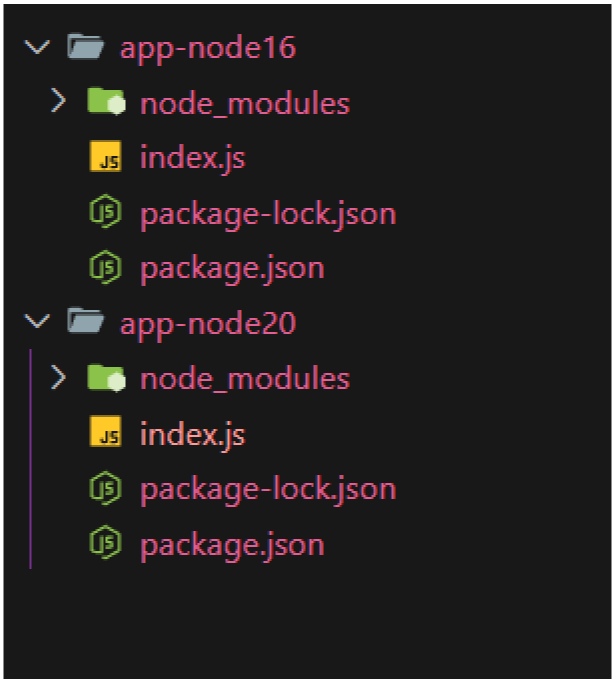
TASK1

Folder Structure



```
app-node16
  node_modules
  index.js
  package-lock.json
  package.json
app-node20
  node_modules
  index.js
  package-lock.json
  package.json
```

Step 1 :

Created Two Apps

Both index.js files in app-node16 and app-node20 are nearly identical, except for the **port number**.

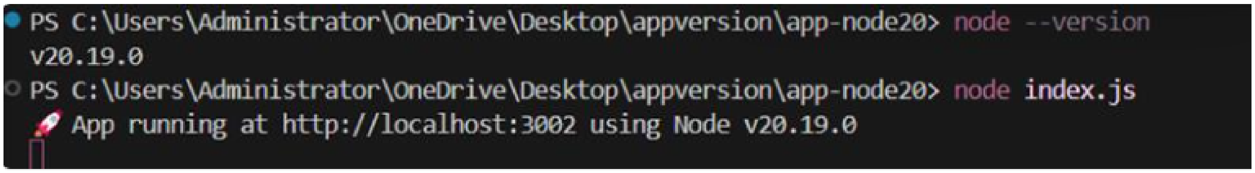
Code for index.js for both

```
const express = require('express');
const app = express();
const port = process.env.PORT || 3000;

let counter = 0;

app.get('/', (req, res) => {
  res.send(`
    <h1>🟢 Node Info Server</h1>
    <p><strong>Node Version:</strong>
${process.version}</p>
    <p><strong>Running on Port:</strong>
${port}</p>
    <p><strong>Directory:</strong> ${__dirname}</p>
    <p>Try hitting <a href="/counter">/counter</a>
to increment a value stored per instance.</p>
  `);
});

app.get('/counter', (req, res) => {
  counter++;
  res.send({
    message: 'Counter incremented!',
    value: counter,
    nodeVersion: process.version,
    dir: __dirname,
  });
});

app.listen(port, () => {
  console.log(`🚀 App running at
http://localhost:${port} using Node
${process.version}`);
});
```

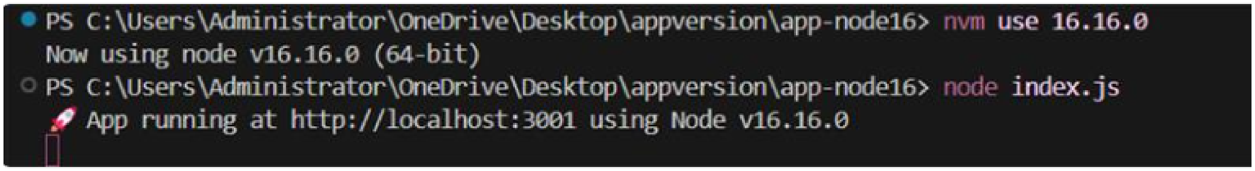
STEP2

Run Both Apps in Parallel

Run each app in separate terminal windows.

