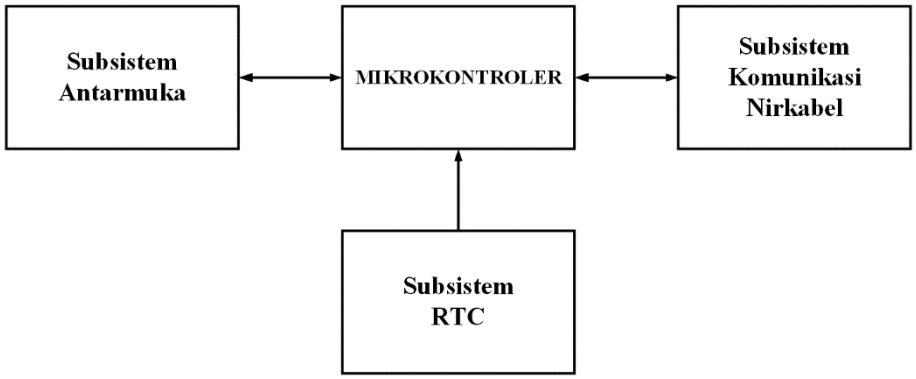
BAB III
ANALISIS DAN PERANCANGAN

Pada penelitian ini akan dilakukan perancangan dan pembuatan perangkat keamanan data pada komunikasi radio yang diberi nama Cryptography Portable (CRYPTOBLE). Perangkat ini terbagi menjadi dua yang salah satunya digunakan sebagai pemancar (*encryptor*) dan yang lain sebagai penerima (*decryptor*). Perangkat ini berfungsi untuk meningkatkan keamanan data dengan merahasiakan/mengkonversi data menggunakan metode kriptografi lalu mengirimkan data tersebut dalam bentuk *ciphertext* dari pemancar ke penerima dan akan dikonversi lagi kedalam bentuk *plaintext*. Perangkat ini menggunakan metode kriptografi XXTEA yang ditanamkan pada mikrokontroler Arduino Nano dan data hasil enkripsi dikirimkan melalui udara menggunakan modul radio NRF24L01 PA LNA. Perangkat ini juga dilengkapi dengan aplikasi berbasis Windows yang berfungsi sebagai antarmuka pengguna untuk melakukan konfigurasi perangkat, yaitu konfigurasi waktu, *baudrate*, kunci, dan alamat radio.

