Rancang Bangun Sistem Enkripsi Sebagai *Security* Komunikasi *Handie-Talkie* (Ht) Menggunakan Mikrokontroler Avr Seri

Mona Arif Muda[1] , M.Komarudin[1] , Yunita Susanty[2]
1. Jurusan Teknik Elektro Universitas Lampung
2. Alumni Jurusan Teknik Elektro Universitas Lampung
Jl. Prof. Dr. Sumantri Brojonegoro No.1 Bandar Lampung
mamba@unila.ac.id, komar@unila.ac.id

Abstrak--Keamanan telah menjadi aspek yang sangat penting dari suatu sistem informasi. Kriptografi dapat digunakan sebagai sistem keamanan yang dapat melindungi sistem informasi tersebut. Dalam teknik kriptografi informasi yang akan dikirim adalah berupa data yang telah diacak dengan menggunakan kunci. Hal inilah yang disebut dengan sistem enkripsi. Dengan demikian informasi hanya dapat diterima oleh pihak yang mempunyai kunci yang sama. Penelitian dilakukan dengan membuat perangkat sistem enkripsi pada *Handie-Talkie* (HT) yang terdiri atas rangkaian HT pengirim dan perangkat lunak sistem enkripsi. Penelitian ini diawali dengan mempelajari berbagai literatur yang terkait dengan sistem enkripsi yang digunakan pada teknik kriptografi. Dan berdasarkan literatur yang dibaca, dibuat rancangan rangkaian dan rancangan program sistem enkripsi pada HT. Hasil rancangan tersebut kemudian direalisasikan dengan membuat rangkaian sistem enkripsi HT melalui program aplikasi. Hasil yang diperoleh dari penelitian ini adalah sistem enkripsi yang dibuat pada HT telah mampu mengacak informasi asli yang dalam hal ini berupa frekuensi suara manusia dan mampu mentransmisikan data hasil enkripsi tersebut dengan berbagai keterbatasan. Dalam hal ini *baud rate* 1200 bps tidak mendukung *range* fekuensi suara manusia. *Baud rate* yang dibutuhkan agar bisa mentransmisikan frekuensi suara manusia adalah sebesar 80Kbps. Dengan *baud rate* yang ada (1200 bps) aplikasi yang mendukung adalah masukan data digital yang berasal dari *keypad.*

Kata kunci: *Handie Talkie*, kriptografi, enkripsi, *keypad*

Abstract--*Security has become the most important aspect in information system. Cryptography can be used as security system to secure the information system. In this cryptography technique, information will be sent as a random data by using the key. This is called encryption. Thus, the information will be only received by others who have the same key. This research was done by designing encryption system tools on HT that consist of transmitter HT circuit and encryption system program. Begun by learning several literatures related to encryption system which is used in cryptography technique. Based on these literatures, then, made a design of circuit and encryption system program on HT. Furthermore, a realization of these designs was made by establishing the encryption system circuit of HT via application program. The result is HT encryption system that is able to randomize the original information in human sound frequency form and with several limits, it is able to transmit the data from encryption system. In this case, the baudrate of 1200 bps cannot support the range of human sound frequency. In order to transmit it, the baudrate of 80 Kbps is required. With the baudrate of 1200 bps, its supporting application is digital data input which is provided by the keypad.*

Keywords*: Handie-Talkie, cryptography, encryption, keypad*

A. Pendahuluan

Keamanan telah menjadi aspek yang sangat penting dari suatu sistem informasi. Sebuah informasi umumnya hanya ditujukan bagi segolongan tertentu. Oleh karena itu sangat penting untuk mencegahnya jatuh kepada pihak-pihak lain yang tidak berkepentingan. Untuk melaksanakan tujuan tersebutlah dirancang suatu sistem keamanan yang berfungsi melindungi sistem informasi

Mengacu pada permasalahan yang ada maka perumusan perancangan ini ditekankan pada aspek berikut :

1. Bagaimana membuat rangkaian *pre-amplifier* yang berfungsi sebagai

Naskah ini diterima pada tanggal 29 Mei 2007, direvisi tanggal 1 Juli 2007 dan disetujui untuk diterbitkan tanggal 1 Agustus 2007.

penguat sinyal agar sesuai dengan *input level* tegangan ADC.
2. Bagaimana membuat program konversi ADC *(Analog to Digital Converter)* yang mampu mengubah sinyal analog yang berasal dari *output pre-amplifier* menjadi data digital 8 bit dan merancang program agar data hasil konversi tersebut bisa dikirim secara serial.
3. Bagaimana membuat program sistem enkripsi sebagai sistem *security* dengan menggunakan kunci yang sama dengan sistem dekripsi agar data yang akan dikirimkan tidak bisa di deteksi oleh pihak lain yang tidak mempunyai kunci yang sama.
4. Bagaimana membuat rangkaian modulator FSK agar sinyal informasi yang hasilkan dapat di transmisikan melalui HT.

