BAB II
TINJAUAN PUSTAKA

2.1 Komunikasi Radio

Komunikasi radio merupakan salah satu teknologi komunikasi nirkabel yang memanfaatkan gelombang radio sebagai media. Komunikasi radio menggunakan gelombang radio untuk mengirim informasi dari pemancar menuju penerima. Perangkat radio untuk komunikasi terdiri atas tiga bagian utama, yaitu pesawat radio, antenna, dan catu daya. Pesawat radio merupakan salah satu bagian dengan fungsi sebagai pengirim dan penerima informasi dalam bentuk gelombang [6]. Terdapat tiga teknik komunikasi, yaitu:

- *Simplex*

  Simplex merupakan teknik komunikasi yang mengandalkan satu arah saja. Artinya pemancar hanya mampu mengirim informasi dan penerima hanya mampu menerima informasi [7].
- *Half Duplex*

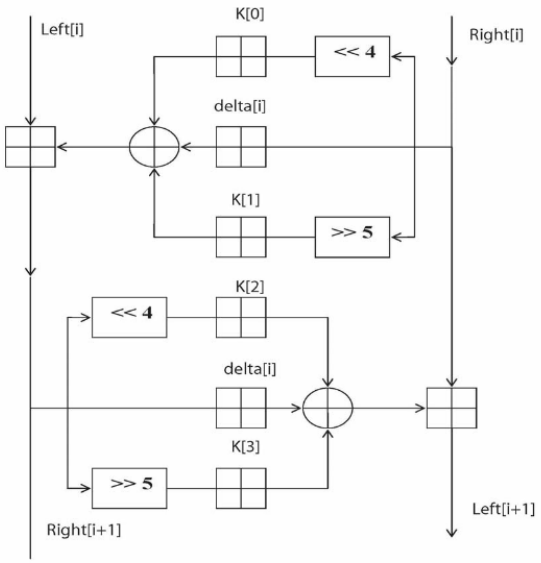
  Half duplex merupakan teknik komunikasi dua arah dengan saling bergantian. Teknik komunikasi ini biasa dijumpai pada perangkat *walkie-talkie* dimana perangkat tersebut hanya dapat mengirim informasi secara bergantian. Contoh terdapat dua orang yang berkomunikasi menggunakan *walkie-talkie*, ketika A sebagai orang yang berbicara maka yang B mendengarkan dan ketika B berbicara maka A yang mendengarkan. Jika kedua orang tersebut berbicara dalam waktu bersamaan maka tidak dapat terjadi komunikasi [7].
- *Full Duplex*

  Full duplex merupakan teknik komunikasi dua arah secara utuh dimana pengirim dan penerima dapat berkomunikasi dua arah dalam waktu yang sama [7].

2.2 Kriptografi *Corrected Block Tiny Encryption Algorithm* (XXTEA)

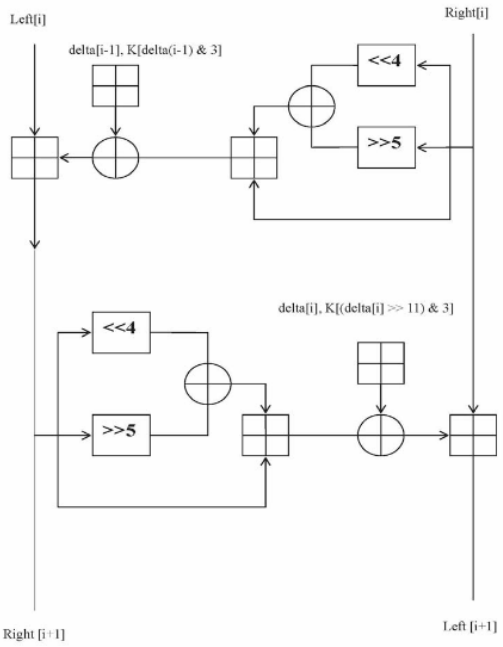
Kriptografi berasal dari Bahasa Yunani: "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan). Ada beberapa definisi kriptografi yang telah dikemukakan dalam berbagai literatur. Namun terdapat dua definisi kriptografi saat ini, yaitu menurut Schneier (1996), Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan [8] dan menurut Menez (1996), Kritografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [9]. Di dalam kriptografi terdapat istilah, seperti *plaintext* dan *ciphertext*. *Plaintext* adalah data atau informasi yang dapat dibaca dan dimengerti maknanya, sedangkan *ciphertext* adalah bentuk pesan yang telah disandikan ke bentuk lain agar pesan tidak dapat dimengerti maknanya oleh pihak lain [10].

Tiny Encryption Algorithm (TEA) merupakan algoritma kriptografi *block cipher* dengan ukuran blok 64-*bit* dan 128-*bit* [11]. Hal yang paling menonjol dari TEA adalah kesederhanaan dalam implementasi, kecepatan proses enkripsi, dan kecepatan proses dekripsi. TEA berbasiskan jaringan *feistel* dan memiliki 32 putaran. Pemodelan jaringan *feistel* sebagai dasar pada algoritma TEA ditunjukkan pada Gambar 2.1.



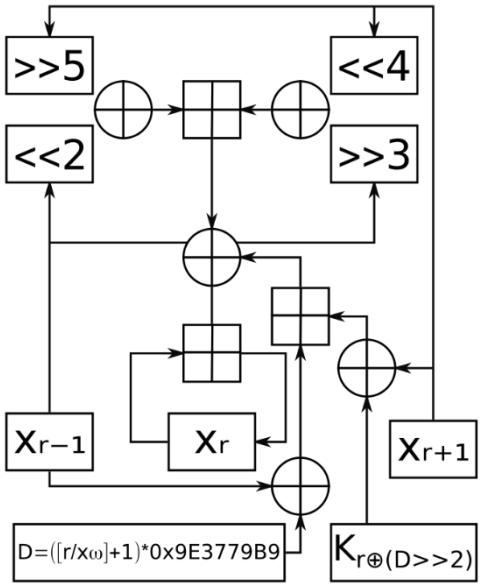
Gambar 2.1. Struktur Jaringan *Feistel* TEA [12]

Algoritma turunan dari TEA adalah *eXtended* TEA (XTEA) yang juga beroperasi dalam ukuran blok 64-*bit* dan panjang kunci 128-*bit*. Karena memiliki kesederhanaan dalam penjadwalan kuncinya, maka algoritma TEA memiliki kerentanan terhadap *equivalent key* [11]. Untuk menutupi kelemahan algoritma TEA tersebut maka diciptakan algoritma XTEA dengan penjadwalan kunci dan jaringan *feistel* yang lebih kompleks dibandingkan dengan TEA. XTEA masih dapat dianggap sebagai algoritma kriptografi yang aman asalkan ronde yang digunakan tidak kurang dari 32 [11]. Pemodelan jaringan *feistel* sebagai dasar pada algoritma XTEA ditunjukkan pada Gambar 2.2.



Gambar 2.2 Struktur Jaringan *Feistel* XTEA [12]

Selanjutnya terdapat algoritma *Corrected Block* TEA (XXTEA) yang juga turunan dari blok TEA (Algoritma berbasis XTEA yang dapat dioperasikan pada blok sebesar apapun). Pemodelan jaringan *feistel* sebagai dasar pada algoritma XXTEA ditunjukkan pada Gambar 2.3.

