

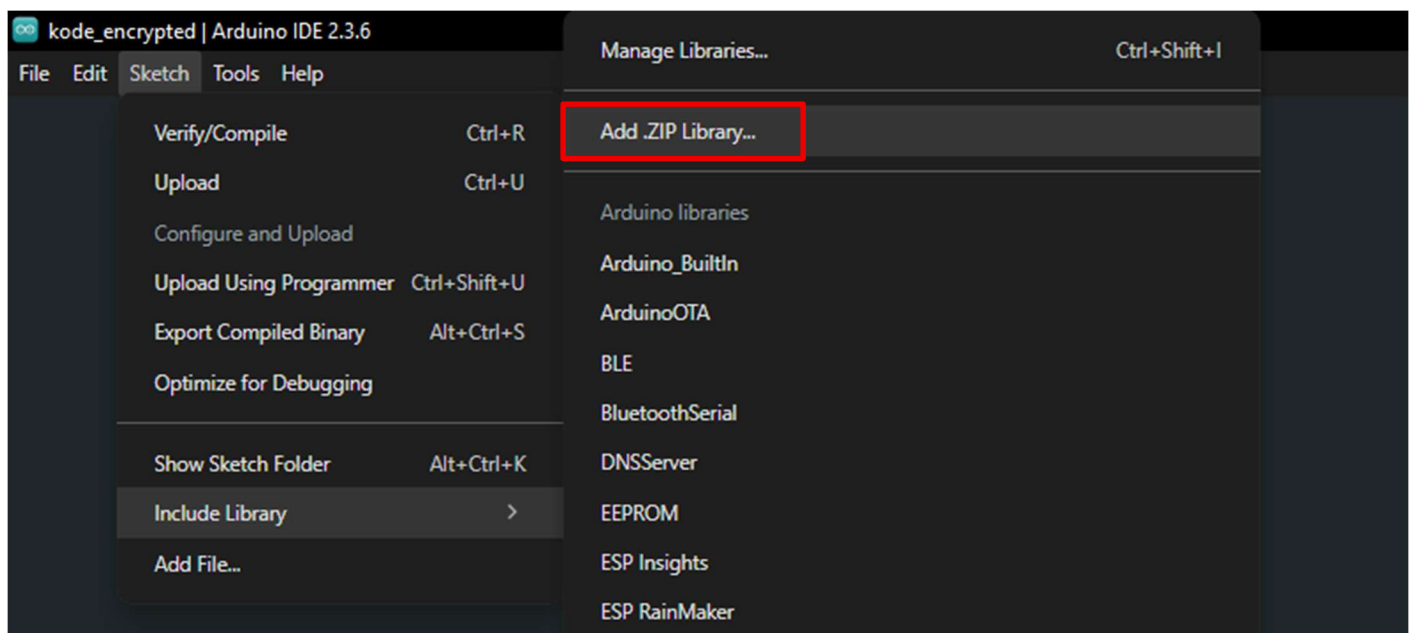
TUTORIAL Enkripsi Dengan Algoritma Kriptografi Ringan: ASCON-128

Perkembangan *Internet of Things* (IoT) telah mendorong kebutuhan akan sistem keamanan yang efisien, terutama karena perangkat IoT umumnya memiliki **keterbatasan dalam daya komputasi, memori, dan konsumsi energi**. Kriptografi konvensional seperti AES sering kali terlalu berat untuk diterapkan secara optimal di perangkat-perangkat ini. Oleh karena itu, dibutuhkan algoritma **kriptografi ringan** yang tetap mampu menjamin **kerahasiaan, integritas, dan autentikasi data**.

