ОТЧЕТ К ЛАБОРАТОРНОЙ РАБОТЕ № 7

Лабораторная работа № 7

Модель открытого текста

Вариант №4

Ф. И. О. студента: Гюнтер Тимофей Вячеславович

Группа: ФИТ-221

Проверил: Дата:

Основные сведения

Формулы вычисления последовательностей для параметров из варианта:

$a = 2, b = 18441, p = 30203; k = \left[\sqrt{p}\right] + 1 = 173 + 1 = 174$

$y_n = a^{n \cdot k}\ mod\ p = 2^{n \cdot 174} mod\ 30203$

$x_n = b \cdot a^n\ mod\ p = 18441 \cdot 2^n\ mod\ 30203$

Результаты

$$i = 58, j = 91$$

$$y_i = z_j = 19060$$

$$x = i \cdot k - j = 10001$$

Проверка по формуле $a^x = b\ mod\ p$:

$$2^{10001}\ mod\ 30203 = 18441$$

Код программы

```
from lab4 import binary_modular_power

from lab6 import integer_sqrt
```

```
# a^x ≡ b (mod p)

def babyStep_giantStep(a, b, p):
    '''
    Шаг младенца, шаг великана - алгоритм нахождения дискретного логарифма по модулю p.\n
    Нахождение x в выражении: `log_a(b) = x (mod p)`
    '''
    k = integer_sqrt(p)+1
    i = 1
    y = binary_modular_power(a, i*k, p)
    z = b*binary_modular_power(a, i, p) % p
    z_list = [z]
    y_list = [y]
    while not [v for v in z_list if v in y_list] :
        i += 1
        y = a**(i*k) % p
        z = b*a**i % p
        y_list.append(y)
        z_list.append(z)
    z_index = [i+1 for i in range(len(z_list)) if z_list[i] in y_list][0]
    y_index = [i+1 for i in range(len(y_list)) if y_list[i] in z_list][0]
```

```
    print(f'y_ind: {y_index}, k: {k}, z_ind: {z_index}, общий эл-т: {y_list[y_index-1]}')
    x = y_index*k - z_index


    return x


# print(babyStep_giantStep(2, 18441, 30203))


def babyStep_giantStep_interface():
    list_input = input('Введите последовательно через пробел соответствующие a, b и p (a^x ≡ b (mod p)):\n')
    a, b, p = map(int, list_input.split())
    x = babyStep_giantStep(a, b, p)
    print(f'Полученная степень x: {x}, проверка: b = {binary_modular_power(a, x, p)}')
# babyStep_giantStep_interface()
```