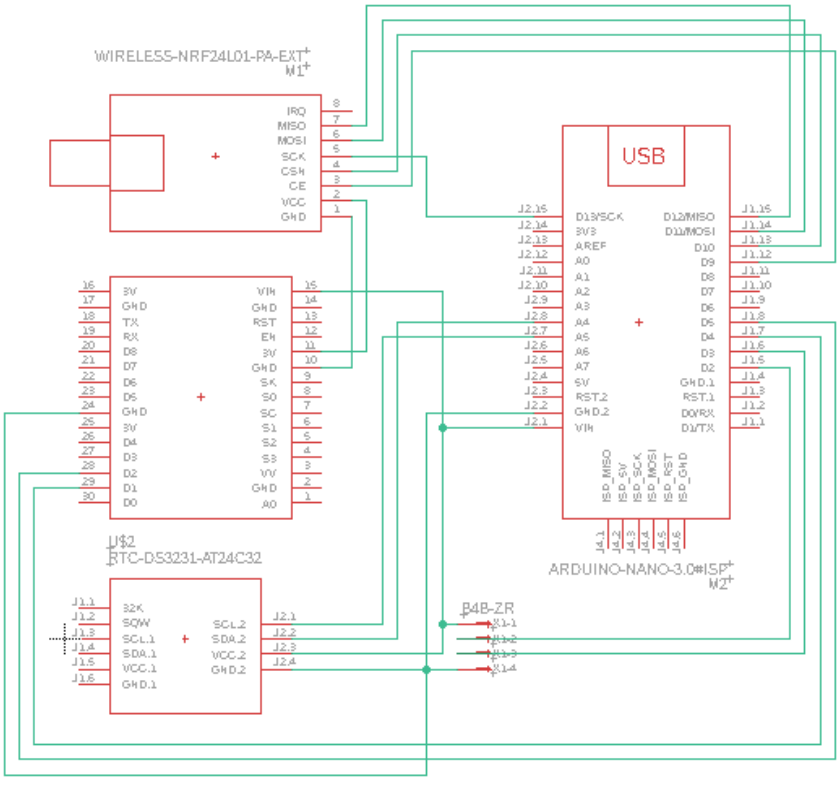
3.1 Perancangan Perangkat CRYPTOBLE

CRYPTOBLE secara garis besar memiliki tiga blok, yaitu antarmuka, RTC dan komunikasi nirkabel. Antarmuka merupakan media tempat komunikasi antara pengguna dan sistem serta tempat pengguna untuk memberikan perintah kepada sistem. Melalui antarmuka, pengguna mengatur sistem sebelum digunakan. Pengaturan dilakukan untuk menentukan waktu, *baudrate*, kunci dan alamat komunikasi radio. RTC berfungsi untuk menunjukan waktu nyata dimana akan digunakan untuk melakukan pergantian kunci pada waktu-waktu tertentu maka waktu antara pemancar dan penerima harus sama. Terakhir komunikasi nirkabel perangkat ini menggunakan modul radio untuk mengirimkan data yang telah dienkripsi. Diagram blok sistem dari CRYPTOBLE ditunjukkan pada Gambar 3.1.



Gambar 3.1 Diagram Blok Sistem CRYPTOBLE

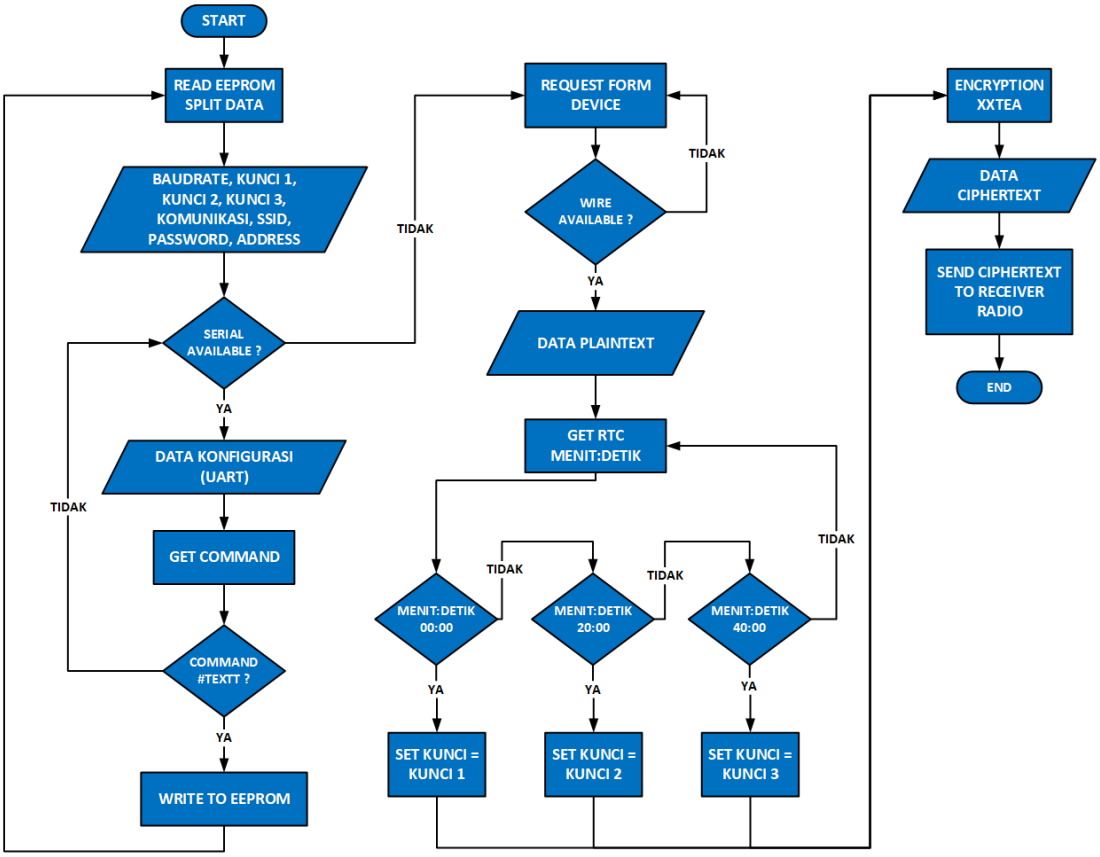
Komunikasi antara perangkat ke aplikasi dan perangkat ke perangkat *input*/*output* menggunakan komunikasi *Universal Synchronous Asynchronous Receiver Transmitter* (USART). Skematik dari CRYPTOBLE ditunjukkan pada Gambar 3.2.



