

УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

Направление подготовки 09.03.04 Программная инженерия

Лабораторная работа №2.4

Дисциплина «Информационная безопасность»

Вариант 13

Выполнил: студент группы Р34131

Кузнецов Максим Александрович

Преподаватель:

Маркина Татьяна Анатольевна

Санкт-Петербург, 2023 г.

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством Китайской теоремы об остатках.

Задание

Вариант	Модуль, N			Блоки зашифрованного текста		
	N_1	N_2	N_3	C_1	C_2	C_3
13	483603920323	484627023409	486046777033	45854580612 105237269523 169259415669 93616181002 111788215636 19646301574 344814513220 284120677804 135039654745 8393533606 277869220393 95747282494 31789892340	274960963762 445004609734 314321127441 121008447611 77289255193 185428067959 268033072619 483476916533 378663280169 145768361237 164058939780 427513468440 16789037076	245417628800 58500957429 337297880630 192371047425 368079140170 444426125103 485088147460 384977923665 52336096116 217360431271 261094805307 77329919173 280539607542

Экспонента для всех вариантов $e = 3$;

Ход работы

1. Вычисляем $M_0 = N_1 * N_2 * N_3$
2. Вычисляем $m_1 = N_2 * N_3$
3. Вычисляем $m_2 = N_1 * N_3$
4. Вычисляем $m_3 = N_1 * N_2$
5. Вычисляем $n_1 = m_1^{-1} \bmod N_1$
6. Вычисляем $n_2 = m_2^{-1} \bmod N_2$
7. Вычисляем $n_3 = m_3^{-1} \bmod N_3$
8. Вычисляем $S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3$
9. Вычисляем $M = (S \bmod M_0)^{\frac{1}{3}}$
10. Преобразуем в текст полученное число
11. Повторяем шаги 8-10 для каждой строки и получаем итоговый текст.

Для решения задачи была разработана программа на Python.

Листинг разработанной программы

```
N1 = 483603920323
N2 = 484627023409
N3 = 486046777033
```

```
C1 = '''
45854580612
105237269523
169259415669
93616181002
111788215636
19646301574
344814513220
284120677804
135039654745
8393533606
277869220393
95747282494
31789892340
'''
```

```
C2 = '''
274960963762
445004609734
314321127441
121008447611
77289255193
185428067959
268033072619
483476916533
378663280169
145768361237
164058939780
427513468440
16789037076
'''
```

```
C3 = '''
245417628800
58500957429
337297880630
```

```

192371047425
368079140170
444426125103
485088147460
384977923665
52336096116
217360431271
261094805307
77329919173
280539607542
'''

c_1 = list(map(int, C1.split()))
c_2 = list(map(int, C2.split()))
c_3 = list(map(int, C3.split()))

M_0 = N1 * N2 * N3
print(f"1. Шаг первый: Вычисляем M_0 = N1 * N2 * N3 = {M_0}")
m_1 = N2 * N3
print(f"2. Шаг второй: Вычисляем m_1 = N2 * N3 = {m_1}")
m_2 = N1 * N3
print(f"3. Шаг третий: Вычисляем m_2 = N1 * N3 = {m_2}")
m_3 = N1 * N2
print(f"4. Шаг четвертый: Вычисляем m_3 = N1 * N2 = {m_3}")
n_1 = pow(m_1, -1, N1)
print(f"5. Шаг пятый: Вычисляем n_1 = (n_1)^-1 mod N1 = {n_1}")
n_2 = pow(m_2, -1, N2)
print(f"6. Шаг шестой: Вычисляем n_2 = (n_2)^-1 mod N2 = {n_2}")
n_3 = pow(m_3, -1, N3)
print(f"7. Шаг седьмой: Вычисляем n_3 = (n_3)^-1 mod N3 = {n_3}")

output = ""

for i in range(len(c_1)):
    S = (c_1[i] * n_1 * m_1) + (c_2[i] * n_2 * m_2) + (c_3[i] * n_3 *
m_3)
    print(f"8. Шаг восьмой: Вычисляем S = c_1 * n_1 * m_1 + c_2 * n_2
* m_2 + c_3 * n_3 * m_3= {S}")
    M = round((S % M_0) ** (1 / 3))
    print(f"9. Шаг девятый: Вычисляем M = (S mod M_0)^(1/3) = {M}")
    msg = M.to_bytes(4, byteorder='big').decode('cp1251')
    print(f"10. Шаг десятый: Преобразуем M в текст = {msg}")
    output += msg

print(f"11. Шаг одиннадцатый: итоговый текст -->{output}")

```

Ссылка на программу: [ссылка](#)

