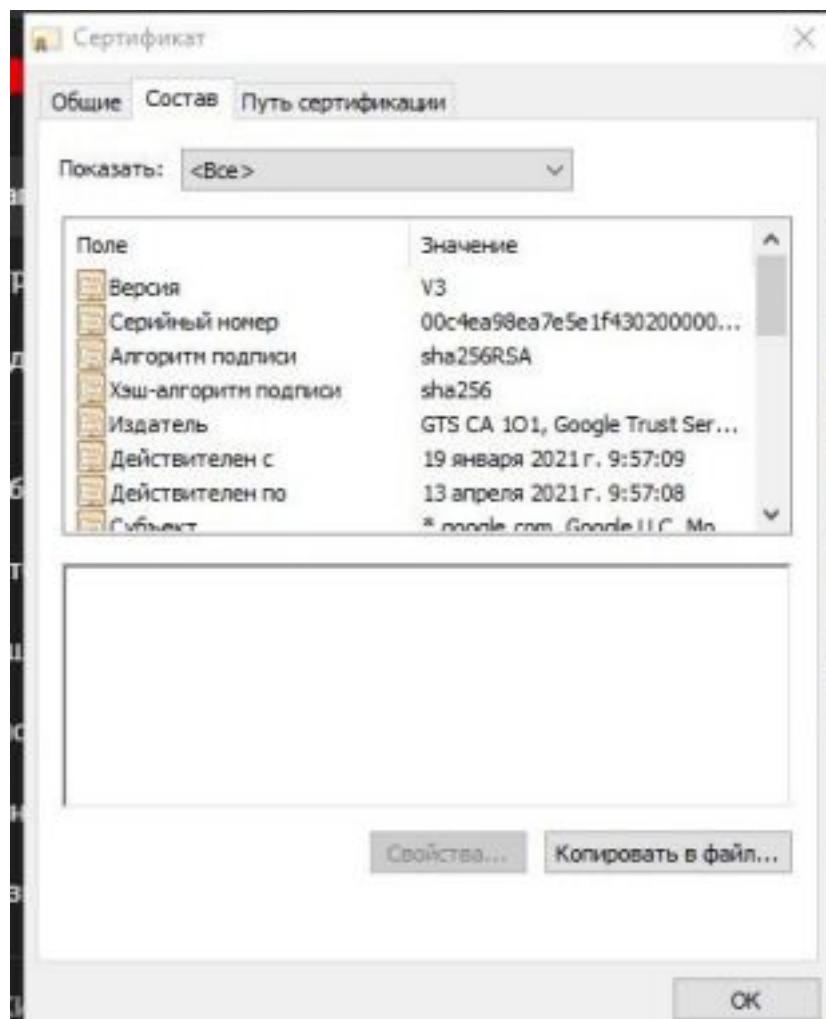


## Lab 7 Report

Алгоритми генерації ключа було вибрано з сертифікат youtube.com.



Для генерації пари ключів в ньому використовується алгоритм на основі

elliptic curves **openssl ecparam -genkey -name prime256v1 -out key.pem**

Специфікація openssl - “prime256v1” це аліас до “secp256r1”.

Генеруємо запит на підпис сертифікату за допомогою команди:

**openssl req -new -sha256 -key key.pem -out csr.pem -config csr.config**

Файл з конфігураціями:

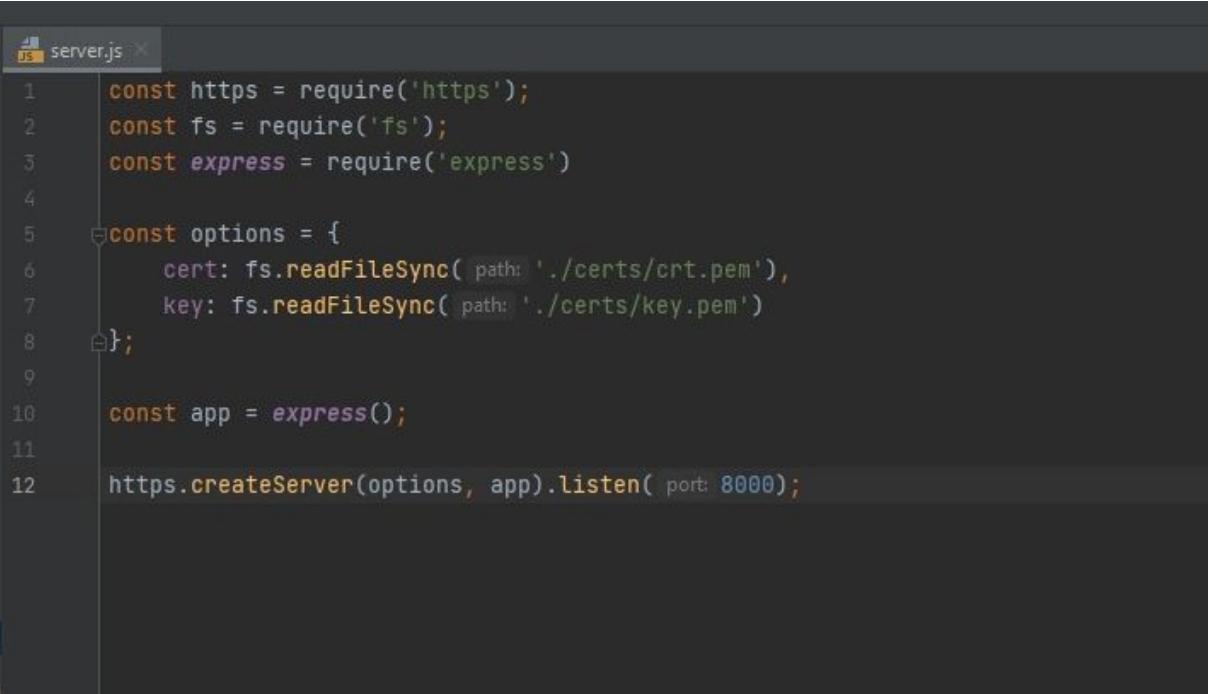
```
[req]
default_bits=2048
prompt=no
default_md=sha256
distinguished_name=distinguished_name

[distinguished_name]
countryName          = UA
stateOrProvinceName = Kyiv
organizationName     = KPI
organizationalUnitName = FICT
commonName           = localhost
emailAddress         = ip72@gmail.com
```

