МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
“БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ”

Кафедра ИИТ

ОТЧЁТ
По лабораторной работе №3
«Атака на алгоритм шифрования RSA посредством метода Ферма»

Выполнил:
Студент группы ИИ-22
Гузаревич Д.А.
Проверил:
Хацкевич А.С.

2024

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

Ход работы

№	Модуль, N	Экспонента, e	Зашифрованный текст, C
19	59046883376179	4044583	3227910961209317838629182964416577671 6262130932846358952004865131300854626 4548325311280105374390354675332003643 4544911979279319283735645707989454955 1319569174668782

Код программы:

```
from math import ceil, isqrt

def find_p_q(N):
    x = ceil(isqrt(N))
    while True:
        y2 = x * x - N
        if y2 >= 0:
            y = isqrt(y2)
            if y * y == y2:
                break
        x += 1

    p = x - y
    q = x + y
    return p, q

def mod_inverse(e, phi):
    t, new_t = 0, 1
    r, new_r = phi, e
    while new_r != 0:
        quotient = r // new_r
        t, new_t = new_t, t - quotient * new_t
        r, new_r = new_r, r - quotient * new_r
    if r > 1:
        raise ValueError(f"e ({e}) и phi ({phi}) не взаимно просты!")
    if t < 0:
        t = t + phi
    return t


def main():
    N = 59046883376179
    e = 4044583
    C =
3227910961209317838629182964416577671626213093284635895200486513130085462645483253
1128010537439035467533200364345449119792793192837356457079894549551319569174668782

    p, q = find_p_q(N)
    fN = (p - 1)*(q - 1)
```

```
    d = mod_inverse(e, fN)
    print(f"p = {p}, q = {q}, phi_N = {fN}\nЗакрытый ключ d = {d}\n")

    message = pow(C, d, N)
    print(f"Исходное сообщение: {message}")

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

Результат работы:

```
p = 7675427, q = 7692977, phi_N = 59046868007776
Закрытый ключ d = 31944145322807

Исходное сообщение: 5328450707174
```

Вывод: изучил атаку на алгоритм шифрования RSA посредством метода Ферма