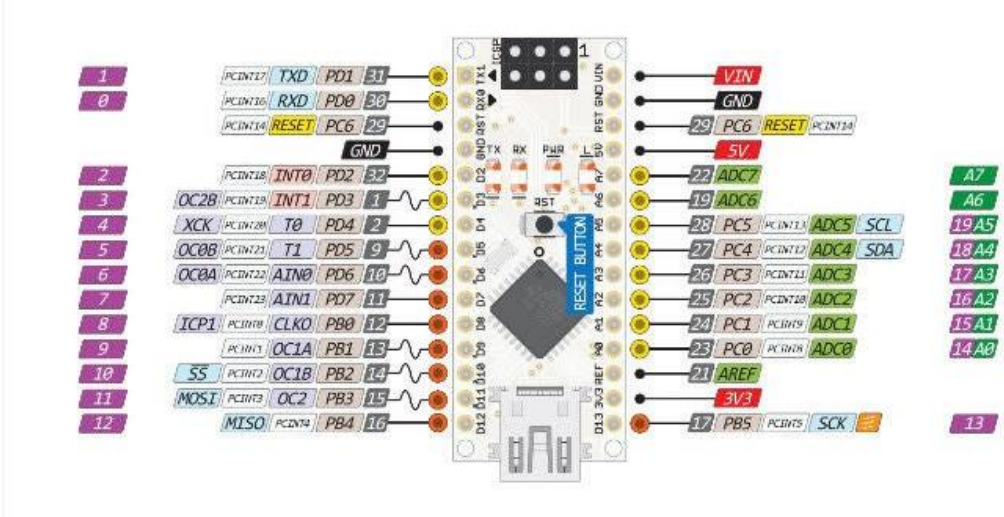


Gambar 2.3 Struktur Jaringan *Feistel* XXTEA [13]

Saarinen (1998) mengungkapkan bahwa terdapat kelemahan dalam proses dekripsi TEA sehingga XXTEA dikeluarkan untuk menutupi kelemahan tersebut [11]. XXTEA juga mempunyai jaringan *feistel* yang tidak seimbang atau disebut dengan UFN (*Unbalance Feistel Network*).

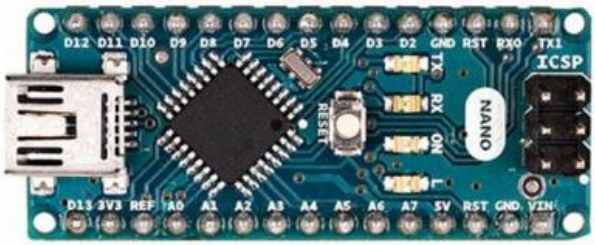
2.3 Mikrokontroler Arduino Nano

Arduino merupakan mikrokontroler *open-source* yang sudah dirangkai lengkap dengan sistem minimum. Arduino diprogram menggunakan Arduino *Software Integrated Development Environment* (IDE) dalam bahasa *C* sehingga mudah digunakan dan dimengerti. Arduino dapat mengolah *input*, seperti sensor cahaya, sensor gerak, tombol atau pesan suara. *Input* tersebut akan diolah dan menghasilkan *output* sesuai yang diinginkan, seperti mengaktifkan motor, menyalakan lampu, mengeluarkan suara serta mengirim pesan menuju perangkat lainnya. Arduino mempunyai beberapa model papan salah satu mikrokontroler Arduino Nano. Pin diagram dari mikrokontroler Arduino Nano ditunjukkan pada Gambar 2.4.



Gambar 2.4 Pin Diagram Arduino Nano [14]

Menggunakan *chip* mikrokontroler ATmega328 dan dikemas dalam ukuran yang kecil mikrokontroler ini sangat cocok untuk *project* berskala kecil. Arduino Nano dibekali dengan 32 KB *flash memory* (2 KB digunakan untuk *bootloader*), 16 MHz *clock speed*, dan memiliki 20 pin I/O [15]. Mikrokontroler Arduino Nano ditunjukkan pada Gambar 2.3.



Gambar 2.5 Mikrokontroler Arduino Nano [15]

Spesifikasi dari mikrokontroler Arduino Nano ditunjukkan pada Tabel 2.1.

