

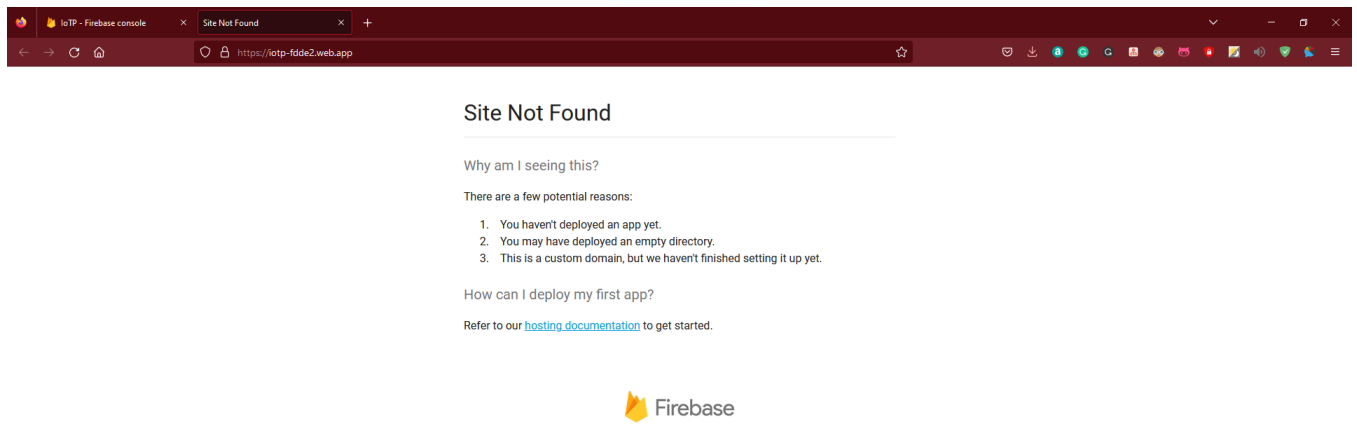
物聯網實務第十四周作業

電機四乙10828241 陳大荃

December 14, 2022

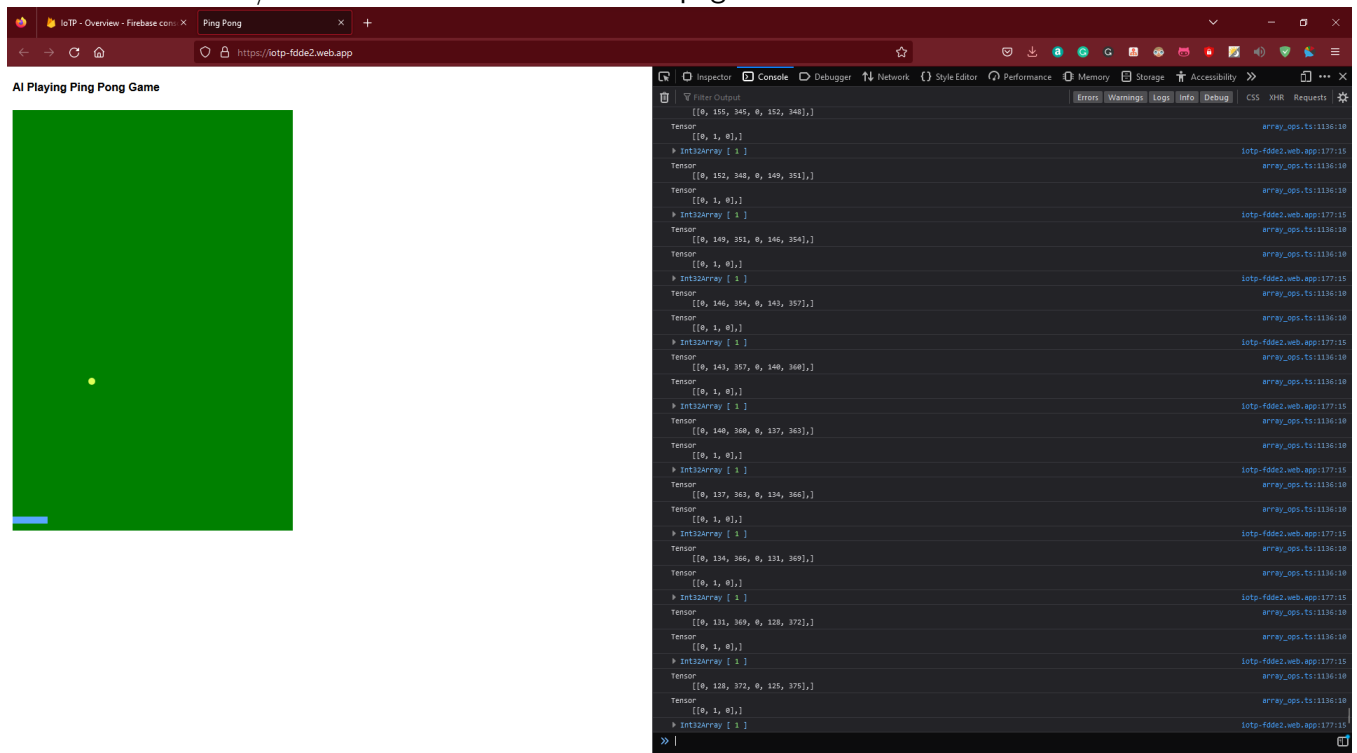
Exercise 13-1 Setup Firebase hosting service.

Setting up a hosting service on the Firebase website.



Exercise 13-2 Hosting ping pong game with Firebase.