Perancangan sistem enkripsi sebagai komunikasi HT dibatasi pada hal-hal berikut:
1. Tidak membahas secara detail perangkat-perangkat yang membangun pesawat komunikasi HT secara keseluruhan. Besaran yang masuk (yang diterima) dan yang dihasilkan pada pesawat komunikasi HT dikondisikan melalui *line microphone* dan *speaker* yang ada pada PTT (*Push To Talk*) eksternal.
2. Besaran yang dikondisikan dalam sistem enkripsi ini adalah berupa sinyal analog yang dihasilkan melalui sumber (*source*) yang diubah menjadi bentuk pulsa-pulsa listrik atau gelombang elektromagnetik.
3. Frekuensi suara manusia yang dikondisikan berada pada *range* 300 hingga 3400 Hz sedangkan frekuensi yang dihasilkan manusia umumnya 100-7500 Hz.
4. Sistem enkripsi yang diimplementasikan dalam perangkat HT tidak memperhitungkan adanya *error detection* dan *error recovery* yang mungkin bisa terjadi.
5. Untuk langkah awal, sistem enkripsi yang digunakan pada HT diupayakan dalam jarak komunikasi yang relatif dekat hingga semaksimal mungkin (sesuai dengan spesifikasi perangkat HT yang digunakan).

Perancangan ini memiliki manfaat-manfaat sebagai berikut :
1. Dapat menjaga keamanan dan keterjaminan informasi yang disampaikan dari sumber (*source*) ke tujuan (*destination*) tanpa diketahui oleh pihak-pihak yang tidak diharapkan melalui perangkat sederhana HT.
2. Dapat mengembangkan penerapan teknologi khususnya teknologi berbasis *security* melalui sistem enkripsi pada perangkat HT.

B. Tinjauan Pustaka

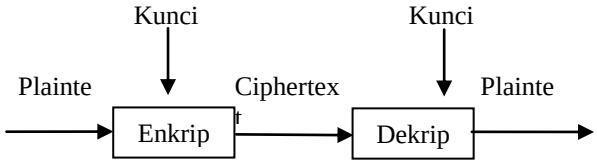
Teori Sistem Enkripsi dan Dekripsi

Salah satu upaya pengamanan sistem informasi yang dapat dilakukan adalah kriptografi. Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi, antara lain seperti kerahasiaan, integritas data, otentikasi, dan ketiadaan penyangkalan. Keempat aspek tersebut merupakan tujuan fundamental dari suatu sistem kriptografi.

Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. *Ciphertext* inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, *ciphertext* tersebut ditranformasikan kembali ke dalam bentuk *plaintext* agar dapat dikenali.

Proses tranformasi dari *plaintext* menjadi *ciphertext* disebut proses *Encipherment* atau enkripsi (*encryption*), sedangkan proses mentransformasikan kembali *ciphertext* menjadi *plaintext* disebut proses dekripsi (*decryption*).

Untuk mengenkripsi dan mendekripsi data, kriptografi menggunakan suatu algoritma (*cipher*) dan kunci (*key*). *Cipher* adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data. Secara sederhana istilah-istilah di atas dapat digambarkan sebagai berikut:



Gambar 1. Proses enkripsi/dekripsi sederhana

Secara umum operasi enkripsi dan dekripsi dapat diterangkan secara matematis sebagai berikut :

EK (M) = C (Proses Enkripsi)
DK (C) = M (Proses Dekripsi)

Pada saat proses enkripsi kita menyandikan pesan M dengan suatu kunci K lalu dihasilkan pesan C. Sedangkan pada proses dekripsi, pesan C tersebut diuraikan dengan menggunakan kunci K sehingga dihasilkan pesan M yang sama seperti pesan sebelumnya.