Gambar 3.2 Skematik CRYPTOBLE

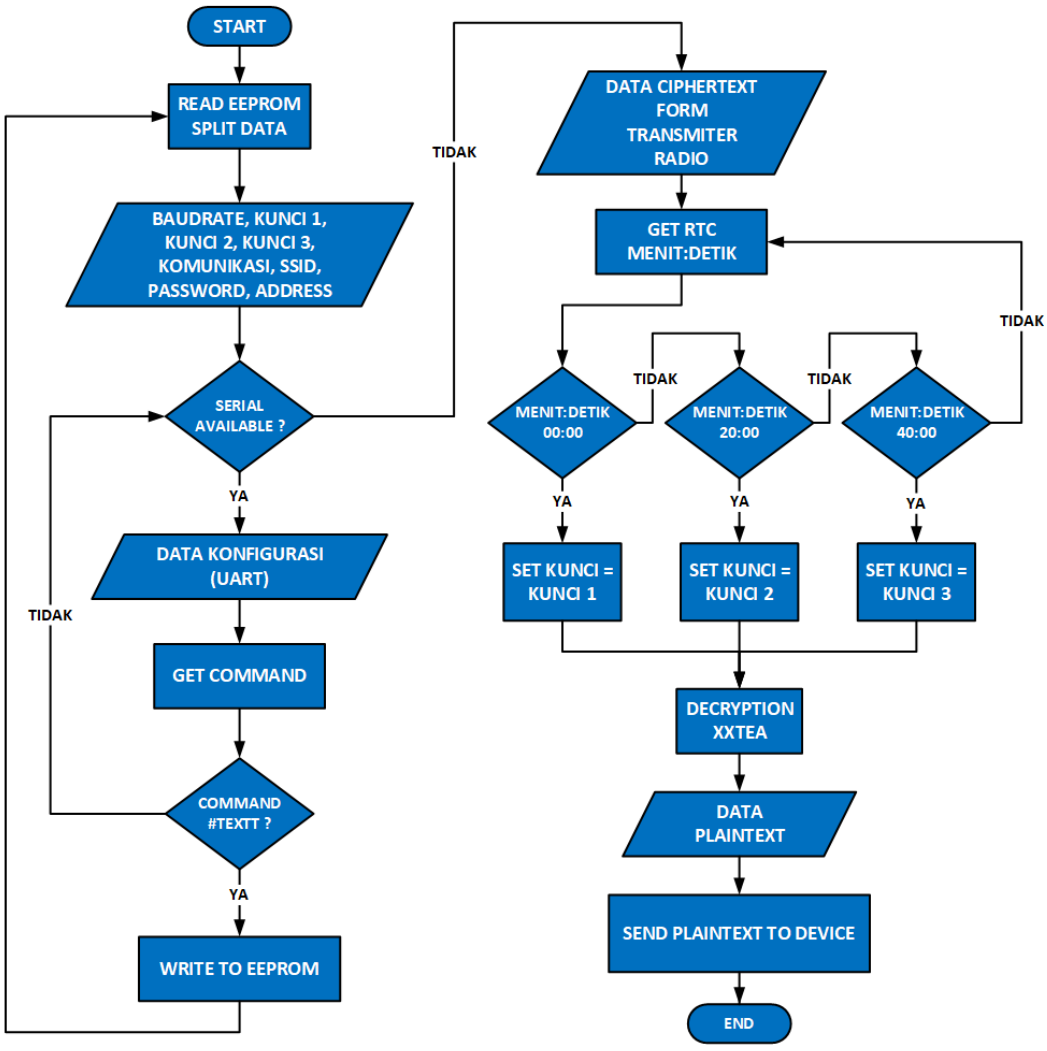
3.2 *Flowchart* Perangkat CRYPTOBLE

Cara kerja CRYPTOBLE dimulai dari mengatur sistem melalui antarmuka. Pertama pengguna menghubungkan aplikasi dengan perangkat menggunakan kabel melalui laptop/PC dan menentukan waktu, *baudrate*, kunci, dan alamat radio. Setelah itu sistem akan menerima pengaturan tersebut dan menyimpannya dalam *Electrically Erasable Programmable Read Only Memory* (EEPROM). Pengaturan ini dilakukan pada perangkat pemancar dan penerima dengan pengaturan yang sama dan CRYPTOBLE dapat digunakan. Selama proses penggunaan, CRYPTOBLE akan menunggu data masuk dari perangkat *input* yang terhubung melalui *port* USART yang disediakan. Ketika data diterima, CRYPTOBLE memeriksa waktu yang ditunjukkan RTC dan melakukan proses acak kunci untuk menentukan kunci. Data *plaintext* akan dienkripsi menggunakan kunci tersebut kedalam bentuk *ciphertext* dan dikirim melalui modul radio menuju perangkat penerima. *Flowchart* CRYPTOBLE pemancar ditunjukkan pada Gambar 3.3.