Put custom HTML/JS content into the hosted webpage.



Exercise 13-3 Install OpenSSL.

After installing OpenSSL, type "openssl" in cmd to prove successful installation.

```
C:\WINDOWS\system32\cmd. x + - □ x
Microsoft Windows [Version 10.0.22621.963]
(c) Microsoft Corporation. All rights reserved.

C:\Users\dachu>openssl
OpenSSL > |
```

Exercise 13-4 Generate pub/priv key pair

Use node RED flow to generate public and private key pair files on the local drive.

The screenshot shows the Node-RED web interface. The main workspace contains a flow with the following components:

- Inject** node (labeled 'ex13-4') connected to a **timestamp** node.
- The **timestamp** node connects to an **exec** node with the command: `openssl genrsa -out yourdomain key 2048`.
- The **exec** node connects to a **debug** node (labeled 'debug 7').
- Another **timestamp** node connects to an **exec** node with the command: `yourdomain key`.
- This **exec** node connects to a **debug** node (labeled 'debug 10').
- A third **timestamp** node connects to an **exec** node with the command: `openssl rsa -in yourdomain key -pubout -out yourdomain_public key`.
- This **exec** node connects to a **debug** node (labeled 'debug 12').
- A fourth **timestamp** node connects to an **exec** node with the command: `yourdomain_public key`.
- This **exec** node connects to a **debug** node (labeled 'debug 14').

The **debug** console on the right shows the following output:

```
12/14/2022, 2:47:55 PM node: debug 7
msg.payload: string[0]
--

12/14/2022, 2:47:55 PM node: debug 8
msg.payload: string[209]
--
Generating RSA private key, 2048 bit long modulus (2
primes).....+++++
.....+++++e is 65537 (0x010001)-

12/14/2022, 2:47:55 PM node: debug 9
msg.payload: Object
--
{ code: 0 }

12/14/2022, 2:47:56 PM node: debug 10
msg.payload: string[1702]
--
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAQCAQEA3UqHYGTk81nZeJ016s4AaopJo54+uHBEZ4HqZ/Oqok6kxleQ
/ADr6w1E2SCBfW2N8zfr3kXopF6AC4SRISevQhKvmp9KbZrc7B48pTaQemvXcIT2rwhYcgyLoDhxtEg6H8T1EUM4tr+ET2LH3v8GHTJ811v6
6yA56Z7uH8K1L0LmLnQ3Vvuhbdw3uYt6Z+9IoPhuZnBBLf7g2vWfEfyVKzuA84r18zheTa7P-dhB1cLnPE0pt+TwISfpvUzNSQqf19n3jcbu
TprVlqg/ozC8B6rHPWbPAd0w1ly3i3r6z+u3zff1H/d/0vdySAlyx5uFV66zaguIDAQ8BaoI8AE87a1Q3m8p2exnwANTyCDg
/n6ZaZz2z7318F117r3p4uB2yYnq3u48pVJa1TA48Bh+KcC7WmfG6uGp3H3EFPLnduXVLElNgeFV7N8vG1Fz7x7NvgV1k4pBwcc8q8hcs1d4I
jV6u5oZ-d7P2Rfkd02T4M8huCnSQK6PF53or+uePTrGzydUkH8BvplU1/7ALw/neSBMTfe-Je
/4SPtd1jOASChIeqaeTDkuvys5PvacpuTAAQ9rPPVg6uQ20E/TozBF8b8yLQ8wEEBTTZAs1tHTCP3XVGvX/fwt7Kzqj19x5s60UmdkqpeJng
/78erpZLdK3Y5uapc8hg
/kCgYEA77qIobMxciP1C03oy80rUdXf913hqlBvVt8H4veP1Jyfy1aCEK-P1Fe11s+DMLPbVEXMBIDUnglo5bzc8PvOY96ADpzo+fybn1wde7Xba
WLBXKOTIAwy698Zgobtc6QKpy67N3K2HmHwtzLqftu20EQ5zyOyHdx2100U3X8CYEA7E+n-gKvkl1feEhdiaH9KwJyP6jlyercYX3j5Yv6d4H
RPR...

12/14/2022, 2:47:58 PM node: debug 11
msg.payload: string[0]
--

12/14/2022, 2:47:58 PM node: debug 12
msg.payload: string[17]
--
"writing RSA key"

12/14/2022, 2:47:58 PM node: debug 13
msg.payload: Object
--
{ code: 0 }

12/14/2022, 2:48:02 PM node: debug 14
msg.payload: string[460]
--
-----BEGIN PUBLIC KEY-----
MIIEBjBjBgkqhkiG9w0BAQEEFAAOCAQEAFAAQCAQEA3UqHYGTk81nZeJ016s4AaopJo54+uHBEZ4HqZ/Oqok6kxleQ
/ADr6w1E2SCBfW2N8zfr3kXopF6AC4SRISevQhKvmp9KbZrc7B48pTaQemvXIT2rwhYcgyLoDhxtEg6H8T1EUM4tr+ET2LH3v8GHTJ811v6
6yA56Z7uH8K1L0LmLnQ3Vvuhbdw3uYt6Z+9IoPhuZnBBLf7g2vWfEfyVKzuA84r18zheTa7P-dhB1cLnPE0pt+TwISfpvUzNSQqf19n3jcbu
=I3Rv1lqg/ozC8B6rHPWbPAd0w1ly3i3r6z+u3zff1H/d/0vdySAlyx5uFV66zaguIDAQ8BaoI8AE87a1Q3m8p2exnwANTyCDg
-----END PUBLIC KEY-----
```