Министерство образования Республики Беларусь

Учреждение образования

«Брестский государственный технический университет»

Кафедра ИИТ

Лабораторная работа №6

По дисциплине «Теоретические интеллектуальные и информационные технологии»

Тема: «Одноключевая система шифрования Диффи и Хеллмана»

Выполнил:

Студент 1 курса

Группы ИИ-21(1)

Кирилович А.А.

Проверил:

Анфилец С. В.

Брест 2021

Цель: познакомиться с одноключеваой системой шифрования Диффи и Хеллмана.

**Ход работы:**

Код:

import random

a=5

p=9

q=set()

e=set()

for i in range(1, p):

    q.add(i)

    e.add((a\*\*i)%p)

while len(q)!=len(e):

    q=set()

    e=set()

    p+=1

    for i in range(1, p):

        q.add(i)

        e.add((a\*\*i)%p)

x\_i=random.randint(1, p-1)

y\_i=(a\*\*x\_i)%p

x\_j=random.randint(1, p-1)

y\_j=(a\*\*x\_j)%p

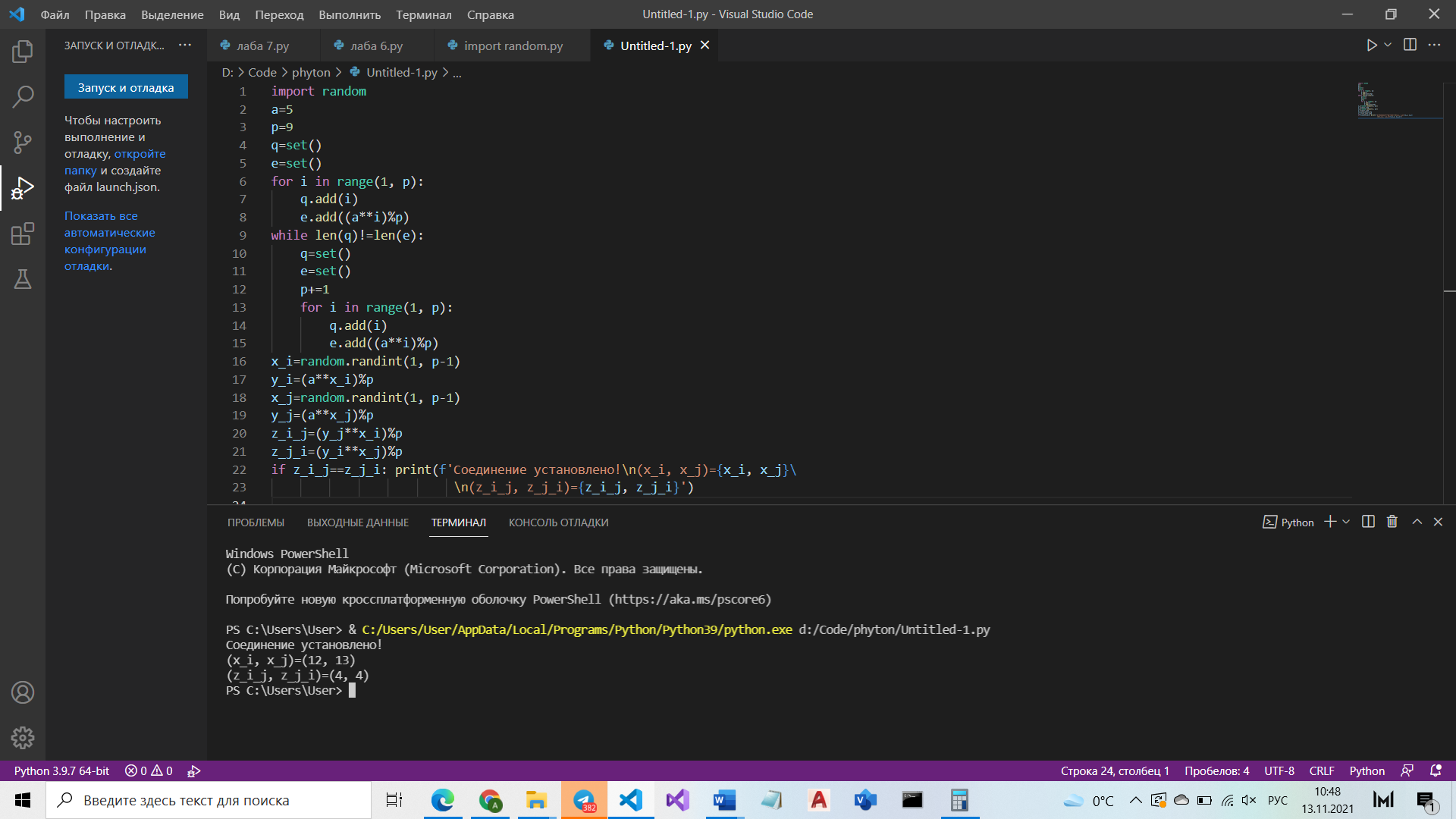
z\_i\_j=(y\_j\*\*x\_i)%p

z\_j\_i=(y\_i\*\*x\_j)%p

if z\_i\_j==z\_j\_i: print(f'Соединение установлено!\n(x\_i, x\_j)={x\_i, x\_j}\

                         \n(z\_i\_j, z\_j\_i)={z\_i\_j, z\_j\_i}')

Результат:



Вывод: Недостаток описанной криптосистемы с открытым распространением ключей состоит в том, что она требует абсолютного доверия партнеров по связи друг к другу, так как в этой одноключевой системе они могут изменять переданный текст. Поэтому она непригодна, например, для не доверяющих друг другу удаленных абонентов. В противном случае система довольно хороша.