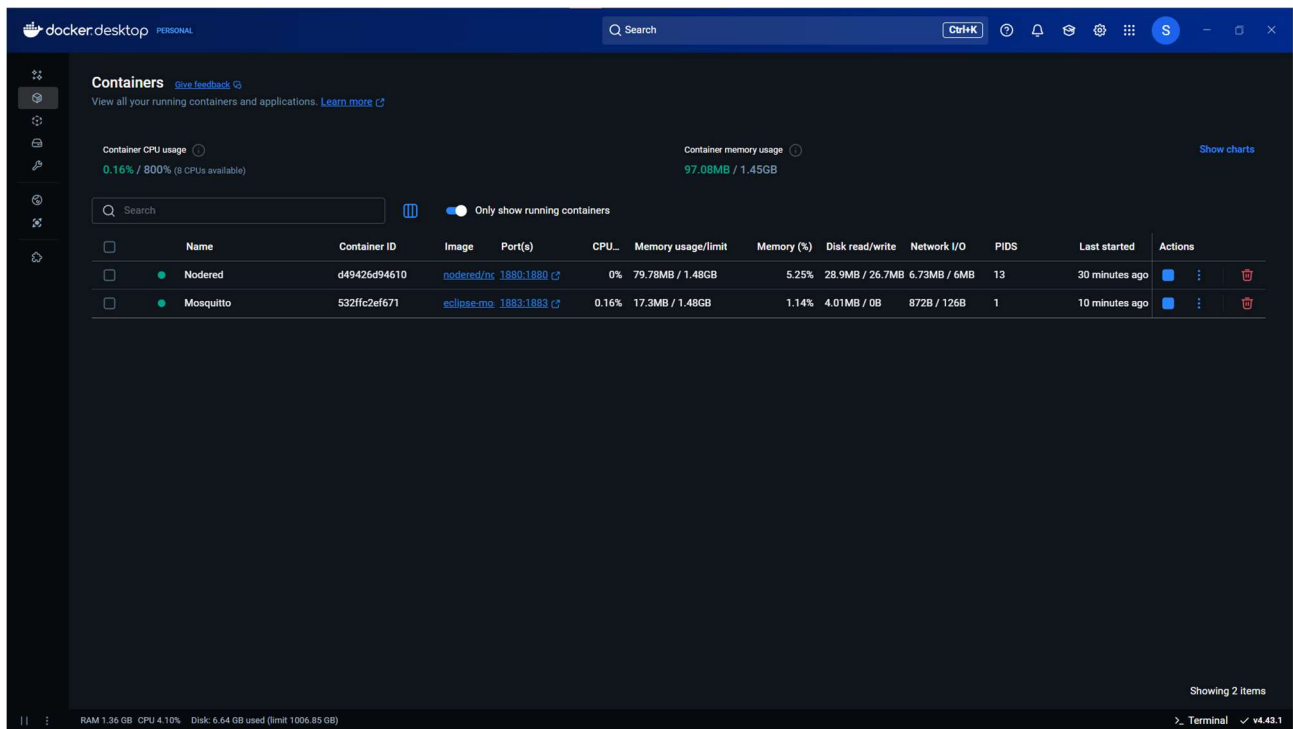
ASCON-128 yang dirancang khusus untuk **efisiensi** dan **keamanan** pada perangkat IoT dengan **sumber daya terbatas**. Dipilih sebagai salah satu algoritma standar oleh *National Institute of Standards and Technology* (NIST) untuk **kriptografi ringan**, **ASCON-128** menawarkan perlindungan data dengan konsumsi sumber daya yang minimal, menjadikannya ideal untuk implementasi di ekosistem IoT yang luas dan beragam.

Langkah-langkah:

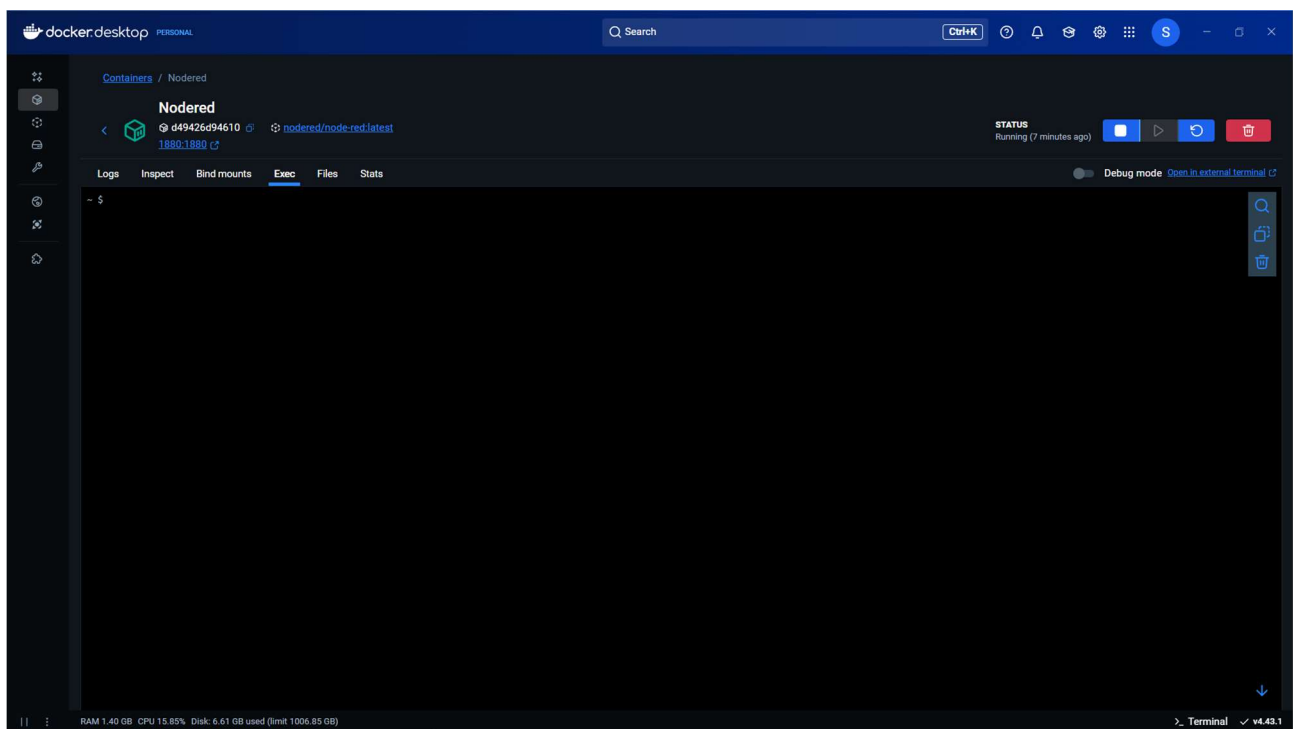
1. Pertama *download* **kode node** dan **kode gateway** pada github. Sesuaikan **UUID** pada **kode node** dan sesuaikan **kode gateway** dari (**nama wifi, password wifi, ip mqtt, UUID dan Key ASCON**)
https://github.com/mhmdnvn18/MATKUL_KEAMANAN-JARINGAN/tree/main/ENKRIPSI/Kode
2. Lalu *download* dan *install* kedua *library* ASCON-128 ke Arduino IDE pada github
https://github.com/mhmdnvn18/MATKUL_KEAMANAN-JARINGAN/tree/main/ENKRIPSI/Library