Gambar 3.3 *Flowchart Encryptor* CRYPTOBLE

Pada perangkat penerima, setelah data *ciphertext* diterima maka akan kembali dilakukan pemeriksaan waktu dan proses acak kunci untuk menyamakan kunci dari perangkat pemancar. *Ciphertext* yang diterima tadi akan didekripsi menggunakan kunci yang sama dan dikirim menuju perangkat *monitoring* yang terhubung oleh perangkat CRYPTOBLE penerima. *Flowchart* CRYPTOBLE penerima ditunjukkan pada Gambar 3.4.

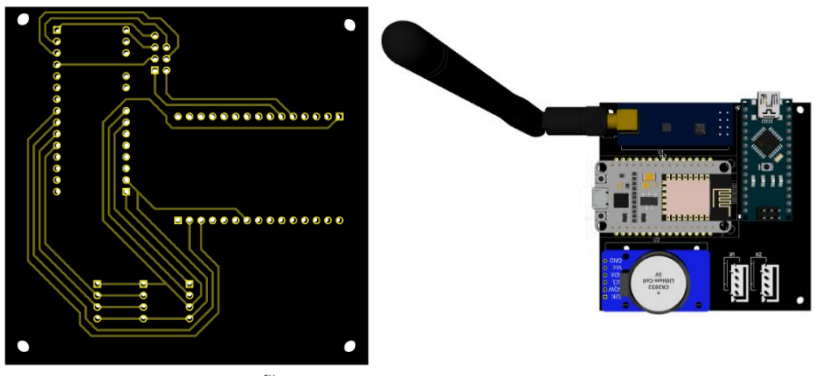


Gambar 3.4 *Flowchart Decryptor* CRYPTOBLE

Proses diatas akan terus berulang selama CRYPTOBLE digunakan dan pengaturan yang telah dilakukan pertama kali oleh pengguna akan tetap tersimpan pada EEPROM sehingga pengguna tidak perlu mengatur ulang sistem dari awal ketika ingin menggunakan CRYPTOBLE pada perangkat lainnya.

