Министерство образования Республики Беларусь

Учреждение образования «Полоцкий государственный университет»

Кафедра вычислительных систем и сетей

ОТЧЕТ

о выполнении лабораторной работы № 1

на тему «Использование библиотеки OpenSSL»

Выполнил: Самохвал П. С.

студент группы 17-ВС

Проверила: Васильева Д.М.

Полоцк

2020

**Цель работы:** создание приложения, которое шифрует и дешифрует содержимое текстового файла, алгоритмом согласно варианту.

**Теоретические сведения:** OpenSSL - Эта свободно распространяемая библиотека предоставляет в распоряжение пользователя набор утилит, реализующих различные криптографические алгоритмы, такие как Triple-DES, Blowfish, AES, RSA и другие. Библиотека содержит набор функций, с помощью которых пользователь может разрабатывать собственные программы для криптографической защиты данных или создавать расширения, не входящие в стандартный набор. Большинство этих функций достаточно хорошо документированы, и наличие примеров программ значительно облегчает задачу изучения порядка их использования.

Для выполнения данной лабораторной работы был выбран симметричный алгоритм AES. Этот алгоритм преобразует один 128-битный блок в другой, используя секретный ключ, который нужен для такого преобразования. Для расшифровки полученного 128-битного блока используют второе преобразование с тем же секретным ключом.

В языке программирования Python для данного шифрования будет использоваться библиотека PyAesCrypt. Ниже представлен листинг кода программы.

**Листинг 1** – код программы.

import os

import pyAesCrypt

def crypt(dir):

    password = input("Введите пароль: ")

    bufferSize = 256 \* 1024

    pyAesCrypt.encryptFile(str(dir),str(dir)+".aes",password,bufferSize)

    print("file crypted")

def decrypt(dir):

    password = input("Введите пароль: ")

    bufferSize = 256 \* 1024

    pyAesCrypt.decryptFile(str(dir),str(os.path.splitext(dir)[0]),password,bufferSize)

    print("file decrypted")

dir = input("Введине имя файла: ")

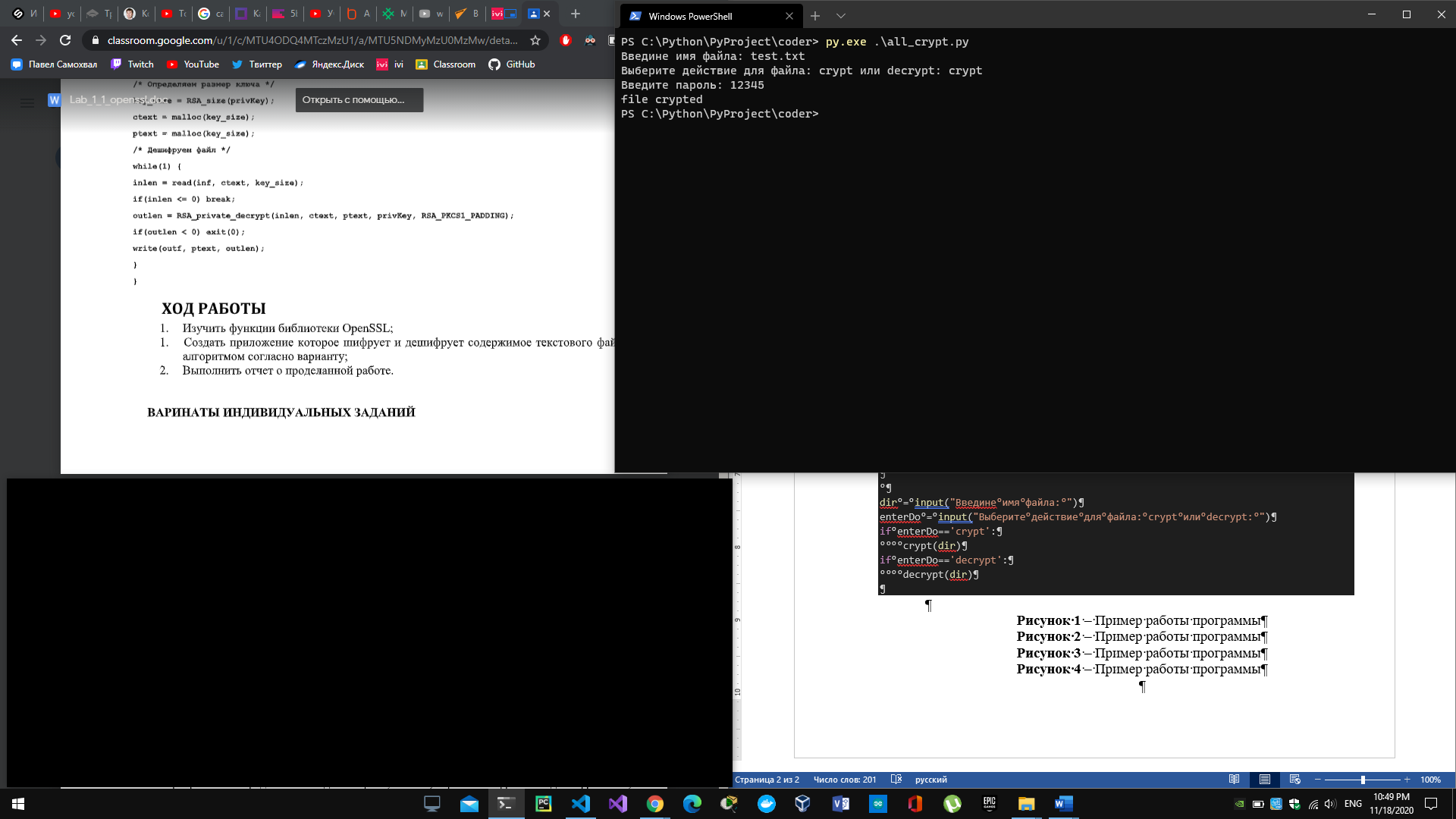
enterDo = input("Выберите действие для файла: crypt или decrypt: ")

