Департамент образования города Москвы

Государственное автономное образовательное учреждение высшего образования города Москва «Московский Городской Педагогический Университет»

Институт цифрового образования
Департамент информатики, управления и технологий

ЛАБОРАТОРНАЯ РАБОТА №5

по дисциплине «Распределенные системы»
Направление подготовки 38.03.05 – «бизнес-информатика»
Профиль подготовки «Аналитика данных и эффективное управление» (очная форма обучения)

Выполнил:
Студент группы АДЭУ-221
Черенков Иван Романович

_____

Проверил:
Босенко Т.М., доцент

_____

Москва
2024

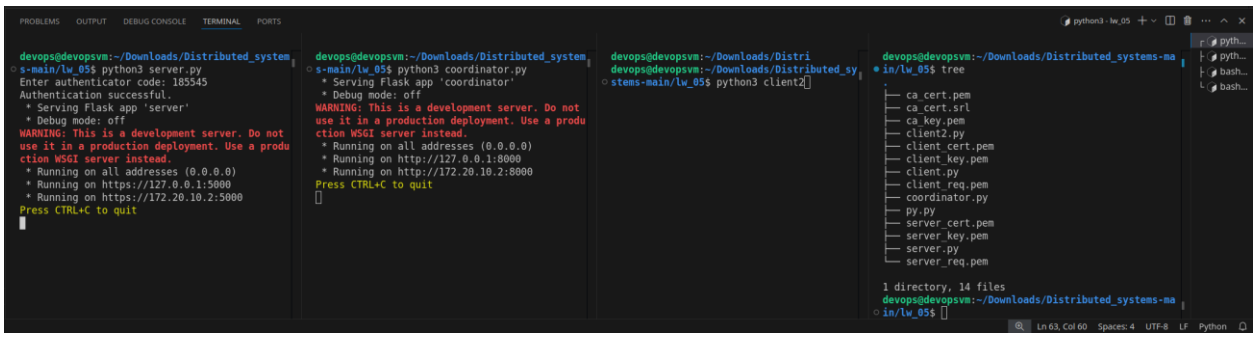
Вариант 20. Сделать двойную аутентификацию файла server.py

Go Run Terminal Help

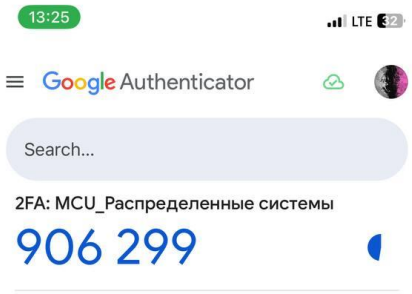
coordinator.py ● server.py × py.py

lw_05 > server.py

```python
from flask import Flask, request, g
import ssl
import binascii
import pyotp
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import padding
from cryptography.x509 import load_pem_x509_certificate
from cryptography.hazmat.backends import default_backend
from cryptography.fernet import Fernet

app = Flask(__name__)

@app.before_request
def verify_client_cert():
    cert = request.get_json()['certificate']
    # Verify certificate against CA
    if not verify_certificate(cert):
        return "Invalid certificate", 401

@app.route('/api/data', methods=['POST'])
def get_data():
    data = request.get_json()['data']
    # Decrypt data
    decrypted_data = decrypt_data(data)
    # Process decrypted data
    return {'result': 'ok'}

def verify_certificate(cert_pem):
    # Load certificate
    certificate = load_pem_x509_certificate(cert_pem.encode(), default_backend())
    # Verify certificate against CA
    try:
        certificate.public_key().verify(
            certificate.signature,
            certificate.tbs_certificate_bytes,
            padding.PKCS1v15(),
            hashes.SHA256()
        )
        return True
    except:
        return False

def decrypt_data(encrypted_data):
    # Load encryption key
    key = open('encryption_key.txt', 'rb').read()
    # Decrypt data
    cipher = Fernet(key)
    return cipher.decrypt(encrypted_data.encode())

if __name__ == '__main__':
    totp = pyotp.TOTP("mcudistibutedsys")
    for x in range(3):
        result = totp.verify(input("Enter authenticator code: "))
        if result:
            print("Authentication successful.")
            context = ssl.create_default_context(ssl.Purpose.CLIENT_AUTH)
            context.load_cert_chain('server_cert.pem', 'server_key.pem')
            context.verify_mode = ssl.CERT_REQUIRED
            context.load_verify_locations('ca_cert.pem')
            app.run(host='0.0.0.0', port=5000, ssl_context=context)
            break
        else:
            print(f"Invalid. Try again. Attempts: {3-x-1}")
```



Как это выглядит на телефоне:



Дерево проекта: