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

Факультет программной инженерии и компьютерной техники

Информационная безопасность

Лабораторная работа №2
Атака на алгоритм шифрования RSA методом повторного шифрования

Вариант 14

Студент: Мокров Семён Андреевич

P34121

Преподаватель: Маркина Татьяна Анатольевна

Санкт-Петербург 2023

Содержание

Цель работы

Изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

Задание

– ознакомьтесь с теорией в [3], рассмотренной в подразделе («Атака повторным шифрованием»);
– получите вариант задания у преподавателя;
– по полученным исходным данным, используя метод перешифрования, определите порядок числа e в конечном поле $Z_{\varphi(N)}$;
– используя значение порядка экспоненты, получите исходный текст методом перешифрования;
– результаты и промежуточные вычисления оформите в виде отчета.

Вариант задания

14	112546779899	280297	70526810403 14149862236 45856385641 70576010398 55035023176 13450029743 87602027501 5373321283 106271591904 105497609146 58279045288 104373761049 16432846070

Листинг разработанной программы

```
from termcolor import colored

source: str = '''
70526810403
14149862236
45856385641
70576010398
55035023176
13450029743
87602027501
5373321283
106271591904
105497609146
58279045288
104373761049
16432846070
'''

N: int = 112546779899
e: int = 280297

print(colored("Стартовые данные:", "green"))
print("Зашифрованная строка: " + source)
print("N: " + str(N))
print("e: " + str(e))

list_source = source.split()
result: str = ""

for i in range(len(list_source)):
    list_source[i] = int(list_source[i])

for y in list_source:
    y_i: int = pow(y, e, N)
    current_result: int = 0
```

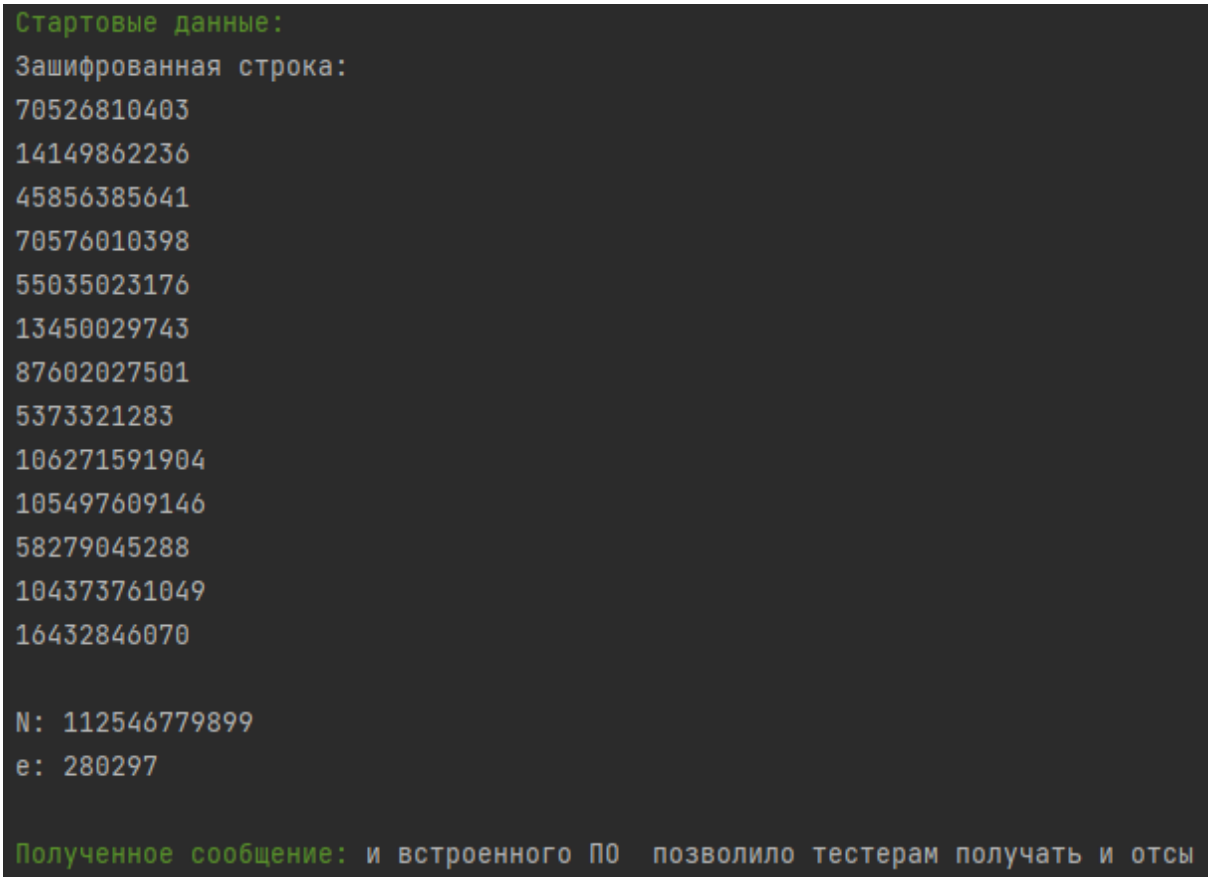
```
    while y_i != y:
        current_result = y_i
        y_i = pow(y_i, e, N)

    current_result_bytes = int.to_bytes(current_result, length=4, byteorder='big')
    result += current_result_bytes.decode('windows-1251')

print(colored("\nПолученное сообщение: ", "green") + result)
```

Исходный код

Исходный код расположен в репозитории:
https://github.com/semwett0301/information-security

Результаты работы программы

Скриншоты вывода программы



Полученное сообщение

и встроенного ПО позволило тестерам получать и отсы

Выводы

В данной лабораторной работе я:

- Ознакомился с принципом взлома RSA при помощи метода повторного шифрования
- Реализовал процесс взлома на Python