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 P34131**

*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 | | | | |
|  |  |  |  |  | |  | |
| 13 | 483603920323 | 484627023409 | 486046777033 | 373852443734 447989059513 140756140384 207791711792 252160015422 151272799305 431450717984 252882800366 112417596471 301753741810 480461056512 334158277030 368394150653 | | 22286870422 343015689591 281801228231 360270382562 264253306719 128520421967 399665129411 448878989738 70913527757 295285211952 247990966487 202711954425 201121363025 | | 22286870422 343015689591 281801228231 360270382562 264253306719 128520421967 399665129411 448878989738 70913527757 295285211952 247990966487 202711954425 201121363025 |

Экспонента для всех вариантов е = 3;

Ход работы

1. Вычисляем
2. Вычисляем
3. Вычисляем
4. Вычисляем
5. Вычисляем
6. Вычисляем
7. Вычисляем
8. Вычисляем
9. Вычисляем
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}")

Результат работы программы:

Изображение выглядит как текст, снимок экрана, меню, шаблон

Автоматически созданное описание

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.