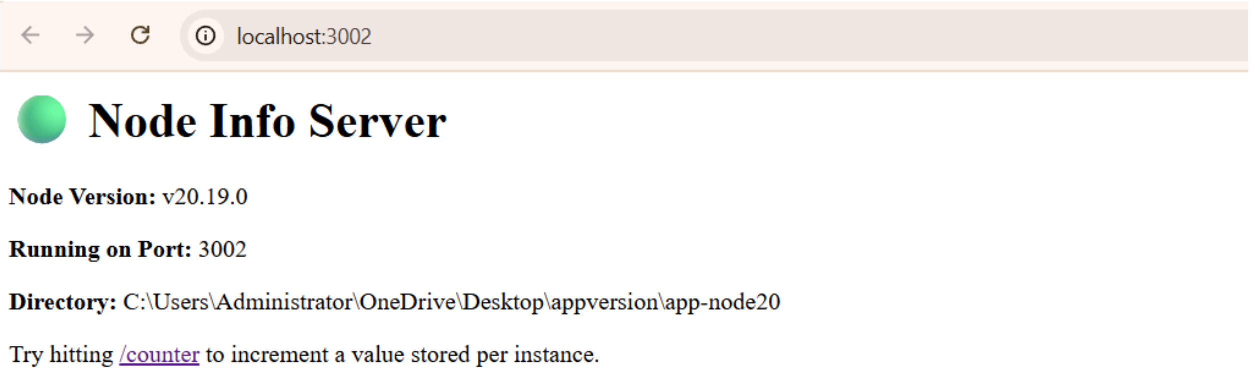


```
PS C:\Users\Administrator\OneDrive\Desktop\appversion\app-node20> node --version
v20.19.0
PS C:\Users\Administrator\OneDrive\Desktop\appversion\app-node20> node index.js
🚀 App running at http://localhost:3002 using Node v20.19.0
```



```
PS C:\Users\Administrator\OneDrive\Desktop\appversion\app-node16> nvm use 16.16.0
Now using node v16.16.0 (64-bit)
PS C:\Users\Administrator\OneDrive\Desktop\appversion\app-node16> node index.js
🚀 App running at http://localhost:3001 using Node v16.16.0
```

ON port 3002, for node20



Node Info Server

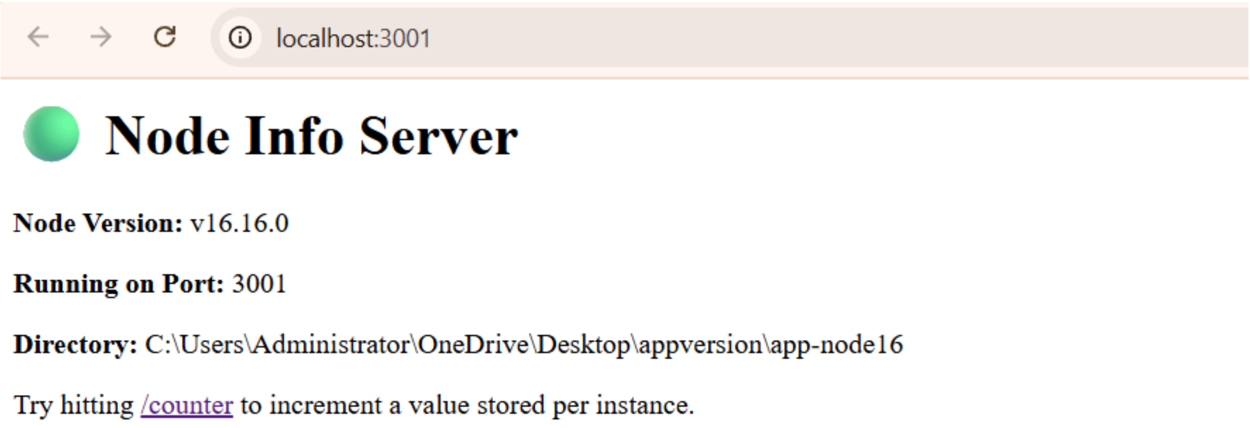
Node Version: v20.19.0

Running on Port: 3002

Directory: C:\Users\Administrator\OneDrive\Desktop\appversion\app-node20

Try hitting /counter to increment a value stored per instance.

ON port 3001, for node16



Node Info Server

Node Version: v16.16.0

Running on Port: 3001

Directory: C:\Users\Administrator\OneDrive\Desktop\appversion\app-node16

Try hitting /counter to increment a value stored per instance.