Tabel 2.1 Spesifikasi Mikrokontroler Arduino Nano [15]

Microcontroller	ATmega328
Operating Voltage	5 V
Input Voltage	7 – 12 V
Flash Memory	32 KB (2 KB *bootloader*)
SRAM	2 KB

Clock Speed	16 MHz
EEPROM	1 KB
DC Current per* I/O *pins	40 mA
Analog IN pins	8
Digital* I/O *pins	22 (6 PWM)
Input Voltage	7 – 12 V

2.4 Modul Radio NRF24l01 PA LNA

Modul NRF24l01 PA LNA digunakan untuk komunikasi jarak jauh dengan menggunakan frekuensi gelombang radio sebesar 2,4 – 2,5 GHz *Industrial*, *Scientific*, *and Medical* (ISM). Modul *wireless* NRF24L01 PA LNA memiliki kecepatan hingga 2 Mbps dengan beberapa opsi *date rate* 250 Kbps, 1 Mbps dan 2 Mbps. Modul ini bisa digunakan sebagai *transmitter* dan *receiver* yang terdiri dari *synthesizer* frekuensi terintegrasi, kekuatan *amplifier*, osilator kristal, *demodulator*, *modulator*, dan *enhanced Shockburst*™ mesin protokol. Pada bagian *output* daya, saluran frekuensi, dan *setup protocol* yang mudah dieksekusi program melalui antarmuka *Serial Peripheral Interface* (SPI). Konsumsi arus yang digunakan sangat rendah, hanya sebesar 0,9 mA pada daya *output* sebesar -6 dBm dan 12.3 mA dalam *mode* RX atau mode *receiver* [16]. Modul NRF24L01 PA LNA ditunjukkan pada Gambar 2.6.

Gambar 2.6 Modul NRF24l01 PA LNA

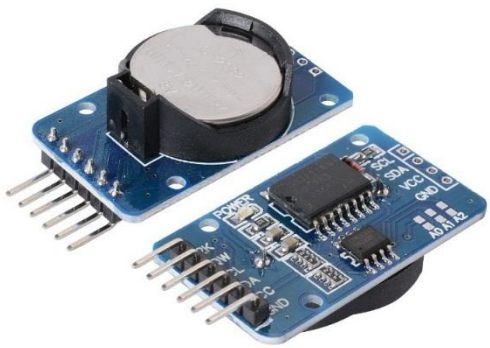
Spesifikasi modul NRF24l01 ditunjukkan pada Tabel 2.2.

Tabel 2.2 Spesifikasi Modul NRF24l01 PA LNA

Parameter	Value	Unit
Minimum supply voltage	1.9	V
Maximum output power	0	dBm
Maximum data rate	2000	Kbps
Supply current in TX mode @ 0 dBm output power	11.3	mA
Supply current in RX mode @ 2000 kbps	12.3	mA
Temperature range	$-40\ to + 85$	℃
Sensitivity @ 1000 kbps	-85	dBm
Supply current in Power Down mode	900	nA

2.5 Modul *Real Time Clock* DS3231

Modul RTC DS3231 adalah *Realtime Clock* (RTC) dengan kompensasi suhu kristal osilator yang terintegrasi (TCX0). TCX0 ini menyediakan sebuah *clock* referensi yang stabil, akurat, dan memelihara akurasi RTX sekitar ± 2 menit pertahun. Modul DS3231 menyediakan waktu dan kalender dengan dua waktu alarm dalam satu hari dan keluaran gelombang persegi yang dapat diprogram. Waktu dan kalender memberikan informasi tentang detik, menit, jam, hari, tanggal, bulan, dan tahun yang terdapat ada register internal dan dapat diakses menggunakan komunikasi *Inter Integrated Circuit* (I2C). RTC DS3231 ditunjukkan pada Gambar 2.7.



Gambar 2.7 Modul RTC DS3231

Spesifikasi modul RTC DS3231 ditunjukkan pada Tabel 2.3.

Tabel 2.3 Spesifikasi Modul RTC DS3231

Features	• RTC count seconds, minutes, hours, date of the month, month, day of the week, and year. • Fast (400 KHz) I2C Interface • Baterry-backup
Accurate	Accuracy ± 2 ppm @ 0 ºC to +40 ºC Accuracy $\pm 3{,}5$ ppm @ -40 ºC to +85 ºC
Operating Voltage	3,3 V
Operating Temperature	Commercial 0 ºC to +70 ºC Industrial -40 ºC to +85 ºC