3. Buka Docker Dekstop, *Run* Mosquitto dan *Run* Node-RED nya

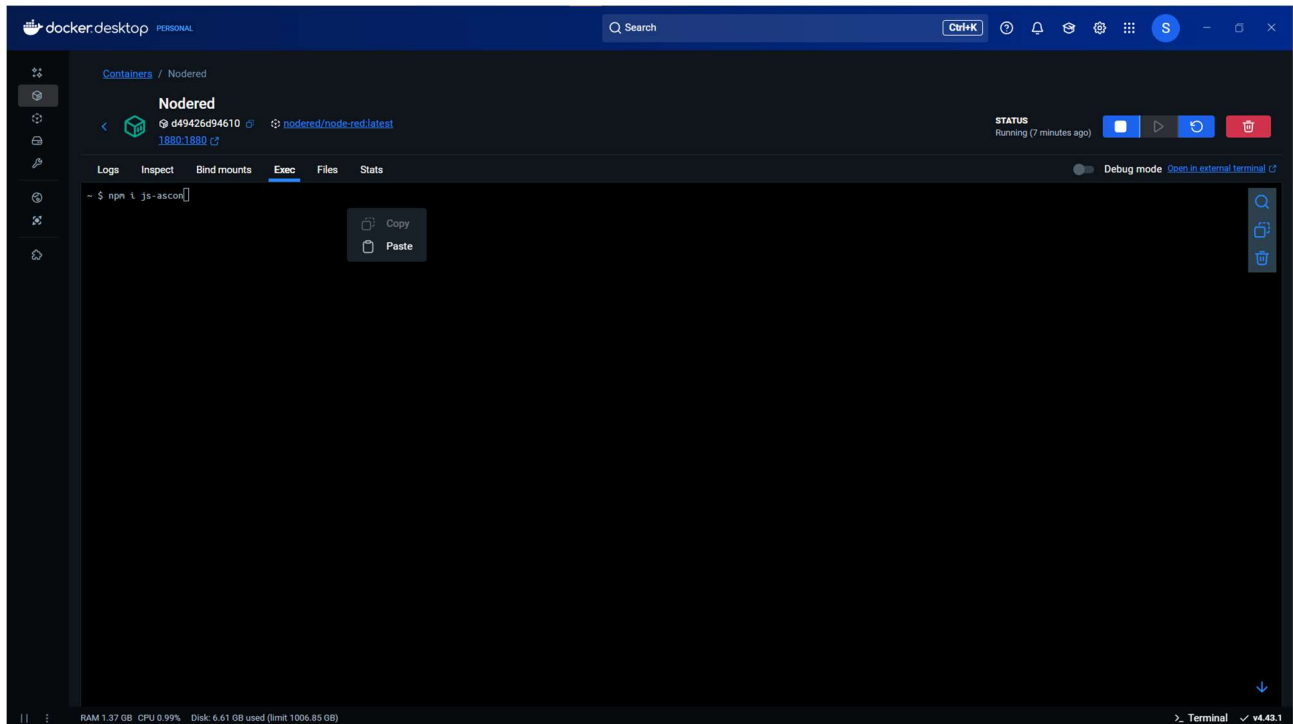


4. Masuk ke Node-Red, dengan klik Nodered, lalu masuk ke exec

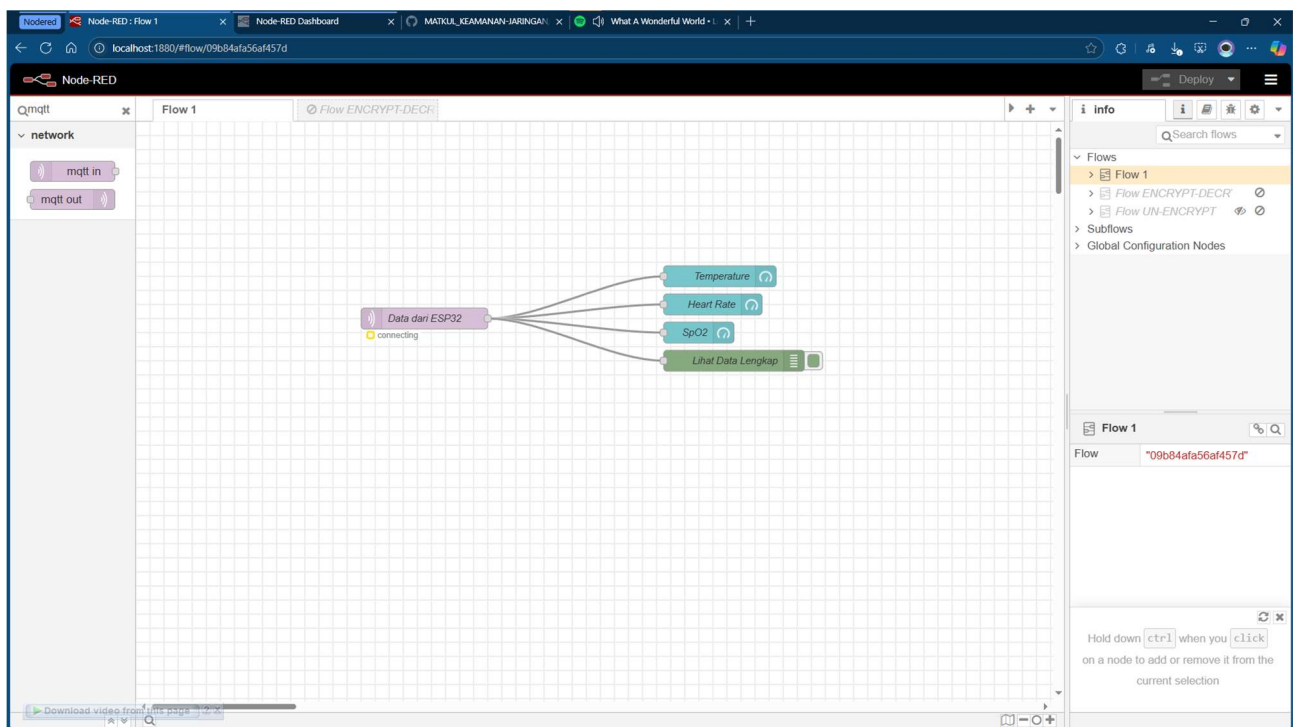


5. Paste command ***npm i js-ascon*** dengan cara klik kanan > *paste*. Lalu Enter.