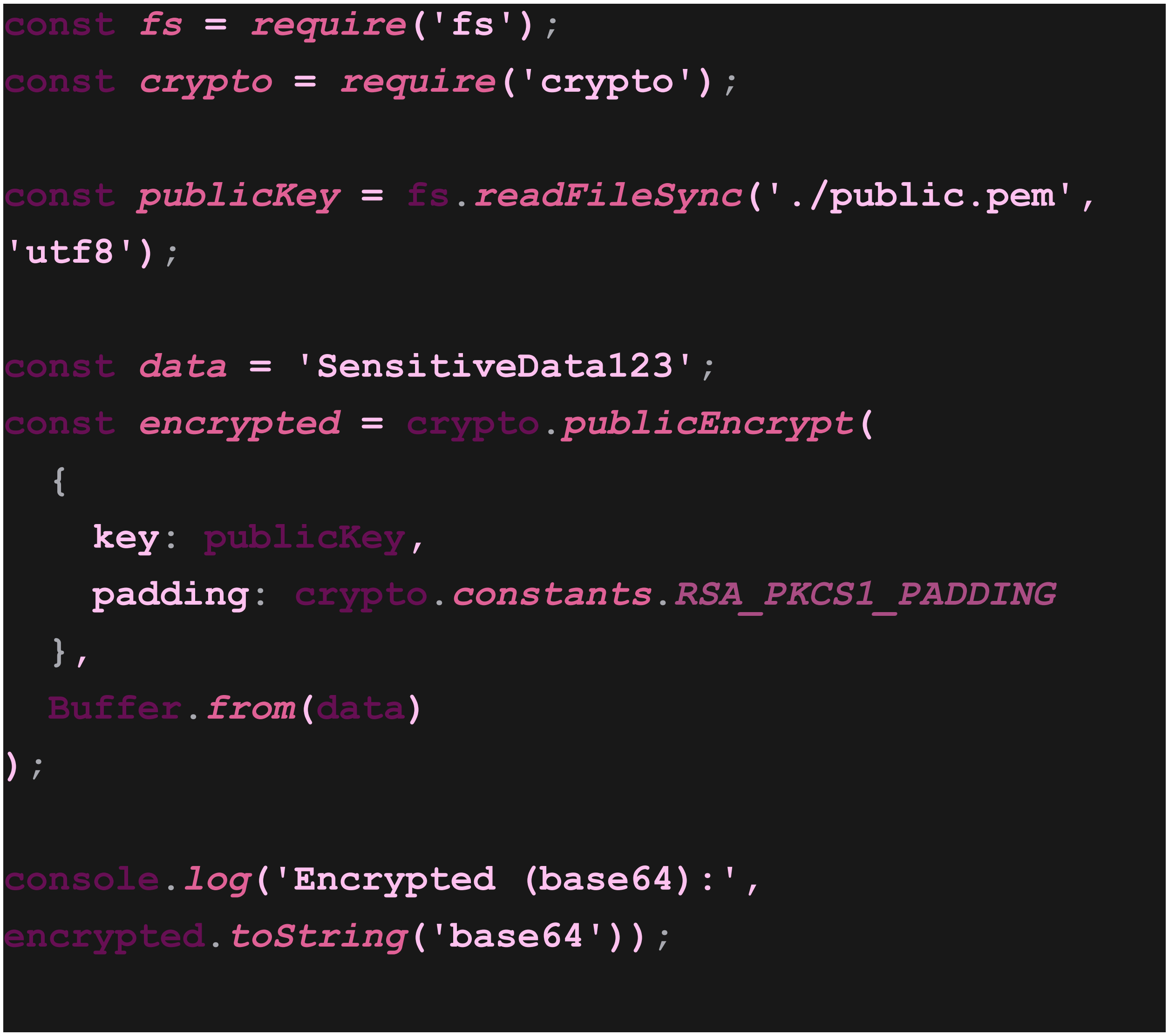
OBSERVATON

Even if we stop the process from one terminal , the either version continues to run in another terminal.