if enterDo=='crypt':

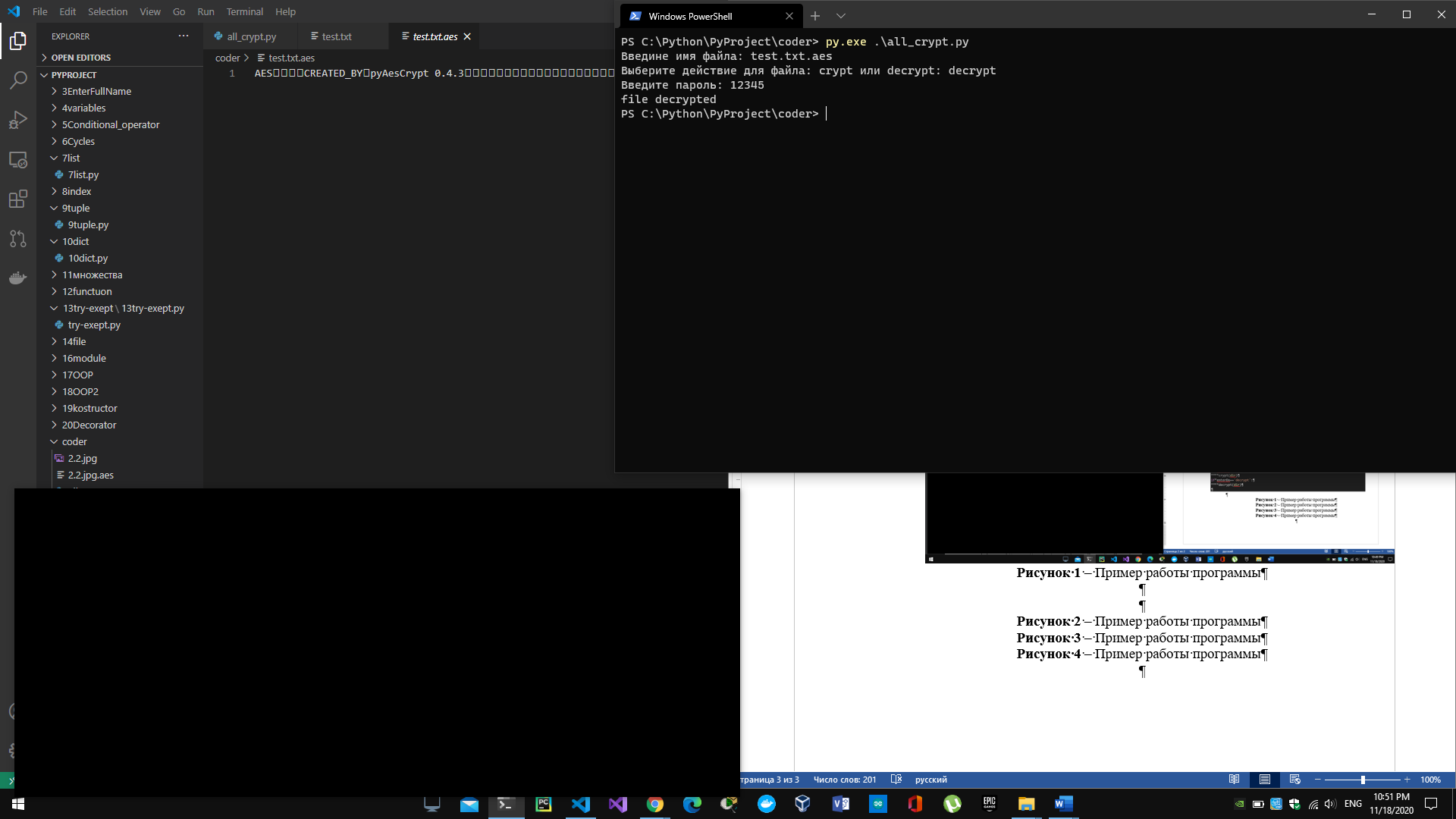
    crypt(dir)