Command ini digunakan untuk menginstal *library* ASCON ke Node-Red

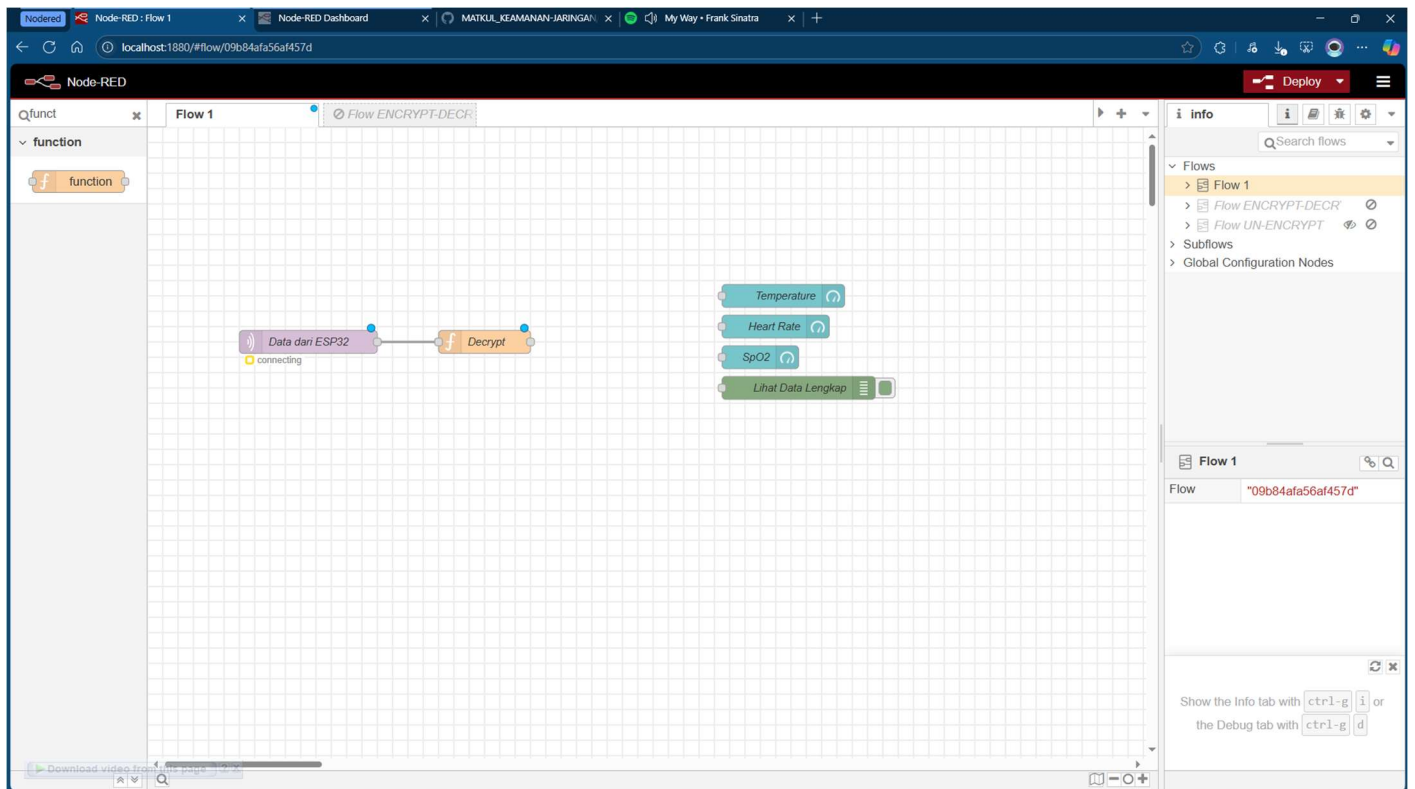


6. Buka *browser* lalu jalankan *nodered*, ketik **localhost:1880** Maka akan tertampil *flow* yang sudah dibuat pada pertemuan sebelumnya.

