

Информационная безопасность. Лабораторная работа № 6 на тему “Разложение чисел на множители”

Мухамеджанов Исматулло Иззатуллоевич

RUDN University, Moscow, Russian Federation

Содержание

- Цели и задачи
- Выполнение
- Результаты
- Список литературы

Цели и задачи

Освоить на практике применение шифров на основе замены

Выполнение

Метод Полларда

```
import math

def pollard_method(n, c):
    a = c
    b = c
    d = 1
    f = lambda x: (x**2 + 5) % n
    while d == 1:
        a = f(a)
        b = f(f(b))
        d = math.gcd(abs(a - b), n)

    if d == n:
        return "Division not found"
    else:
        return d

pollard_method(1359331, 1)
```

[18] Python

... 1181

Figure 1: Программа (1)

Факторизация Числа

```
def factors(n):
    k = round(math.sqrt(n))
    number_list = []
    for i in range(k, n+1):
        if n % i == 0:
            number_list.append(i)

    for j in number_list:
        print(f"{n} = {j}*{n//j}", end=" , откуда ")
        res = (j + n//j) // 2
        res_2 = int(math.sqrt(res**2 - n))
        print(f"s={res}, t={res_2} и {n}={res}^2-{res_2}^2")

factors(65)
```

[38]

Python

... 65 = 13*5, откуда s=9, t=4 и $65=9^2-4^2$
65 = 65*1, откуда s=33, t=32 и $65=33^2-32^2$

Figure 2: Программа (2)

Результаты

Освоены методы разложения чисел на множители

Список литературы

1. Методические материалы курса