Лабораторная работа №6

Разложение чисел на множители

Кубасов В.Ю.

Вводная часть

Актуальность

- Разложение чисел занимает достаточно много времени при условии используемых в шифровании порядков. Однако помимо перебора существуют алгоритмы, оптимизирующие данный процесс.

Цели и задачи

Реализовать алгоритмы:

- Алгоритм реализующий p-метод Полларда

Выполнение работы

Нахождение НОД по Евклиду:

```
function euklid(a, b)
    if (a == 0)
        return 1;
    end;
    ri_1 = a; ri = b; i = 1;
    while (true)
        riplus1 = ri_1 % ri;
        if (riplus1 == 0)
            break;
        end;
        ri_1 = ri;
        ri = riplus1;
    end;
    return ri;
```

Нахождение нетривиальног множителя

```
function pollard(n, c, func)
    a = c;
    b = c;
    while(true)
        a = func(a) % n;
        b = func(func(b) % n) % n;
        d = euklid(a - b, n);
        if (1 < d && d < n)
            return d;
        end;
        if (d == n)
            println("Делитель не найден");
            return -1;
        end;
```

Выводы:

Выводы:

- В ходе лабораторной работы реализовали вероятностные алгоритмы определения числа на простоту