3.3 Ilustrasi Perangkat CRYPTOBLE

CRYPTOBLE dirancang sebagai produk yang *portable* atau mudah dipindahkan dari suatu perangkat ke perangkat lainnya. Material dari *case* CRYPTOBLE terbuat dari plastik. Desain PCB dari perangkat ini memiliki ukuran kurang lebih 8×8 cm^2. Ilustrasi PCB dan 3D perangkat CRYPTOBLE ditunjukkan pada Gambar 3.5.



Gambar 3.5 Ilustrasi Desain PCB dan 3D Perangkat CRYPTOBLE

Desain fisik dikemas dalam *case* dengan dimensi sekitar $9 \times 8.5 \times 3$ cm^3. Terdapat beberapa lubang untuk *port* komunikasi yang tersedia. Pada bagian atas terdapat *port* untuk komunikasi CRYPTOBLE dengan perangkat *input* dan bagian samping terdapat *port* untuk konfigurasi atau pengaturan sistem CRYPTOBLE. Ilustrasi 3D *case* perangkat CRYPTOBLE ditunjukkan pada Gambar 3.6.

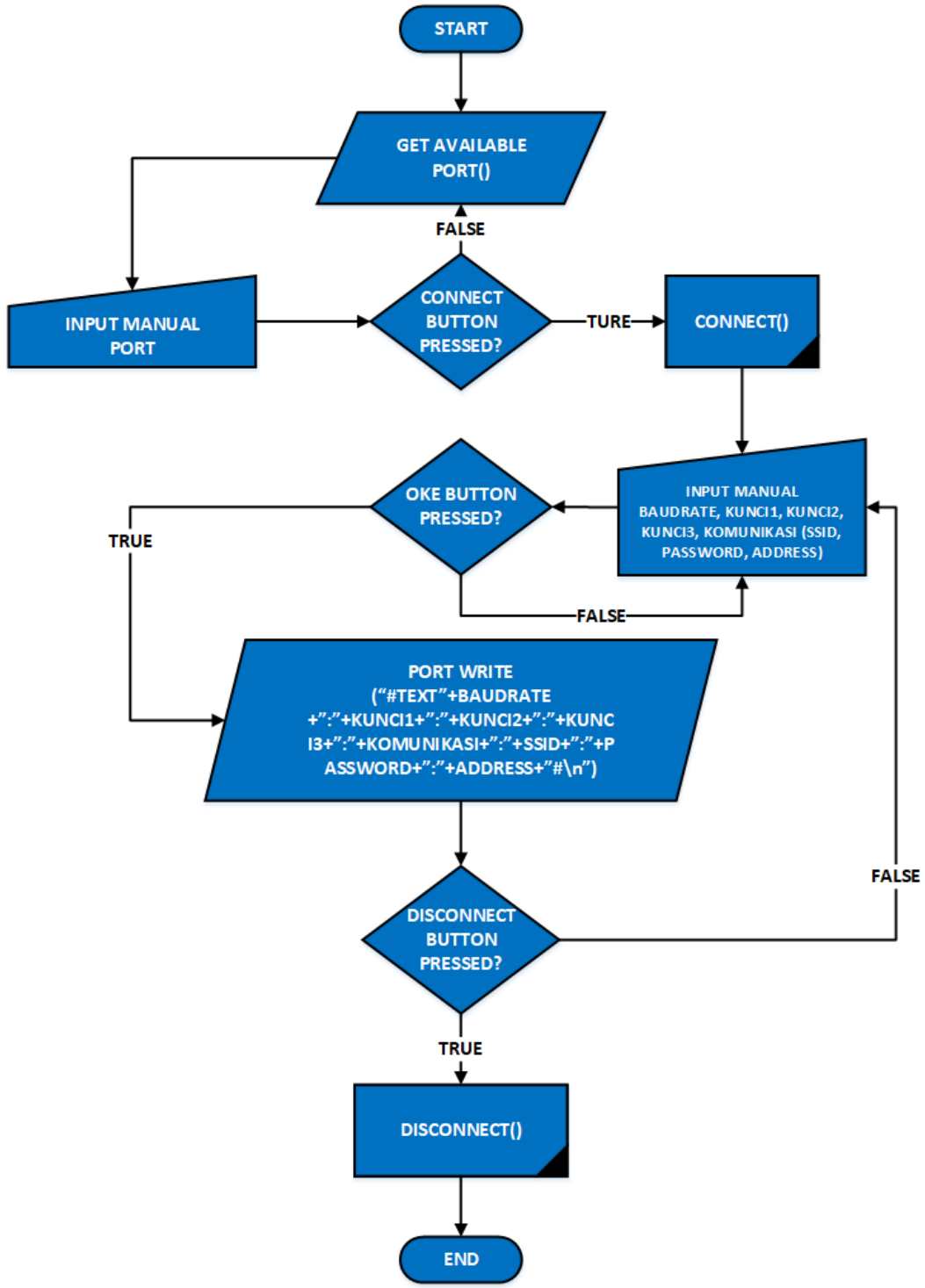
Gambar 3.6 Ilustrasi 3D *Case* Perangkat CRYPTOBLE