Feature	Benefit
Isolated apps	Avoids version conflicts
Separate ports	No port collision
Portable	Each app is self-contained

TASK 2

Encrypt.js



```javascript
const fs = require('fs');
const crypto = require('crypto');

const publicKey = fs.readFileSync('./public.pem', 'utf8');

const data = 'SensitiveData123';
const encrypted = crypto.publicEncrypt(
  {
    key: publicKey,
    padding: crypto.constants.RSA_PKCS1_PADDING
  },
  Buffer.from(data)
);

console.log('Encrypted (base64):', encrypted.toString('base64'));
```

Server.js(for decryption)

```
const express = require('express');
const fs = require('fs');
const crypto = require('crypto');

const app = express();
const PORT = 3000;

// Middleware to parse JSON bodies
app.use(express.json());

// Load the private key
const privateKey = fs.readFileSync('private.pem', 'utf8');

// Add your POST route for /decrypt
app.post('/decrypt', (req, res) => {
  console.log('Received encrypted payload');

  try {
    const encryptedBase64 = req.body.encrypted;
    const encryptedBuffer = Buffer.from(encryptedBase64, 'base64');

    const decrypted = crypto.privateDecrypt(
      {
        key: privateKey,
        padding: crypto.constants.RSA_PKCS1_PADDING
      },
      encryptedBuffer
    );

    res.json({ decrypted:
decrypted.toString('utf8') });
  } catch (err) {
    console.error('Decryption error:',
err.message);
    res.status(500).json({ error: 'Decryption
failed' });
  }
});

// Start the API server
app.listen(PORT, () => {
  console.log(`Decryption API running on
http://localhost:${PORT}`);
});
```

1.Generate RSA Key Pair

Created:

- **A private key (`private.pem`) – kept on the server for decryption.**

- **A public key (`public.pem`) – used for encryption**

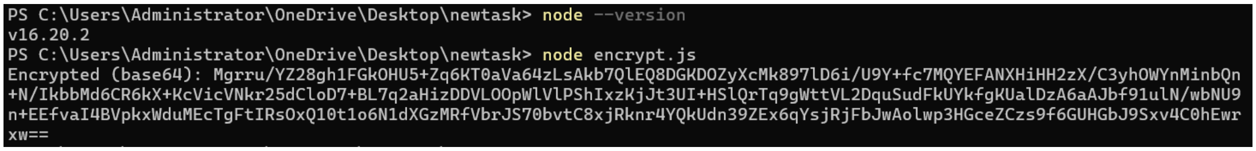
Command

```
openssl genrsa -out private.pem 2048
openssl rsa -in private.pem -pubout -out public.pem
```

2. Encrypt Data using public key

wrote a script encrypt.js that:

- Loads public.pem
- Encrypts a message
- Converts it to Base64 to safely send over API

