

Отчет по лабораторной работе
“Атака на алгоритм шифрования RSA посредством метода Ферма”
по дисциплине
“Информационная безопасность”
Вариант 4

Выполнил:
студент группы Р34131
Бусыгин Дмитрий Алексеевич
Преподаватель:
Маркина Татьяна Анатольевна

Санкт-Петербург
2024

Цель работы.....	3
Вариант.....	3
Выполнение в программе BCalc.exe.....	3
Результат работы программы BCalc.exe.....	4

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством метода Ферма.

Вариант

№	Модуль, N	Экспонента, e	Блок зашифрованного текста, C
4	89318473363897	2227661	3403106899606 26746900101177 67769260919924 77873792354218 15782947730235 15100267747684 28877721728826 62898555111378 4989704651236 55293402838380 4108112294245 8492269964172

Выполнение в программе BCalc.exe

1. Вычисляем $n = [\sqrt{N}] + 1$. Получаем число **9450846**, но в первой строке таблицы видим сообщение «[error]». Это свидетельствует о том, что N не является квадратом целого числа.

2. $t1 = n + 1$. Возводим число t1 в квадрат: $t1^2 = 89318509017409$.

Вычисляем $w1 = t1^2 - N = 35653512$. Проверяем, является ли w1 квадратом целого числа: A:= w1, B:= 2, нажимаем « $D = A^{(1/B)}$ » => в первой строке таблицы появляется сообщение «[error]», следовательно проделываем п. 2 заново с $t2 = n + 2$ и так далее, пока не найдем, что некоторое wi является квадратом целого числа.

3. При вычислении квадратного корня w5 первая строка таблицы остается пустой, а $D = \sqrt{w5} = 10548$, что свидетельствует об успехе факторизации. $t5 = 9450851$.

4. Вычисляем $p = t5 + \sqrt{w5} = 9461399$ и $q = t5 - \sqrt{w5} = 9440303$.

Вычисляем $\Phi(N) = (p - 1)(q - 1) = 89318454462196$. Вычисляем d, как обратный к e: A:= e, B:= -1, C:= $\Phi(N)$, нажимаем « $D = A^B \bmod C$ » => $D = d = 15910526683025$.

5. Производим дешифрацию шифрблока, полученное из 12 блоков сообщение: *одномаршрутный (single route) и всемаршрутный (a*

Результат работы программы BCalc.exe

Исходные данные и расчет

BCalc

A
3911198817

B
15910526683025

C
89318473363897

D
й (a

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

Clear D

Clear A, B, C

Clear grid

N	89318473363897
n=sqrt (N)	9450846
t1	9450847
t1^2	89318509017409
w1	35653512
t2	9450848
t2^2	89318527919104
w2	54555207
t3	9450849
t3^2	89318546820801
w3	73456904
t4	9450850
t4^2	89318565722500
w4	92358603
t5	9450851
t5^2	89318584624201
w5	111260304
sqrt (w5)	10548
p	9461399
q	9440303
phi (N)	89318454462196
e	2227661
d	15910526683025
block1	3403106899606

Дешифрация сообщения

BCalc

A
3911198817

B
15910526683025

C
89318473363897

D
й (a

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

Clear D

Clear A, B, C

Clear grid

block1	3403106899606
msg1	4007980526
decr1	одно
block2	26746900101177
msg1	3974164728
decr2	марш
block3	67769260919924
msg3	4042519277
decr3	руть
block4	77873792354218
msg4	4226359336
decr4	ый (
block5	15782947730235
msg5	1936289383
decr5	sing
block6	15100267747684
msg6	1818566770
decr6	le r
block7	28877721728826
msg7	1869968485
decr7	oute
block8	62898555111378
msg8	690022432
decr8) и

BCalc

A
3911198817
B
15910526683025
C
89318473363897
D
й а

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			

Clear D	
Clear A, B, C	
Clear grid	

block6	15100267747684
msg6	1818566770
decr6	le r
block7	28877721728826
msg7	1869968485
decr7	oute
block8	62896555111378
msg8	690022432
decr8) и
block9	4989704651236
msg9	3807503852
decr9	всем
block10	55293402838380
msg10	3773888752
decr10	аршр
block11	4108112294245
msg11	4092784123
decr11	утны
block12	8492269964172
msg12	3911198817
decr12	й а