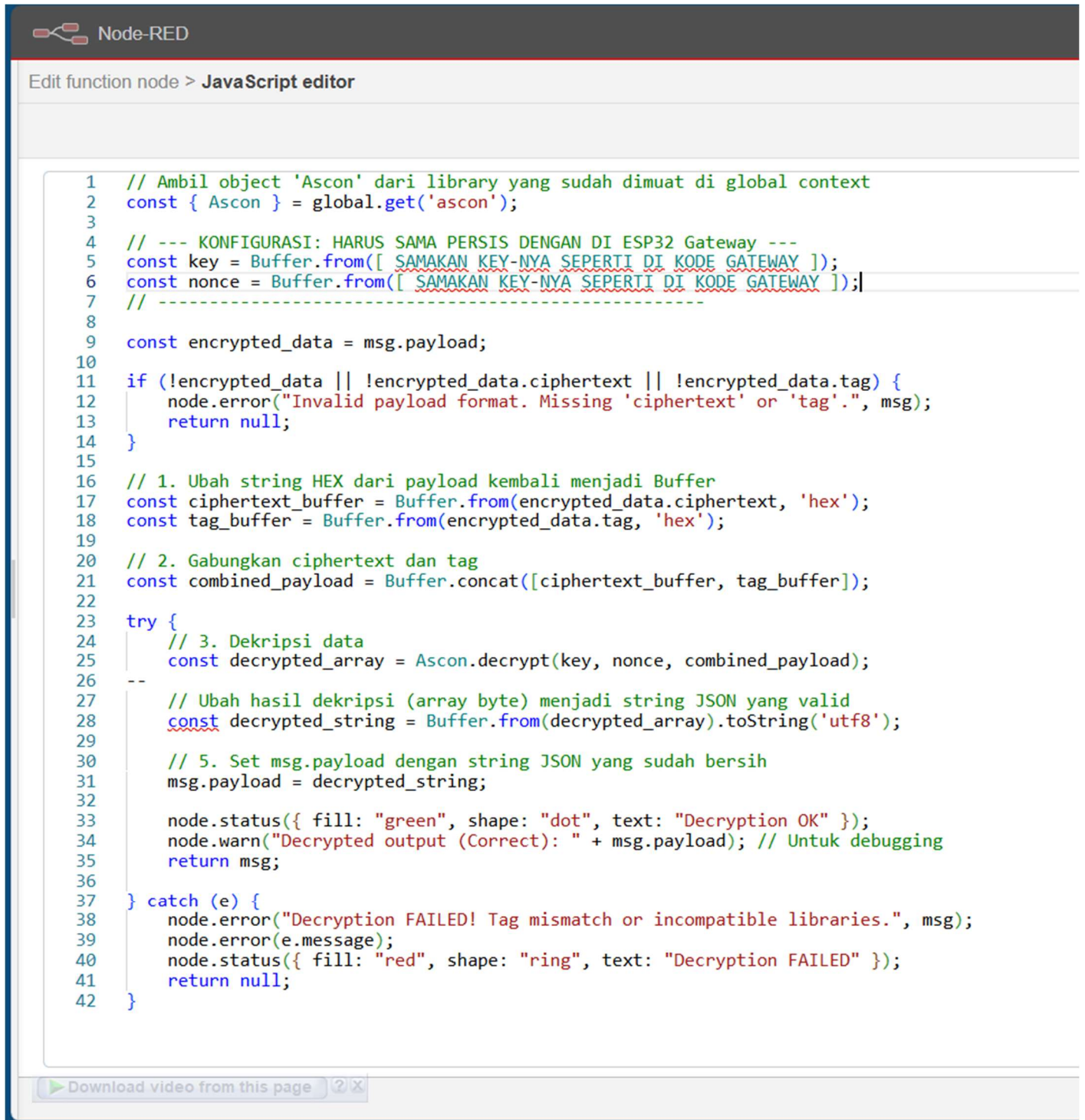


7. Lalu tambahkan *flow function*,

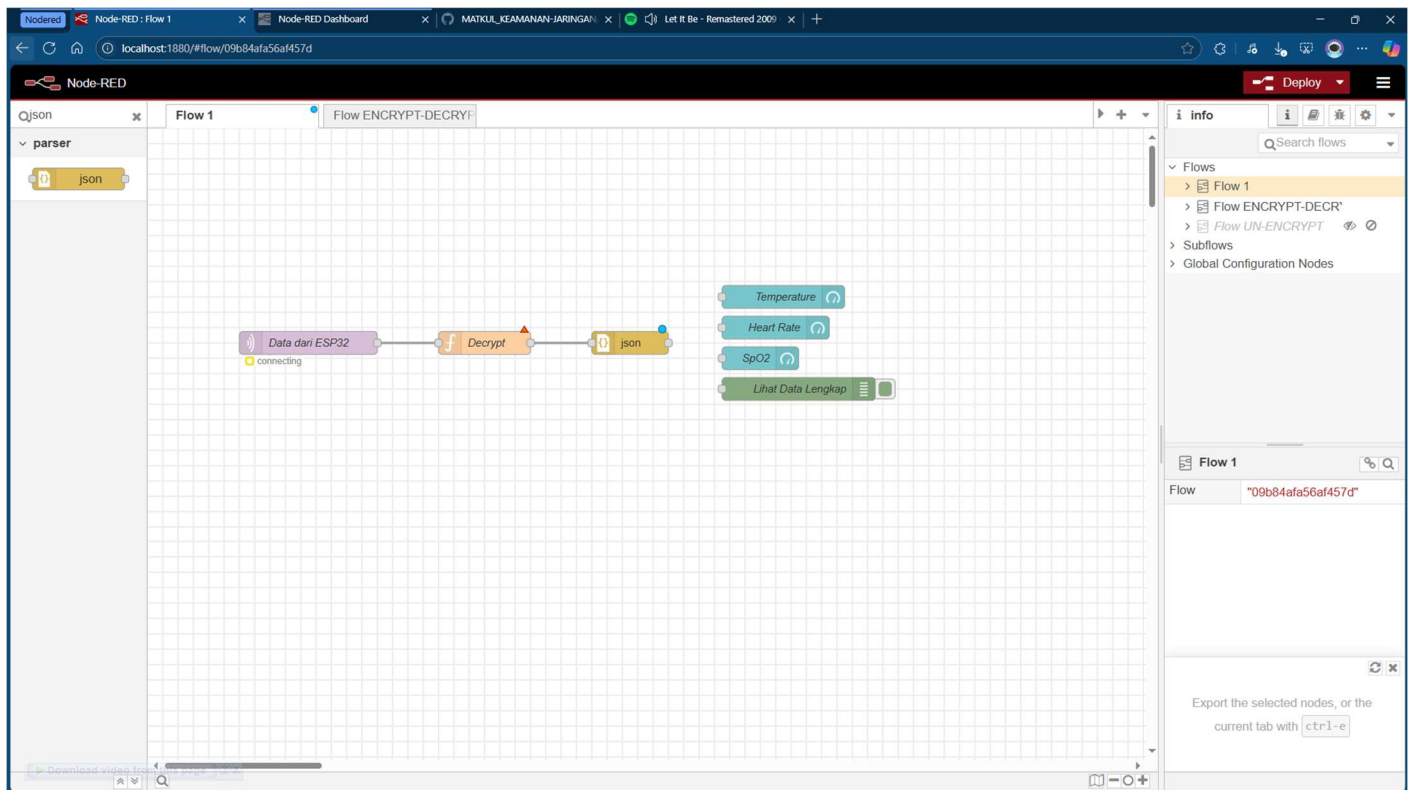
Flow ini digunakan untuk sebagai dekripsi ASCON-128 dari sisi *backend* sebelum ditampilkan pada ui