3.4 Perancangan CRYPTOBLE Configuration

CRYPTOBLE dilengkapi dengan aplikasi konfigurasi untuk mengatur sistem sebelum digunakan. Aplikasi ini diberi nama CRYPTOBLE Configuration. Aplikasi akan dibuat menggunakan *tools development* dari Windows, yaitu Visual Studio. Visual Studio menggunakan bahasa *C#*. Perancangan aplikasi ini harus memenuhi beberapa fitur, diantaranya terdapat kolom *PORT* dan *BAUDRATE* sebagai fitur konfigurasi perangkat untuk mengatur *baudrate*. Terdapat kolom *KUNCI1*, *KUNCI2*, dan *KUNCI3* sebagai fitur kata kunci untuk memasukkan kunci yang akan digunakan pada proses enkripsi data. Terdapat kolom *SSID*, *PASSWORD*, dan *ADDRESS* sebagai fitur konfigurasi komunikasi nirkabel untuk memasukan data konfigurasi komunikasi nirkabel yang digunakan pada CRYPTOBLE. Setelah konfigurasi dilakukan oleh pengguna maka pengaturan konfigurasi tersebut dikirim melalui komunikasi serial.

3.5 *Flowchart* CRYPTOBLE Configuration

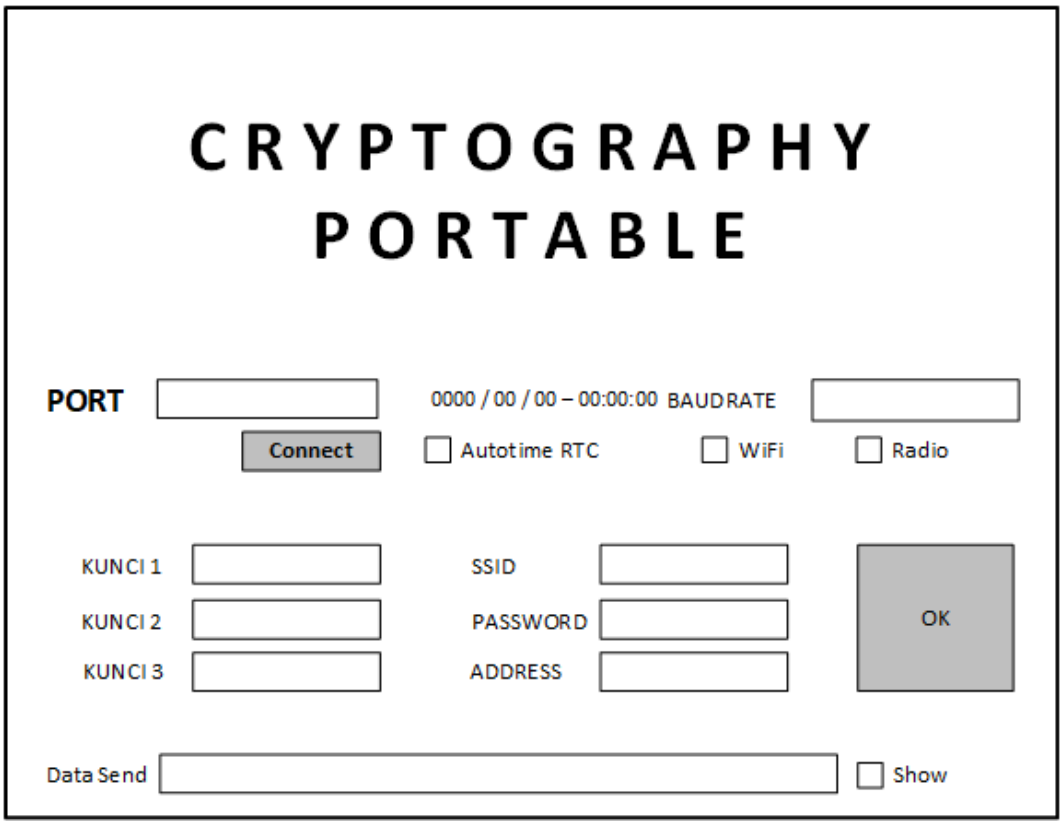
Aplikasi CRYPTOBLE Configuration dapat digunakan pada laptop/PC berbasis Windows. Ketika ingin melakukan pengaturan, pertama pengguna menghubungkan laptop/PC dengan perangkat CRYPTOBLE menggunakan kabel USB. Ketika dijalankan CRYPTOBLE Configuration akan mendeteksi komunikasi serial yang terhubung dengan laptop/PC. Jika komunikasi serial tersedia maka muncul pada kolom *PORT* nama dari komunikasi serial tersebut, contoh “COM 3”. Pengguna memilih komunikasi serial