

Национальный исследовательский университет ИТМО
Факультет Программной Инженерии и Компьютерной Техники

Вариант №26
Лабораторная работа №2.3
«Атака на алгоритм шифрования RSA методом
бесключевого чтения»
По дисциплине:
«Информационная безопасность»

Работу выполнила:
Студентка группы Р34102
Никонова Наталья Игоревна
Преподаватель:
Рыбаков Степан Дмитриевич

Санкт-Петербург

2023

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

Вариант

№	N	E1	E2	C1	C2
26	199463062753	419513	830477	177528135337 131197957980 181321285074 96738779356 127632416974 161779284378 148599198368 2033602084 141914496373 105405878640 120038779975 7139491789	63508097139 142467940607 131649552179 182684157712 22912524157 94825501208 189716623763 86236434624 94875774697 120252092430 26215384541 53782670605

Выполнение

1. Решение уравнения $e_1 * r - e_2 * s = \pm 1$

The screenshot shows the BCalc application window. On the left, there are input fields for A, B, and C, and a result field D. Below these are several buttons for mathematical operations. On the right, a table displays the steps of the extended Euclidean algorithm:

	AD - BC = 1
e1	419513
e2	830477
r	218475
s	110362

2. Возводим $c1[0]$ в степень r по модулю N , а $c2[0]$ – в степень $(-s)$ по модулю N .

BCalc

A	63508097139
B	-110362
C	199463062753
D	145094947478

D = A + B

D = A^B mod C

D = text(A)

D -> A

D = A * B

D = A^(1 / B)

D = number(A)

D -> table

D = A div B

A*D · B^C = N

Increase number of rows

	AD - BC = 1
e1	419513
e2	830477
r	218475
s	110362
c1	177528135337
c2	63508097139
c1^r	1093710883
c2^(-s)	145094947478
N	199463062753

Перемножаем полученные значения

BCalc

A	1093710883
B	111599966245
C	0
D	122058097624589144335

D = A + B

D = A^B mod C

D = text(A)

D -> A

D = A * B

D = A^(1 / B)

D = number(A)

D -> table

D = A div B

A*D · B^C = N

Increase number of rows

D = A mod C

	AD - BC = 1
e1	419513
e2	830477
r	218475
s	110362
c1	177528135337
c2	63508097139
c1^r	1093710883
c2^(-s)	111599966245
N	199463062753
c1^r*c2^(s)	122058097624589144335

Берем модуль

BCalc

A	158691923125002003074
B	0
C	199463062753
D	3975081454

D = A + B

D = A^B mod C

D = text(A)

D -> A

D = A * B

D = A^(1 / B)

D = number(A)

D -> table

D = A div B

A*D · B^C = N

Increase number of rows

D = A mod C

	AD - BC = 1
e1	419513
e2	830477
r	218475
s	110362
c1	177528135337
c2	63508097139
c1^r	1093710883
c2^(-s)	145094947478
N	199463062753
c1^r*c2^(s)	158691923125002003074
mod N	3975081454

Расшифровываем значение

A	3975081454	AD - BC = 1
B	0	e1 419513
C	0	e2 830477
D	0	r 218475
МОНО		s 110362
D = A + B	D = A^B mod C	c1 177528135337
D = A * B	D = A^(1 / B)	c2 63508097139
D = A div B	A*D - B*C = N	c1^r 1093710883
D = A mod C	Increase number of rows	c2^(-s) 145094947478
		N 199463062753
		c1^r*c2^(s) 158691923125002003074
		mod N 3975081454
		text МОНО

3. Текст получился не битый – все высчитано верно и можно продолжать расшифровывать текст

c1	131197957980	c1	161779284378
c2	142467940607	c2	94825501208
c1^r	53544889324	c1^r	134488296193
c2^(-s)	9162749179	c2^(-s)	146399457422
*	490618390693126864996	*	19689013592264428194446
mod N	4025412604	mod N	552527085
text	поль	text	одн
c1	181321285074	c1	148599198368
c2	131649552179	c2	189716623763
c1^r	125925619509	c1^r	84685337907
c2^(-s)	91326209934	c2^(-s)	40162803630
*	11500309563347940002406	*	3401200596699036202410
mod N	3991806183	mod N	3760253159
text	но з	text	а из
c1	96738779356	c1	2033602084
c2	182684157712	c2	86236434624
c1^r	194343675467	c1^r	75916506396
c2^(-s)	55328911260	c2^(-s)	179642871635
*	10752823973855882058420	*	13637859213474284477460
mod N	3774210784	mod N	552727264
text	ахва	text	ста
c1	127632416974	c1	141914496373
c2	22912524157	c2	94875774697
c1^r	124029759789	c1^r	116443442636
c2^(-s)	149794311078	c2^(-s)	61777863558
*	18578952420763081642542	*	7193627111390607858888
mod N	4075352828	mod N	3992381673
text	ТИТЬ	text	нций

c1	105405878640
c2	120252092430
c1^r	18429026961
c2^(-s)	57260719857
*	1055259350050921064577
mod N	740356078
text	, no
c1	120038779975
c2	26215384541
c1^r	121704007889
c2^(-s)	44117095228
*	5369227305668276253692
mod N	4059229951
text	стоя
c1	7139491789
c2	53782670605
c1^r	66208570704
c2^(-s)	84135096222
*	5570464466902130280288
mod N	3991793184
text	нно

Итоговая расшифрованная фраза: монополюно захватить одна из станций, постоянно

Вывод

В ходе выполнения лабораторной работы я познакомилась с очередным методом атаки на шифр RSA. Этот экземпляр оказался достаточно простым, без неизвестно заранее количества возведений в степень как во втором способе и без подбора значений. Но вначале необходимо решить уравнение через расширенный алгоритм Евклида для двух взаимно простых чисел (потому что $\text{НОД} = 1$), а его реализация рекурсивна и неизвестна сложность.