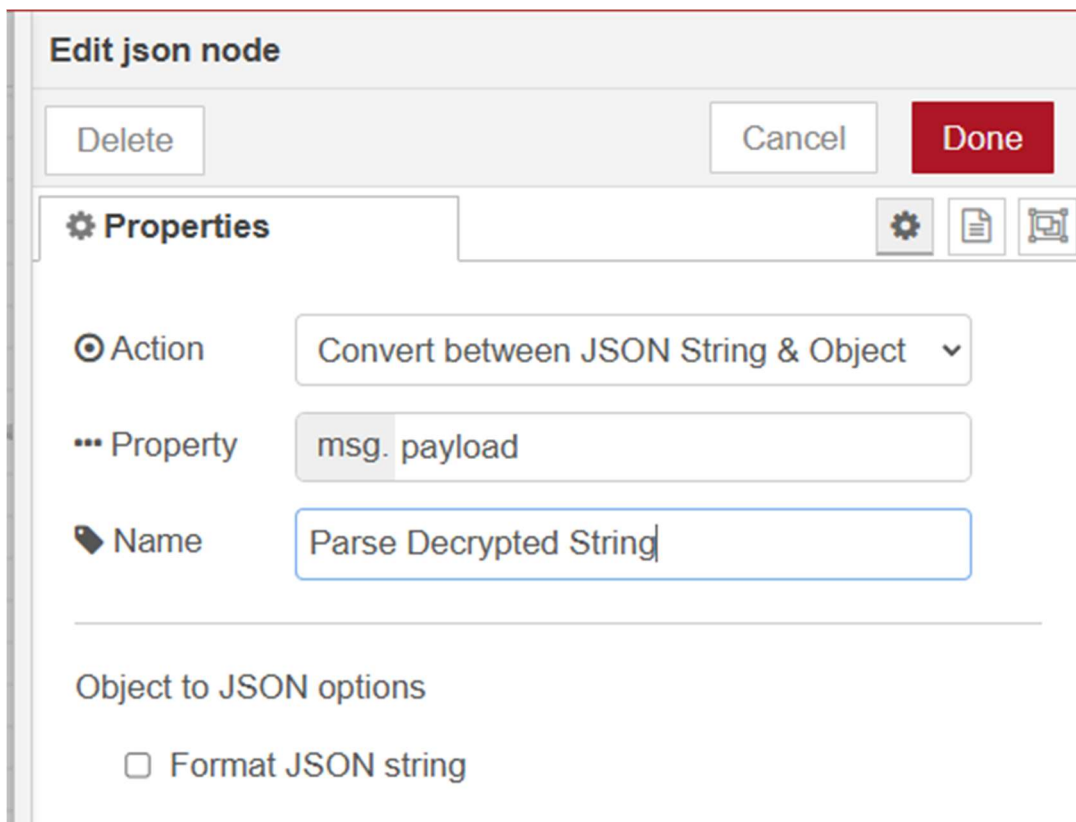
9. Double klik **function**, lalu isi *name* dengan *Decrypt* dan lalu isi pada **On Message** dengan *command* seperti gambar di bawah. Lalu *DONE*

The image shows a screenshot of the Node-RED web interface. At the top, there's a header with the Node-RED logo and the text "Node-RED". Below that, a tab says "Edit function node > JavaScript editor". The main area contains a JavaScript code editor with a line number margin on the left (lines 1 to 42). The code is for a function node that decrypts data using the Ascon library. It starts by getting the 'ascon' library from the global context. Then it defines a key and nonce using Buffer.from, with comments indicating they should match the gateway's configuration. The function takes a message (msg) and extracts its payload. It checks if the payload has 'ciphertext' and 'tag' properties. If not, it returns null. If yes, it converts the ciphertext and tag to buffers. Then it concatenates them and uses the Ascon.decrypt function to decrypt the data. The result is converted back to a UTF-8 string and set as the message's payload. Finally, it updates the node's status to 'green' and logs a success message. A catch block handles decryption failures, setting the status to 'red' and logging an error. At the bottom of the editor, there's a button that says "Download video from this page" with a question mark icon.