dari CRYPTOBLE dan menekan tombol *Connect* sehingga membuka jalur serial antara laptop/PC dengan CRYPTOBLE untuk mengirimkan data. Selanjutnya pengguna memasukkan data-data konfigurasi yang diperlukan seperti *baudrate*, kunci 1, kunci 2, kunci 3, dan komunikasi nirkabel yang akan digunakan dan menekan tombol OK untuk mengirimkan data-data konfigurasi tersebut ke CRYPTOBLE. Terakhir pengguna menekan tombol *Disconnect* untuk menutup jalur komunikasi serial. *Flowchart* konfigurasi aplikasi CRYPTOBLE Configuration ditunjukkan pada Gambar 3.7.



Gambar 3.7 *Flowchart* Konfigurasi Aplikasi CRYPTOBLE Configuration

3.6 Ilustrasi CRYPTOBLE Configuration

Sesuai dengan perancangan aplikasi CRYPTOBLE Configuration, ilustrasi desain aplikasi CRYPTOBLE Configuration ditunjukkan pada Gambar 3.8.



Gambar 3.8 Ilustrasi Desain Aplikasi CRYPTOBLE Configuration

Ilustrasi perancangan aplikasi memenuhi beberapa fitur, diantaranya terdapat kolom *PORT* dan *BAUDRATE* sebagai fitur konfigurasi perangkat untuk mengatur *baudrate*. Terdapat kolom *KUNCI1*, *KUNCI2*, dan *KUNCI3* sebagai fitur kata kunci untuk memasukkan kunci yang akan digunakan pada proses enkripsi data. Terdapat kolom *SSID*, *PASSWORD*, dan *ADDRESS* sebagai fitur konfigurasi komunikasi nirkabel untuk memasukan data konfigurasi komunikasi nirkabel yang digunakan pada CRYPTOBLE. Setelah konfigurasi dilakukan oleh pengguna maka pengaturan konfigurasi tersebut dikirim melalui komunikasi serial.