

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

Лабораторная работа №6

по дисциплине “Информационная безопасность”

**на тему “Атака на алгоритм шифрования RSA,
основанная на Китайской теореме об остатках”**

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 китайской теореме об остатках.

Задание

Используя Китайскую теорему об остатках, получить исходный текст;

Исходные данные

Вариант 3:

$e = 3$

$N_1 = 380077454101$

$N_2 = 380903460337$

$N_3 = 383306345689$

$C_1 = 120321295984 \ 116941070964 \ 156315192664 \ 260149644765 \ 357688967002$
 $165841867143 \ 349826484990 \ 337993834720 \ 117681826230 \ 36279369135 \ 124613350713$
 106958422772

$C_2 = 261990433834 \ 232071459327 \ 305414687540 \ 348455852917 \ 206680974925$
 $327578130329 \ 5548686870 \ 295985428633 \ 157420509616 \ 256913681356 \ 271869775627$
 310864218021

$C_3 = 322305651846 \ 286065905390 \ 188633713225 \ 131649116365 \ 253206684415$
 $46677871611 \ 65268441973 \ 317133281785 \ 52226297600 \ 255637668770 \ 201873507225$
 260192105953

Ход работы

Шаг 1.

Необходимо вычислить значения:

$$M_0 = N_1 * N_2 * N_3$$

$$m_1 = N_2 * N_3$$

$$m_2 = N_1 * N_3$$

$$m_3 = N_1 * N_2$$

$$n_1 = m_1^{-1} \bmod N_1$$

$$n_2 = m_2^{-1} \bmod N_2$$

$$n_3 = m_3^{-1} \bmod N_3$$

Результаты вычислений представлены на рисунке 1.

144772817463148191492037	AD - BC = 0
B	N1 380077454101
-1	N2 380903460337
C	N3 383306345689
383306345689	C1_1 120321295984
D	C2_2 261990433834
307247910922	C3_3 322305651846
<div> <div>D = A + B</div> <div>D = A^B mod C</div> <div>D = text(A)</div> <div>D -> A</div> </div>	M0 55492339616899976706281903012778493
<div> <div>D = A * B</div> <div>D = A^(1 / B)</div> <div>D = number(A)</div> <div>D -> table</div> </div>	m1 146002713442070422437193
<div> <div>D = A div B</div> <div>A*D - B*C = N</div> <div>Increase number of rows</div> </div>	m2 145686100010232936720589
<div> <div>D = A mod C</div> </div>	m3 144772817463148191492037
	n1 16043866453
	n2 59502902859
	n3 307247910922

Рисунок 1. Шаг 1 - расчет констант

Шаг 2.

Для каждого блока итеративно необходимо рассчитать значение S и M

$$S = c_{1,i} * n_1 * m_1 + c_{2,i} * n_2 * m_2 + c_{3,i} * n_3 * m_3$$

$$M_i = (S \bmod M_0)^{(1/e)}$$

Значение M хранит зашифрованный текст.

На рисунке 2 представлено итеративное декодирование закодированной фразы.

552460320			
B			
3			
C			
55492339616899976706281903012778493			
D			
на			

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

s1	16889499538699926544411123976828906728723
s1 mod M0	34548441260528085004022336000
M1	3256937960 => "В ни"
s2	15010236107837547426158186286751107492572
s2 mod m0	58156296940615221797975270009
M2	3874350569 => "жней"
s3	11404366209704341061964436591889554756513
M3	553115889 => " час"
s4	94859657852126019884686686227882495684881
M4	4075299052 => "ти м"
s5	13892456091117370070357268990791111418055
M5	4007978475 => "одел"
s6	53044527252961864007616560244578645203858
M6	3894431571 => "и OS"
s7	37707655976740083014255686018199839260117
M7	824242144 => "1 па"
s8	17464007173500793331615832919633025499461
M8	3940938491 => "кеты"
s9	39633875074275621982290438263789728387586
M9	552657127 => " раз"
s10	13683158344862560401924617484116582478298
M10	3790136032 => "бива"
s11	11628235182385645483814516344910454903276
M11	4277334527 => "ются"
s12	14518990430472673995684137784376144503722
M12	552460320 => " на "

s1	16889499538699926544411123976828906728723
s1 mod M0	34548441260528085004022336000
M1	3256937960 => "В ни"
s2	15010236107837547426158186286751107492572
s2 mod m0	58156296940615221797975270009
M2	3874350569 => "жней"
s3	11404366209704341061964436591889554756513
M3	553115889 => " час"
s4	94859657852126019884686686227882495684881
M4	4075299052 => "ти м"
s5	13892456091117370070357268990791111418055
M5	4007978475 => "одел"
s6	53044527252961864007616560244578645203858
M6	3894431571 => "и OS"
s7	37707655976740083014255686018199839260117
M7	824242144 => "1 па"
s8	17464007173500793331615832919633025499461
M8	3940938491 => "кеты"
s9	39633875074275621982290438263789728387586
M9	552657127 => " раз"
s10	13683158344862560401924617484116582478298
M10	3790136032 => "быва"
s11	11628235182385645483814516344910454903276
M11	4277334527 => "ются"
s12	14518990430472673995684137784376144503722
M12	552460320 => " на "

Рисунок 2. Декодирование закодированной фразы

Результат

Была получена фраза “В нижней части модели OSI пакеты разбиваются на ”

Вывод

В ходе выполнения лабораторной работы была изучена атака на алгоритм шифрования RSA посредством китайской теореме об остатках.