if enterDo=='decrypt':

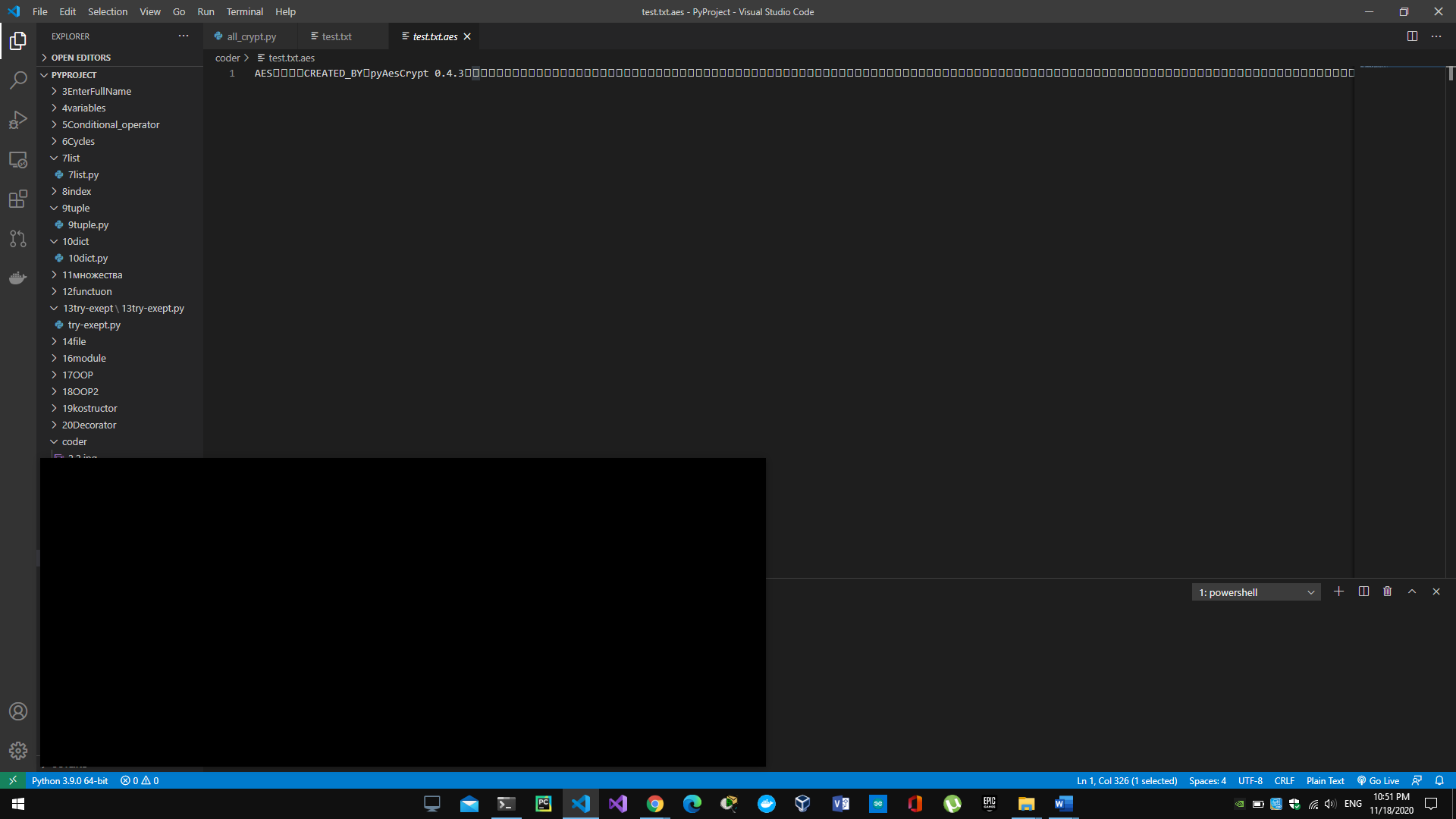
    decrypt(dir)