Результат работы программы:

```
1. Шаг первый: Вычисляем  $M_0 = N_1 * N_2 * N_3 = 113913581827329323872903190292895531$ 
2. Шаг второй: Вычисляем  $m_1 = N_2 * N_3 = 235551402791040694565497$ 
3. Шаг третий: Вычисляем  $m_2 = N_1 * N_3 = 235054126833517878341659$ 
4. Шаг четвертый: Вычисляем  $m_3 = N_1 * N_2 = 234367528415058691841107$ 
5. Шаг пятый: Вычисляем  $n_1 = (n_1)^{-1} \bmod N_1 = 397183092488$ 
6. Шаг шестой: Вычисляем  $n_2 = (n_2)^{-1} \bmod N_2 = 25306047792$ 
7. Шаг седьмой: Вычисляем  $n_3 = (n_3)^{-1} \bmod N_3 = 61477186524$ 
8. Шаг восьмой: Вычисляем  $S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3 = 9461606488385560063080307974941720471191061568$ 
9. Шаг девятый: Вычисляем  $M = (S \bmod M_0)^{(1/3)} = 3236815083$ 
10. Шаг десятый: Преобразуем M в текст = Анал
8. Шаг восьмой: Вычисляем  $S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3 = 13335600552596321037493467716387716864076042652$ 
9. Шаг девятый: Вычисляем  $M = (S \bmod M_0)^{(1/3)} = 3907510514$ 
10. Шаг десятый: Преобразуем M в текст = изат
8. Шаг восьмой: Вычисляем  $S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3 = 22564956831317203589019812413050619874657946672$ 
9. Шаг девятый: Вычисляем  $M = (S \bmod M_0)^{(1/3)} = 4008770336$ 
10. Шаг десятый: Преобразуем M в текст = оры
8. Шаг восьмой: Вычисляем  $S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3 = 12249977089278485252472980909944879876716672980$ 
9. Шаг девятый: Вычисляем  $M = (S \bmod M_0)^{(1/3)} = 4025544434$ 
10. Шаг десятый: Преобразуем M в текст = прот
8. Шаг восьмой: Вычисляем  $S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3 = 16221691512077024882604659412504592282936605560$ 
9. Шаг девятый: Вычисляем  $M = (S \bmod M_0)^{(1/3)} = 4008373995$ 
10. Шаг десятый: Преобразуем M в текст = окол
8. Шаг восьмой: Вычисляем  $S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3 = 9344435316783047923657683853241266273926900620$ 
9. Шаг девятый: Вычисляем  $M = (S \bmod M_0)^{(1/3)} = 4007796976$ 
10. Шаг десятый: Преобразуем M в текст = ов р
8. Шаг восьмой: Вычисляем  $S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3 = 40843436385936807701252956142866415143127097632$ 
9. Шаг девятый: Вычисляем  $M = (S \bmod M_0)^{(1/3)} = 3773296869$ 
10. Шаг десятый: Преобразуем M в текст = азре
8. Шаг восьмой: Вычисляем  $S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3 = 35004210037976830754973558723020259707179806788$ 
9. Шаг девятый: Вычисляем  $M = (S \bmod M_0)^{(1/3)} = 4175494898$ 
10. Шаг десятый: Преобразуем M в текст = шакот
8. Шаг восьмой: Вычисляем  $S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3 = 15640380904970277016913957181912135235996672040$ 
9. Шаг девятый: Вычисляем  $M = (S \bmod M_0)^{(1/3)} = 552137201$ 
10. Шаг десятый: Преобразуем M в текст = исс
8. Шаг восьмой: Вычисляем  $S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3 = 4784131534905751753048886107979988760101407180$ 
9. Шаг девятый: Вычисляем  $M = (S \bmod M_0)^{(1/3)} = 3957712110$ 
10. Шаг десятый: Преобразуем M в текст = ледо
8. Шаг восьмой: Вычисляем  $S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3 = 30734411439208665233014149917415886834292179364$ 
9. Шаг девятый: Вычисляем  $M = (S \bmod M_0)^{(1/3)} = 3806393084$ 
10. Шаг десятый: Преобразуем M в текст = вать
8. Шаг восьмой: Вычисляем  $S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3 = 12614995615907325978567577799998012475046622868$ 
9. Шаг девятый: Вычисляем  $M = (S \bmod M_0)^{(1/3)} = 552083694$ 
10. Шаг десятый: Преобразуем M в текст = и о
8. Шаг восьмой: Вычисляем  $S = c_1 * n_1 * m_1 + c_2 * n_2 * m_2 + c_3 * n_3 * m_3 = 7116120691603481600862145081499351356720233624$ 
9. Шаг девятый: Вычисляем  $M = (S \bmod M_0)^{(1/3)} = 3790413856$ 
10. Шаг десятый: Преобразуем M в текст = он
11. Шаг одиннадцатый: итоговый текст -->Анализаторы протоколов разрешают исследовать и обн
```

Итоговый текст: Анализаторы протоколов разрешают исследовать и обн

Вывод

В ходе выполнения данной лабораторной работы я:

- ознакомился с методом для атаки на алгоритм шифрования RSA, основанном на Китайской теореме об остатках.
- Реализовал данный метод на языке Python.