Университет ИТМО

Факультет ФПИ и КТ

Отчёт

по лабораторной работе 2.2

«Иформационная безопасность»

Вариант 7

Студент:

Ляо Ихун

Гр.P34131

Преподаватель:

Маркина Татьяна Анатольевна

Цель работы:

изучить атаку на алгоритм шифрования RSA посредством повторного шифрования.

Задача:

7	255886599799	1042193	75872140695 243623122014 66870731769 142602808011 42354989089 119395329034 242619634774 180213272917 166447493863 167768838568 120544075858 77559779546 136453339801

Выполнение:

```
N = 255886599799
e = 1042193
C = [
    75872140695,
    243623122014,
    66870731769,
    142602808011,
    42354989089,
    119395329034,
    242619634774,
    180213272917,
    166447493863,
    167768838568,
    120544075858,
    77559779546,
    136453339801
]


print(f"N = {N}")
print(f"e = {e}")
print(f"C = {C}")

for c in C:
    yi = pow(c, e, N)
    res = 0
    while yi != c:
        res = yi
        yi = pow(yi, e, N)
    print(res.to_bytes(4, byteorder='big').decode('cp1251'), end='')
```

Результат:

Вывод:

В ходе выполнения работы мы реализовали атаку на алгоритм шифрования RSA посредством повторного шифрования на языке python.