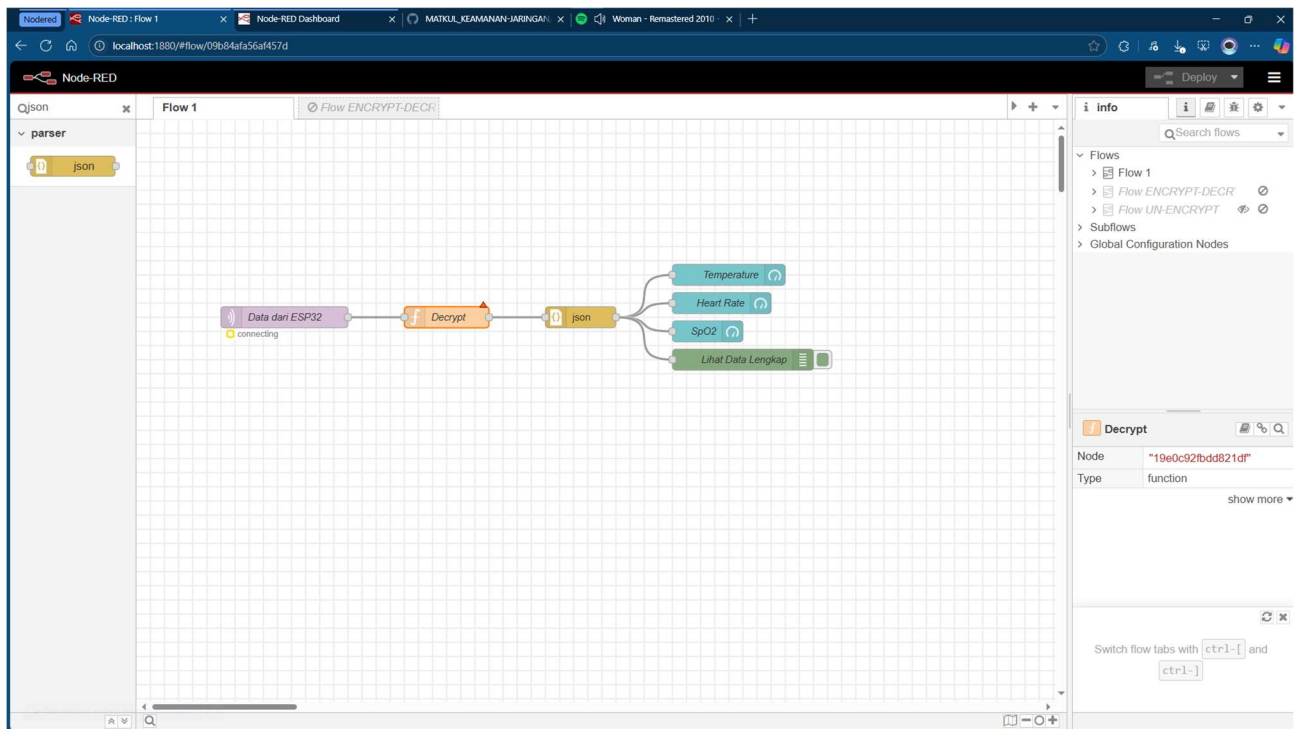
10. Lalu tambahkan *flow JSON*,



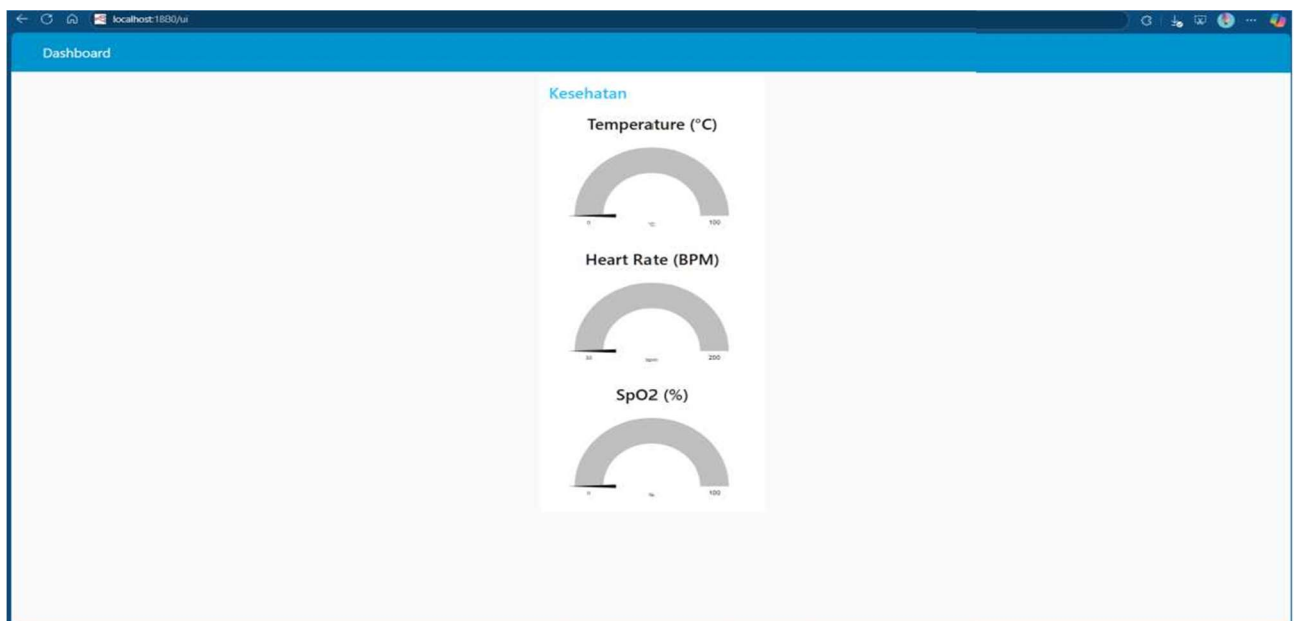
11. Double klik **json**, isi parameter seperti gambar di bawah. Lalu **DONE**.



12. Sambungkan semua *flow*-nya. Lalu *DEPLOY*.



13. Buat tab baru lalu ketikkan <http://localhost:1880/ui>



14. Uji keseluruhan sistemnya.