Презентация по лабораторной работе №6

Математические основы защиты информации и информационной безопасности

Быстров Г. А.

20 ноября 2024

Российский университет дружбы народов, Москва, Россия

Цели и задачи

- Получить понимание как раскладывать числа на множители.
- Реализовать алгоритм p-метода Полларда
- Реализовать метод квадратов (Теорема Ферма о разложении)

Выполнение лабораторной работы

1. Реализовал алгоритм p-метода Полларда (рис. 1).

```python
from math import gcd

def calc(x, mod):
    return (x**2 + 7) % mod

def pollard(n):
    x = 2
    y = 2
    d = 1

    while d == 1:
        x = calc(x, n)
        y = calc(calc(y, n), n)
        d = gcd(abs(x - y), n)

    if d == n:
        print("Делитель не найден")
        return None
    else:
        return d

number = 1359331
divisor = pollard(number)
if divisor:
    print(f"Число {number} разлагается как {divisor} * {number // divisor}")
```

```
Число 1359331 разлагается как 1151 * 1181
```

Рис. 1: Код и вывод

Выполнение лабораторной работы

2. Реализовал метод квадратов (Теорема Ферма о разложении) (рис. 2).

```python
from math import isqrt

def ferma(n):
    if n % 2 == 0:
        print("Число должно быть нечетным")
        return None
    s = isqrt(n) + 1
    squared = s**2 - n

    while not perfect_square(squared):
        s += 1
        squared = s**2 - n

    t = isqrt(squared)
    p = s - t
    q = s + t
    return p, q

def perfect_square(x):
    if x < 0:
        return False
    sqrt_x = isqrt(x)
    return sqrt_x**2 == x

number = 1359331
factors = ferma(number)

if factors:
    print(f"Число {number} разлагается как {factors[0]} * {factors[1]}")
```

```
Число 1359331 разлагается как 1151 * 1181
```

Результаты

Успешно удалось получить понимание как раскладывать числа на множители. Реализовал на практике алгоритм p-метода Полларда и метод квадратов (Теорема Ферма о разложении).