Підписуємо його за допомогою раніше створеного ключа, таким чином отримуємо self-signed certificate:

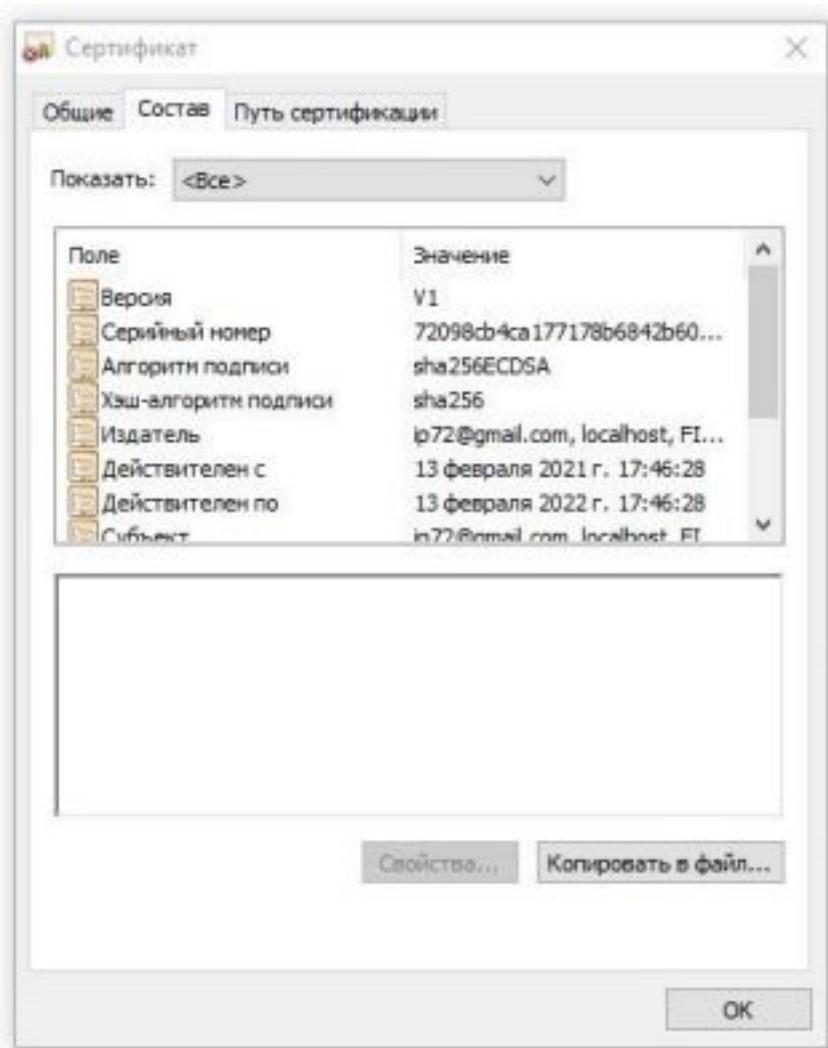
```
openssl x509 -req -in csr.pem -signkey key.pem -out crt.pem -days 365 -sha256
```

Добавляємо наш ключ та сертифікат до серверу написаного на node.js.



A screenshot of a code editor window titled "server.js". The code is written in JavaScript and sets up an HTTPS server using the Node.js modules `https`, `fs`, and `express`. It includes certificate and key files from a local directory.

```
1 const https = require('https');
2 const fs = require('fs');
3 const express = require('express')
4
5 const options = {
6   cert: fs.readFileSync('./certs/crt.pem'),
7   key: fs.readFileSync('./certs/key.pem')
8 };
9
10 const app = express();
11
12 https.createServer(options, app).listen( port: 8000);
```



Для генерації ключа було використано алгоритм на базі еліптичної кривої, так як він вважається більш надійним для шифрування, ніж базовий алгоритм RSA.

Згенерований сертифікат може знаходитись поруч з кодом серверу, так як це не є секретною інформацією. Для збереження приватного ключа бажано використовувати місця з підвищеним захистом та обмеженим доступом, наприклад спеціальні програми по типу “Keychain” для того, щоб безпечно зберігати приватні ключі та надавати до них доступ тільки авторизованим користувачам чи програмам.