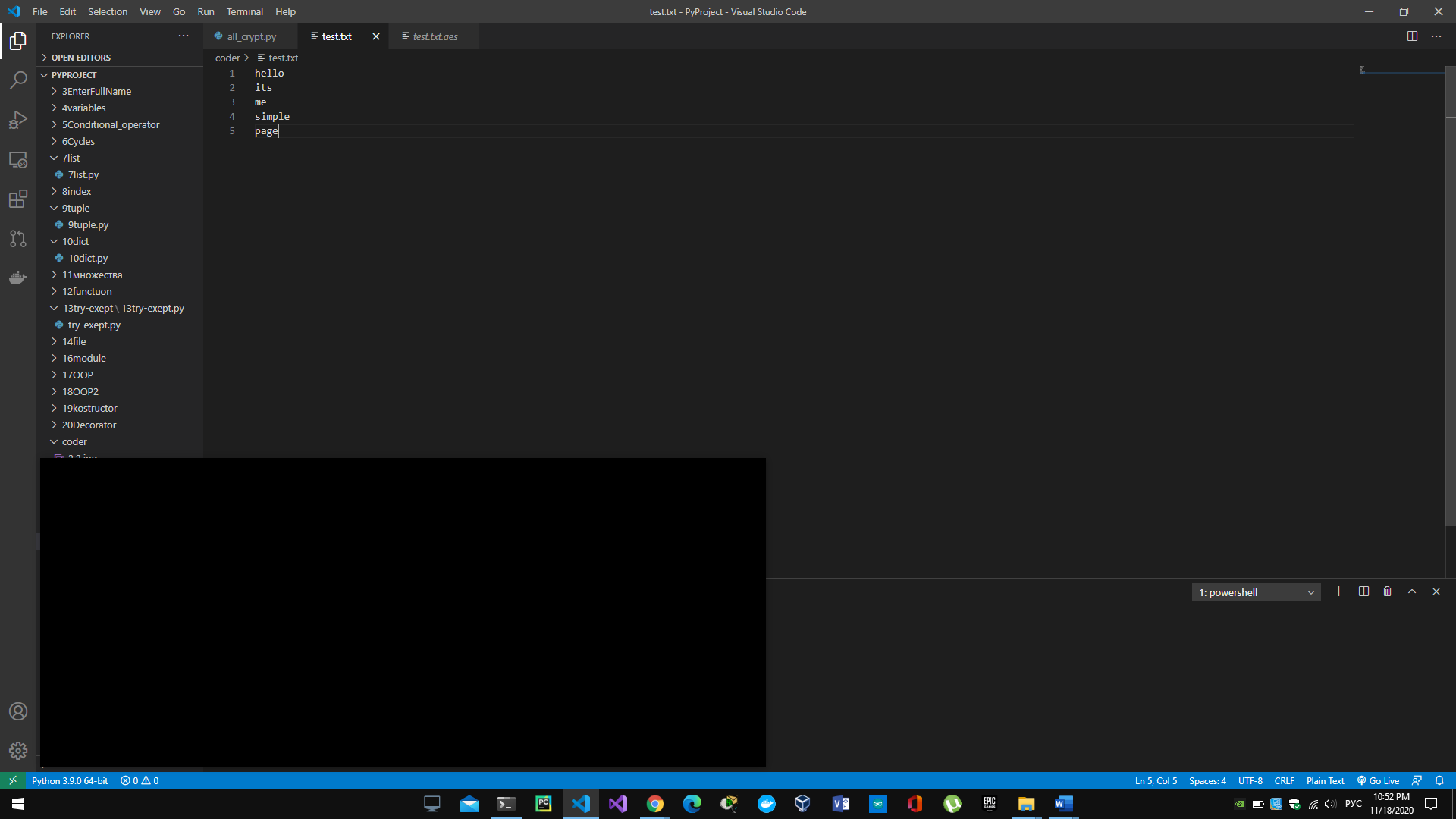
**Рисунок 1** – Пример работы программы



**Рисунок 2** – Пример работы программы



**Рисунок 3** – Пример зашифрованного файла



**Рисунок 4** – Пример расшифрованного файла

**Вывод:** в ходе выполнения данной лабораторной работы было создано приложение, которое шифрует и дешифрует данные симметричным алгоритмом AES.