Министерство образования Республики Беларусь

Учреждение образования

«Брестский государственный технический университет»

Кафедра ИИТ

Лабораторная работа №7

По дисциплине «Теоретические интеллектуальные и информационные технологии»

Тема: «Двухключевая система RSA»

Выполнил:

Студент 1 курса

Группы ИИ-21(1)

Кирилович А.А.

Проверил:

Анфилец С. В.

Брест 2021

**Цель работы:** Построить двухкючевую систему RSA

**Задание.** Построить двухключевую систему с использованием алгоритма RSA и выполнить в ней операцию шифрования и дешифрования трех первых букв фамилии студента (при количестве букв меньше 3, недостающие буквы берутся из имени). Пара простых чисел P и Q выбирается из диапазона ближайших к количеству букв в фамилии и имени студента.

Код программы:

import random

def gcf(a, b):

    while a != b:

        if a > b:

            a = a - b

        else:

            b = b - a

    return a

P=7

Q=11

N=P\*Q

L=(P-1)\*(Q-1)

D=random.randint(2,L-1)

while gcf(D, L)!=1:

    D=random.randint(2,L-1)

E=1

while (E\*D)%L!=1:

    E+=1

C1=(2\*\*E)%N

C2=(1\*\*E)%N

C3=(3\*\*E)%N

print(f'Зашифрованный тест: ({C1, C2, C3})')

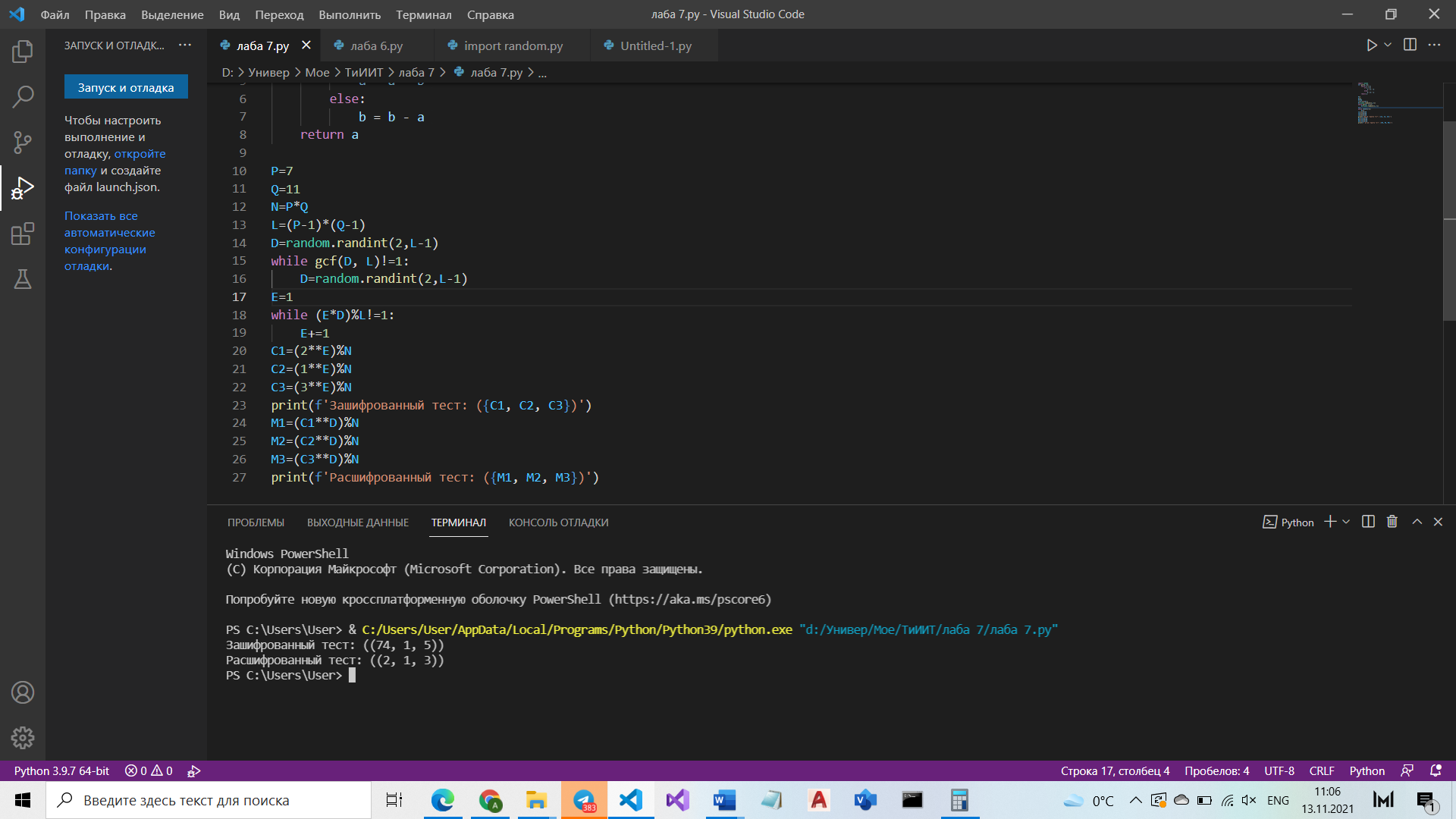
M1=(C1\*\*D)%N

M2=(C2\*\*D)%N

M3=(C3\*\*D)%N

print(f'Расшифрованный тест: ({M1, M2, M3})')

Результат:



**Вывод:** ознакомился с двухключевой системой шифрования RSA.