687	82810335170 187684665216 48173641649 96024498047 247351492178 97241452868 255901558905 27364319220 227156630511 66990230889 183816391944 104719299259

Ход работы

1) Решаем уравнение $e_1 \cdot r - e_2 \cdot t = \pm 1$.
   для этого в поле A помещаем значение e_1 в поле B помещаем значение e_2.
   После нажатия кнопки «A*D - B*C =N», $C = s = 204285$, $D = r = 177668$
2) Производим дешифрацию: c_1 возводим в степень r, а c_2 в степень s по модулю N.
   $c_1^r = 693599752686$, $c_2^{-s} = 145671594031$
3) После находим $m\text{^}(e_1 r - e_2 s) = 10103778159240296425308$, перемножив c_1^r и c_2^r.
4) Берем модуль от полученного значения $m\text{^}(e_1 r - e_2 s)\ mod$ N.
   Получаем: 4075692116
5) Преобразуем в текст «то Т»
6) Повторяем алгоритм для остальных значений С

C1	C2	$m\text{^}(e_1 r - e_2 s)$	$m\text{^}(e_1 r - e_2 s)\ mod$ N	Дешифрованный текст
216147098445	187684665216	78937650747437903687 4	112932811 1	СР-п
216743861265	48173641649	46186359834117322773 800	404219261 3	роце

669729429098	960244980447	65939967765027250878 36	4059111665	сс с
191820297330	247351492178	6834486101997585217496 2	3857769189	ерве
190353918873	972414528688	1870543168678264582532 8	4 041 220 33 5	ра п
110095200781	255901558905	8467252152121312822000 4	4007981794	одтв
901839653666	273643192220	1280633689721636466559 2	3857770212	ержд
296876615222	227156630511	3867232217645264903544	3773166112	ает
154988611456	669902308889	4765704327269521753754 0	686891247	(с п
166443759664	183816391944	4176899185647681268278	4008505081	омощ
9906682687	104719299259	2424145410141789995618	4244512800	ью

Вывод

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