УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

Направление подготовки 09.03.04 Программная инженерия

**Лабораторная работа №2.2**

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 повторного шифрования.

Задание

|  |  |  |  |
| --- | --- | --- | --- |
| Вариант | Модуль, N | Экспонента, е | Блок зашифрованного текста, C |
| 13 | 915012974539 | 1001953 | 763770087861 432343847598 764682728575 206635140312 627210520886 794063631890 309297959146 68118108284 116045398315 912085643674 257483784869 167814127445 55188158350 |

Ход работы

. Проделываем данное действие до тех пор, пока Как только получим , то это значит, что наш текст. И так для каждого зашифрованного фрагмента C.

Для решения задачи была разработана программа на Python.

Листинг разработанной программы

import math

import random

N = 915012974539

e = 1001953

C = '''

763770087861

432343847598

764682728575

206635140312

627210520886

794063631890

309297959146

68118108284

116045398315

912085643674

257483784869

167814127445

55188158350

'''

output = ""

for enc in list(map(int, C.split())):

y\_next = pow(enc, e, N)

enc\_msg = 0

while y\_next != enc:

enc\_msg = y\_next

y\_next = pow(y\_next, e, N)

msg = enc\_msg.to\_bytes(4, byteorder='big').decode('cp1251')

print(f"Оригинал: {enc}, полученный текст: {enc\_msg} -- {msg}")

output += msg

print(f"Итоговый текст -->{output}")

Результат работы программы:

Изображение выглядит как текст, снимок экрана, Шрифт, черно-белый

Автоматически созданное описание

Итоговый текст: устранения проблемы. Добавление микропроцессора, ОЗУ

Вывод

В ходе выполнения данной лабораторной работы я:

* ознакомился с методом повторного шифрования для атаки на алгоритм шифрования RSA.
* Реализовал данный метод на языке Python.