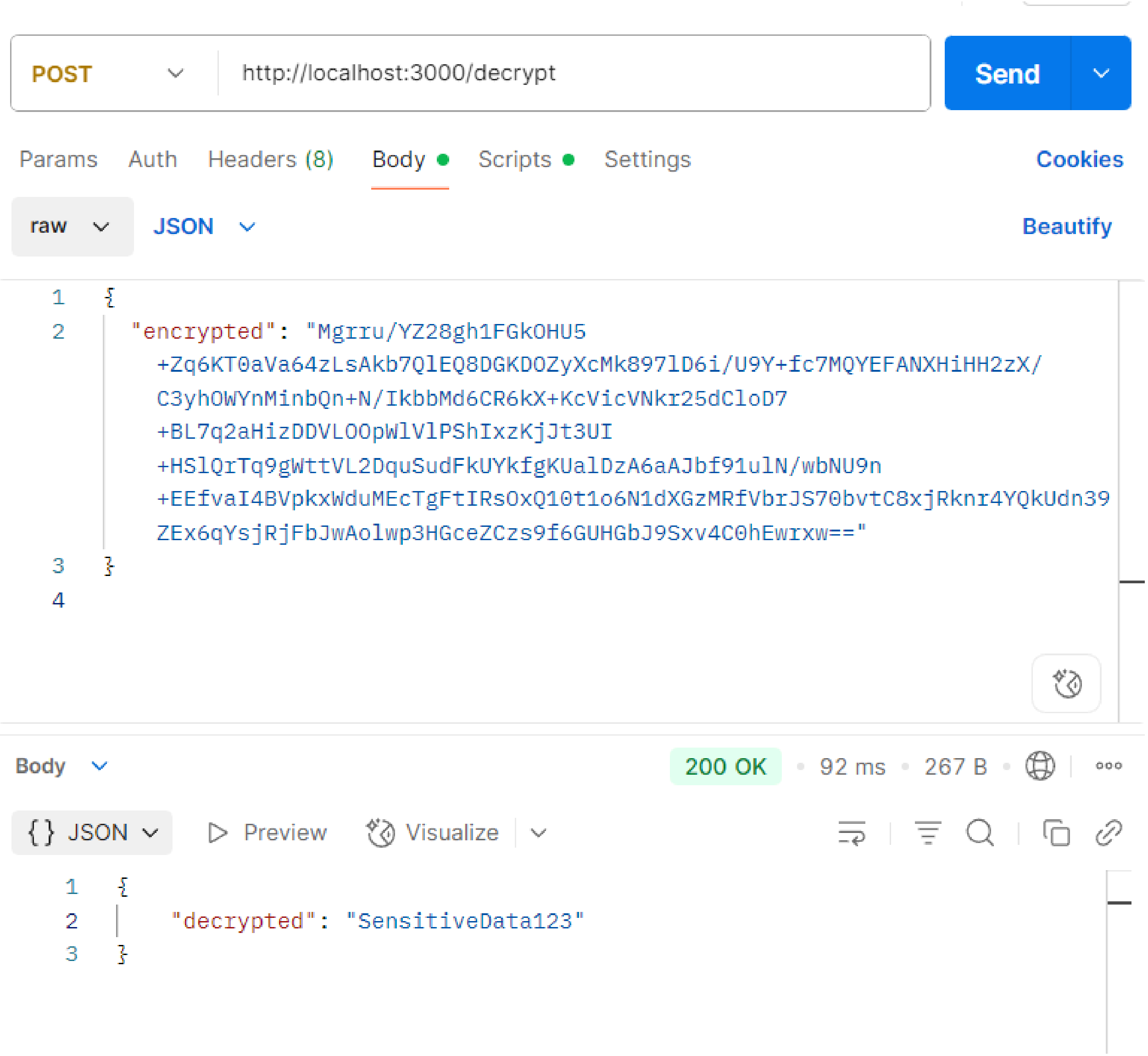


```
PS C:\Users\Administrator\OneDrive\Desktop\newtask> node --version
v16.20.2
PS C:\Users\Administrator\OneDrive\Desktop\newtask> node encrypt.js
Encrypted (base64): Mgrru/YZ28gh1FGkOHU5+Zq6KT0aVa64zLsAkb7QlEQ8DGKDOZyXcMk897lD6i/U9Y+fc7MQYEFANXHiHH2zX/C3yhOWYnMinbQn
+N/IkbbMd6CR6kX+KcVicVNkr25dCloD7+BL7q2aHizDDVLOOpWlVlPShIxzKjJt3UI+HSlQrTq9gWttVL2DquSudFkUYkfgKUalDzA6aAJbf91ulN/wbNU9
n+EEfvaI4BVpkxWduMEcTgFtIRsOxQ10t1o6N1dXGzMRfVbrJS70bvtC8xjRknr4YQkUdn39ZEx6qYsjRjFbJwAolwp3HGceZCzs9f6GUHGbJ9Sxv4C0hEwr
xw==
```

3. Decryption API (Server-side: `server.js`)

Created an Express server with a POST /decrypt endpoint.

- Accepts encrypted Base64 string in the request body
- Converts it to binary
- Decrypts it using the `private.pem` key
- Returns original message in the response

