Министерство образования Республики Беларусь

Учреждение образования

“Брестский государственный технический университет”

Кафедра интеллектуально-информационных технологий

Лабораторная работа №3
“Атака на алгоритм шифрования RSA”

По дисциплине “Современные методы защиты компьютерных систем”

Выполнила:
студентка 4 курса
группы ИИ-22
Леваневская Н.И.
Проверил:
Хацкевич А.С.

Брест-2024

Лабораторная работа 1

АТАКА НА АЛГОРИТМ ШИФРОВАНИЯ RSA ПОСРЕДСТВОМ МЕТОДА ФЕРМА

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

Ход работы:

– ознакомиться с теорией, изложенной в п. 1.2 («Взлом алгоритма RSA при неудачном выборе параметров криптосистемы»);

– получить вариант задания у преподавателя (табл. 1 приложения);

– используя разложение модуля на простые числа методом Ферма и полученные исходные данные, определить следующие показатели:

– множители модуля (p и q);

– значение функции Эйлера для данного модуля $\varphi(N)$;

– обратное значение экспоненты по модулю $\varphi(N)$;

– дешифровать зашифрованный текст, исходный текст должен быть фразой на русском языке;

– результаты и промежуточные вычисления оформить в виде отчета.

Ход работы:

Код программы:

```
from sympy import mod_inverse
from math import isqrt

def int_to_ascii(number):
    bin_str = bin(number)[2:]
    bytes_array = []
    for i in range(0, len(bin_str), 8):
        byte_str = bin_str[i:i + 8].zfill(8)
        byte = int(byte_str, 2)
        bytes_array.append(byte)

    ascii_chars = bytes(bytes_array).decode('windows-1251', errors='ignore')
    return ascii_chars


def main():
    N = 65815671868057
    e = 7423489
    C = 38932868535359

    n = isqrt(N) + 1

    i = 2
    D = 0
    while True:
        t = n + i
```

```
        w = pow(t, 2) - N
        D = isqrt(w)

        if D * D == w:
            break

        i += 1

    p = t + D
    q = t - D
    AB = (p - 1) * (q - 1)
    d = mod_inverse(e, AB)

    M = pow(C, d, N)
    text = int_to_ascii(M)

    print(f"Дешифрованное значение (M) = {M}")
    print(f"Дешифрованный текст: {text}")


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

Результат работы программы:

```
Дешифрованное значение (M) = 3402418120
Дешифрованный текст: КМЗИ
```

Вывод: Изучила атаку на алгоритм шифрования RSA посредством метода Ферма**.**