Министерство образования Республики Беларусь
Учреждение образования
“Брестский государственный технический университет”
Кафедра интеллектуально-информационных технологий

Лабораторная работа №3
“Атака на алгоритм шифрования RSA посредством метода бесключевого чтения”

Выполнил:
студент 4 курса
группы ИИ-22
Сидоренко А. А.
Проверила:
Хацкевич А. С.

Брест 2024

Цель работы: изучить атаку на алгоритм шифрования RSA посредством метода бесключевого чтения.

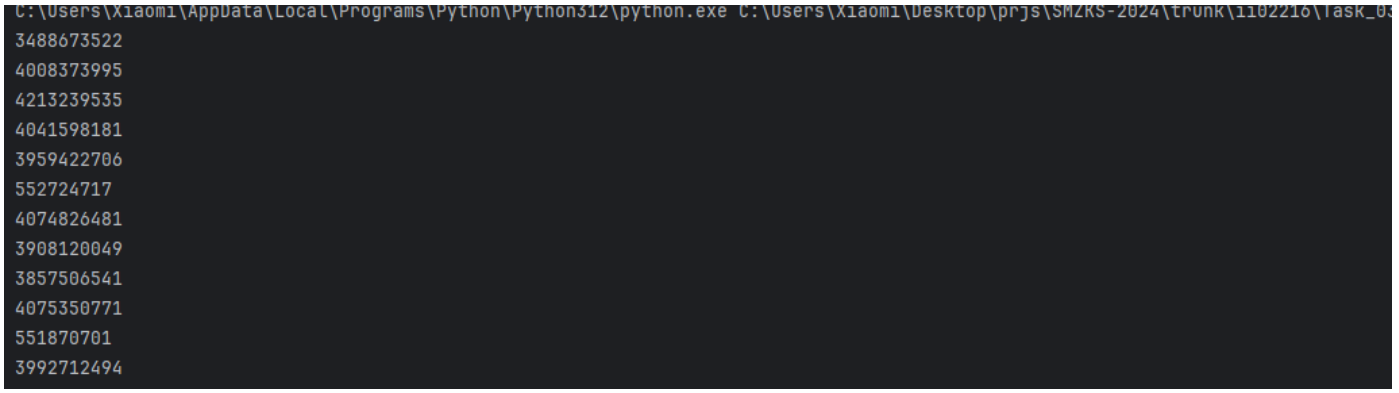
Ход работы:

- ознакомиться с теорией;
- по исходным данным определить значения r и s пр условии, что e1*r - e2*s = 1. Для этого необходимо использовать расширенный алгоритм Евклида;
- используя значения r и s, получить исходный текст;
- результаты и промежуточные вычисления значений для любых трех блоков шифрованного текста оформить в виде отчета.

Код программы:

```
def extended_gcd(a, b):
    x0, y0, x1, y1 = 1, 0, 0, 1
    while b != 0:
        q = a // b
        a, b = b, a % b
        x0, x1 = x1, x0 - q * x1
        y0, y1 = y1, y0 - q * y1

    return a, x0, y0


def main():
    N = 420882327013
    e1 = 1372369
    e2 = 961447
    c1 = [373413138774, 142492164990, 181970101695, 71400620884, 83588687662,
111752930680, 154836140461, 191336073909,
          186412386345, 303121580659, 167437105893, 279265271451]
    c2 = [105783140624, 384545054504, 91022339898, 266856044417, 106548952403,
160772152396, 128969469496, 242028887287,
          256618243529, 47586486979, 306022591934, 419219258598]

    gcd, r, s = extended_gcd(e1, e2)

    if gcd != 1:
        print("Error")
        return
    for i in range(len(c2)):
        K = pow(c1[i], r, N)
        B = pow(c2[i], -abs(s), N)
        T = (B * K) % N
        print(T)


if __name__ == "__main__":
    main()
```

Вывод программы:



Вывод: освоил на практике основные принципы атаки на RSA