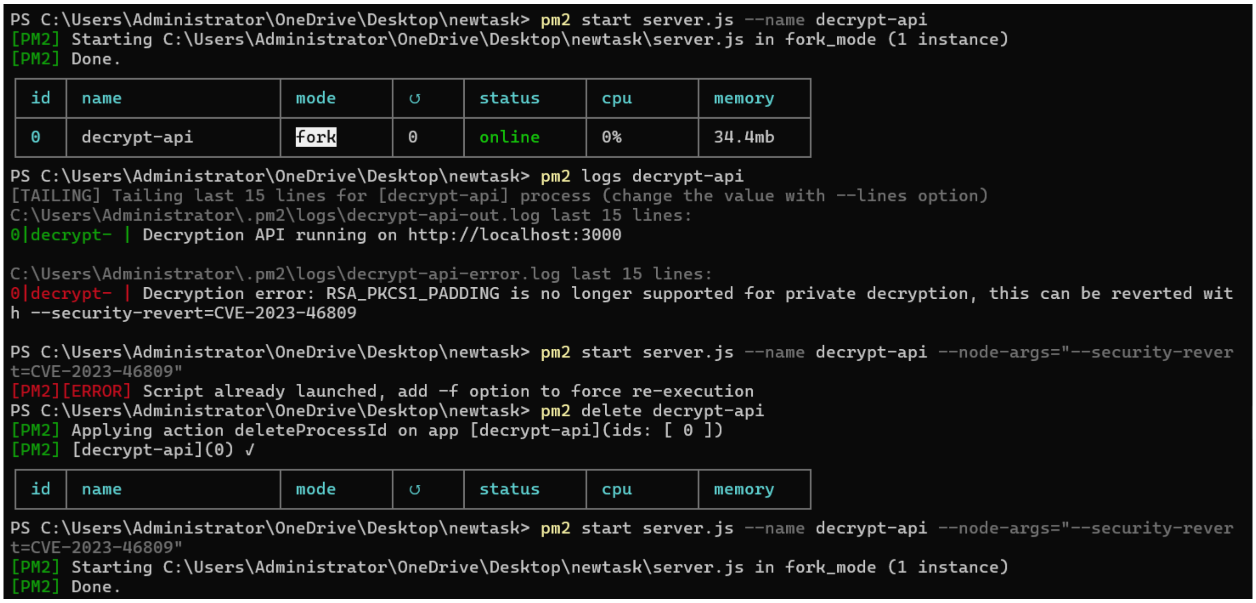


```
{
  "encrypted": "Mgrru/YZ28gh1FGkOHU5
    +Zq6KT0aVa64zLsAkb7QlEQ8DGKDOZyXcMk897lD6i/U9Y+fc7MQYEFANXHiHH2zX/
    C3yhOWYnMinbQn+N/IkbbMd6CR6kX+KcVicVNkr25dCloD7
    +BL7q2aHizDDVLOOpWlVlPShIxzKjJt3UI
    +HSlQrTq9gWttVL2DquSudFkUYkfgKUalDzA6aAJbf91ulN/wbNU9n
    +EEfvaI4BVpkxWduMEcTgFtIRsOxQ10t1o6N1dXGzMRfVbrJS70bvtC8xjRknr4YQkUdn39
    ZEx6qYsjRjFbJwAolwp3HGceZCzs9f6GUHGbJ9Sxv4C0hEwrxw=="
}
```

```
{
    "decrypted": "SensitiveData123"
}
```

