

федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»

Лабораторная работа №5

по дисциплине “Информационная безопасность”

на тему “Атака на алгоритм шифрования RSA

методом бесключевого чтения ”

Вариант 3

Выполнила: Студентка гр. Р3402

Калугина М. М.

Преподаватель: к.т.н, доцент

Маркина Т.А.

г. Санкт-Петербург

2021 г.

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

Задание

Определить значения r и s при условии, чтобы $e_1 \cdot r - e_2 \cdot s = 1$, используя расширенный алгоритм Евклида.

Используя полученные выше значения r и s , записать исходный текст.

Исходные данные

Вариант 3:

$N = 445632735571$

$e_1 = 1120289$

$e_2 = 559633$

$C_1 =$ 348555354398 351363944134 96907337112 141119651255 317600466893
84967944527 340088880266 311235549494 41838603784 333172824695 89494655477
3256803669

$C_2 =$ 366337925832 29318249989 120058862823 428190500861 322426909958
286841513079 150392378882 441874945028 297137742269 304115257300
123106598046 110955623263

Ход работы

Шаг 1. Решение уравнения

Решаем уравнение $e_1 \cdot r - e_2 \cdot s = \pm 1$: для этого помещаем в поле A, B, C значения e_1 , e_2 и N соответственно.

В результате, в поле C будет храниться значение s , а в поле D -- значение r .

Результат первого шага: $s = 64611$, $r = 32276$ (см. рис. 1).

A		AD - BC = 1
1120289	e1	1120289
B	e2	559633
559633	N	445632735571
C		
64611	s	64611
D	r	32276
32276		

Рисунок 1. Шаг 1.

Шаг 2. Дешифрование зашифрованного текста.

Для дешифрации: каждый блок s_1 возводим в степень r , а каждый блок s_2 – в степень $(-s)$ по модулю N .
После, значения перемножаются по модулю N и этот результат приводится к тексту. На рисунке 2 представлено дешифрование первого блока:

3488542975		AD - BC = 1
B	N	445632735571
1	e1	1120289
C	e2	559633
445632735571		
D	s	64611
Поря	r	32276
D = A + B	c1_1	348555354398
D = A^B mod C	c2_1	366337925832
D = text(A)	c1_1^r	269103635128
D -> A	c2_1^(-s)	228476133539
D = A * B	c*d	61483758075335259357992
D = A^(1 / B)	mod N	3488542975
D = number(A)	m1	"Поря"
D -> table		
D = A div B		
A*D - B*C = N		
Increase number of rows		
D = A mod C		

Рисунок 2. Дешифрация первого блока.

На рисунке 3 представлено дешифрование всего текста:

3774014955		AD - BC = 1
B	N	445632735571
298611707106	e1	1120289
C	e2	559633
445632735571		
D	s	64611
ател	r	32276
D = A + B	m1	"Поря"
D = A^B mod C	m2	"дков"
D = text(A)	m3	"ые н"
D -> A	m4	"омер"
D = A * B	m5	"а со"
D = A^(1 / B)	m6	"отве"
D = number(A)	m7	"тств"
D -> table	m8	"уют "
D = A div B	m9	"посл"
A*D - B*C = N	m10	"едов"
Increase number of rows	m11	"ател"
D = A mod C	m12	"ьно "

Рисунок 3. Дешифрование закодированного текста.

Результат

В результате была получена фраза: "Порядковые номера соответствуют последовательно"

Вывод

В ходе данной лабораторной работы был изучен метод атаки на алгоритм шифрования RSA посредством метода бесключевого чтения.