4. **Run Server with PM2**

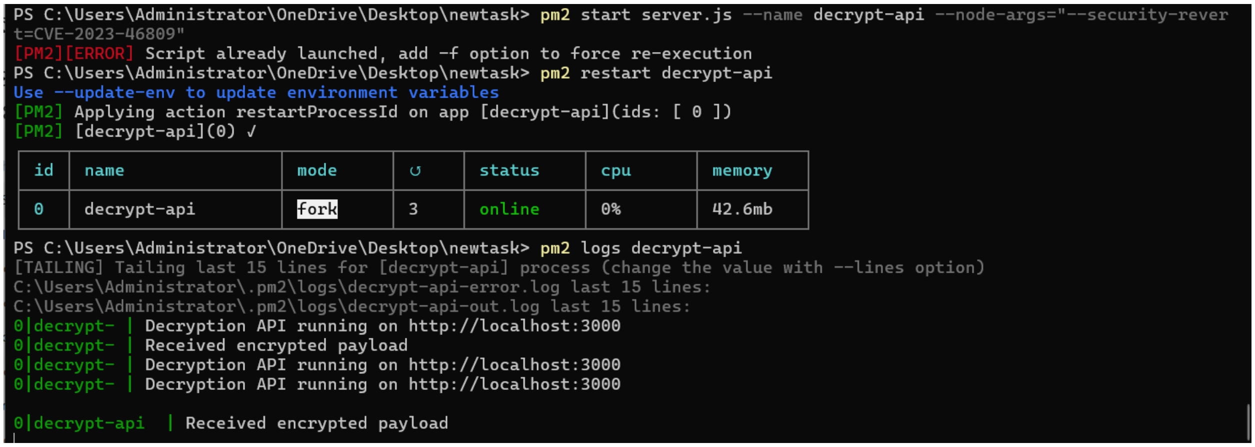
The `--security-revert` was required because Node.js by default blocks PKCS#1 decryption unless reverted.



```
PS C:\Users\Administrator\OneDrive\Desktop\newtask> pm2 start server.js --name decrypt-api
[PM2] Starting C:\Users\Administrator\OneDrive\Desktop\newtask\server.js in fork_mode (1 instance)
[PM2] Done.
┌────┬────────────────────┬──────────┬──────┬───────────┬──────────┬──────────┐
│ id │ name               │ mode     │ ↺    │ status    │ cpu      │ memory   │
├────┼────────────────────┼──────────┼──────┼───────────┼──────────┼──────────┤
│ 0  │ decrypt-api        │ fork     │ 0    │ online    │ 0%       │ 34.4mb   │
└────┴────────────────────┴──────────┴──────┴───────────┴──────────┴──────────┘
PS C:\Users\Administrator\OneDrive\Desktop\newtask> pm2 logs decrypt-api
[TAILING] Tailing last 15 lines for [decrypt-api] process (change the value with --lines option)
C:\Users\Administrator\.pm2\logs\decrypt-api-out.log last 15 lines:
0|decrypt- | Decryption API running on http://localhost:3000

C:\Users\Administrator\.pm2\logs\decrypt-api-error.log last 15 lines:
0|decrypt- | Decryption error: RSA_PKCS1_PADDING is no longer supported for private decryption, this can be reverted wit
h --security-revert=CVE-2023-46809

PS C:\Users\Administrator\OneDrive\Desktop\newtask> pm2 start server.js --name decrypt-api --node-args="--security-rever
t=CVE-2023-46809"
[PM2][ERROR] Script already launched, add -f option to force re-execution
PS C:\Users\Administrator\OneDrive\Desktop\newtask> pm2 delete decrypt-api
[PM2] Applying action deleteProcessId on app [decrypt-api](ids: [ 0 ])
[PM2] [decrypt-api](0) ✓
┌────┬────────────────────┬──────────┬──────┬───────────┬──────────┬──────────┐
│ id │ name               │ mode     │ ↺    │ status    │ cpu      │ memory   │
└────┴────────────────────┴──────────┴──────┴───────────┴──────────┴──────────┘
PS C:\Users\Administrator\OneDrive\Desktop\newtask> pm2 start server.js --name decrypt-api --node-args="--security-rever
t=CVE-2023-46809"
[PM2] Starting C:\Users\Administrator\OneDrive\Desktop\newtask\server.js in fork_mode (1 instance)
[PM2] Done.
```

Using the command

pm2 start server.js --name decrypt-api --node-args="--security-revert=CVE-2023-46809"



```
PS C:\Users\Administrator\OneDrive\Desktop\newtask> pm2 start server.js --name decrypt-api --node-args="--security-rever
t=CVE-2023-46809"
[PM2][ERROR] Script already launched, add -f option to force re-execution
PS C:\Users\Administrator\OneDrive\Desktop\newtask> pm2 restart decrypt-api
Use --update-env to update environment variables
[PM2] Applying action restartProcessId on app [decrypt-api](ids: [ 0 ])
[PM2] [decrypt-api](0) ✓
┌────┬────────────────────┬──────────┬──────┬───────────┬──────────┬──────────┐
│ id │ name               │ mode     │ ↺    │ status    │ cpu      │ memory   │
├────┼────────────────────┼──────────┼──────┼───────────┼──────────┼──────────┤
│ 0  │ decrypt-api        │ fork     │ 3    │ online    │ 0%       │ 42.6mb   │
└────┴────────────────────┴──────────┴──────┴───────────┴──────────┴──────────┘
PS C:\Users\Administrator\OneDrive\Desktop\newtask> pm2 logs decrypt-api
[TAILING] Tailing last 15 lines for [decrypt-api] process (change the value with --lines option)
C:\Users\Administrator\.pm2\logs\decrypt-api-error.log last 15 lines:
C:\Users\Administrator\.pm2\logs\decrypt-api-out.log last 15 lines:
0|decrypt- | Decryption API running on http://localhost:3000
0|decrypt- | Received encrypted payload
0|decrypt- | Decryption API running on http://localhost:3000
0|decrypt- | Decryption API running on http://localhost:3000

0|decrypt-api  | Received encrypted payload
```