Dengan demikian keamanan suatu pesan tergantung pada kunci ataupun kunci-kunci yang digunakan, dan tidak tergantung pada algoritma yang digunakan. Sehingga algoritma-algoritma yang digunakan tersebut dapat dipublikasikan dan dianalisis, serta produk-produk yang menggunakan algoritma tersebut dapat diproduksi massal. Tidaklah menjadi masalah apabila seseorang mengetahui algoritma yang kita gunakan. Selama ia tidak mengetahui kunci yang dipakai, ia tetap tidak dapat membaca pesan.

Teknik kriptografi yang digunakan pada sistem enkripsi ini adalah Kriptografi Vigenere. Kunci pada kriptografi Vigenere adalah sebuah kata bukan sebuah huruf. Kata kunci ini akan dibuat berulang sepanjang *plaintext*, sehingga jumlah huruf pada kunci akan sama dengan jumlah huruf pada *plaintext*. Pergeseran setiap huruf pada *plaintext* akan ditentukan oleh huruf pada kunci yang mempunyai posisi yang sama dengan huruf pada *plaintext*. Kriptografi Vigenere ini dikenal sebagai *polyalphabetic substitution cipher*, karena enkripsi terhadap satu huruf yang sama bisa menghasilkan huruf yang berbeda.

Pergeseran setiap huruf pada *plaintext* ditentukan oleh huruf pada posisi yang sama

Tabel 1. Tabel pergeseran huruf pada kriptografi Vigenere

Kunci	A	B	C	D	E	F	G	H	I
Pergeseran k	0	1	2	3	4	5	6	7	8
Kunci	J	K	L	M	N	O	P	Q	R
Pergeseran k	9	10	11	12	13	14	15	16	17
Kunci	S	T	U	V	W	X	Y	Z	
Pergeseran k	18	19	20	21	22	23	24	25	

Pesawat Komunikasi Multiarah

Pesawat komunikasi multiarah merupakan pesawat yang bisa digunakan untuk memancarkan dan juga bisa untuk menerima sinyal-sinyal elektromagnetik pada jalur komunikasi tertentu. Pesawat ini sering disebut peawat "*transceiver*" yang berasal dari kata *transmitter* (memancar) dan *receiver* (menerima). Jadi, alat ini dapat digunakan untuk pembicaraan secara langsung.

Bentuk yang paling sederhana dari pesawat *transceiver* ini adalah *walky talky* yang secara sederhana hanya mampu untuk berkomunikasi kurang lebih 1 kilometer

saja. Bentuk lainnya yang lebih menjangkau adalah pesawat HT, CB (*Citizen Band*), 80 meter band, 11 meter band, dan sebagainya. Semua itu adalah bentuk pesawat *transceiver* yang sempurna. Sedang pada pesawat *Walky Talky* bukanlah pesawat komunikasi yang memadai karena hanya menggunakan penguat tunggal pada sistem modulatornya sehingga sifatnya hanya untuk permainan saja.

Selain bentuk-bentuk pesawat tersebut, sekarang ini orang lebih tertarik dengan pesawat *transceiver* jalur FM yang dirasa lebih bening dan enak didengarkan, disamping antena yang digunakan juga relatif sederhana. Hanya saja pesawat *transceiver* jalur FM ini tidak mampu menembus jarak sejauh pesawat *transceiver* jalur AM.

Modulator FSK (Frequency Shift Keying)

FSK merupakan sistem modulasi digital yang relatif sederhana. Fungsi FSK adalah merubah data biner menjadi isyarat dengan frekuensi tertentu untuk merepresentasikan biner 1 dan frekuensi yang lain untuk representasi biner 0. FSK merupakan sistem modulasi digital yang relatif sederhana. FSK biner adalah sebuah bentuk modulasi sudut dengan *envelope* konstan yang mirip dengan FM konvensional, kecuali bahwa dalam modulasi FSK, sinyal pemodulasi berupa aliran pulsa biner yang bervariasi diantara dua level tegangan *diskrit* sehingga berbeda dengan bentuk perubahan yang kontinyu pada gelombang analog.

Mikrokontroler AVR Seri ATmega8535

Atmel merupakan salah satu *vendor* yang mengembangkan dan memasarkan produk mikroelektronika yang telah menjadi suatu teknologi standar. Dan AVR (*Alf and Vegard's Risc Processor*) adalah suatu teknologi yang memiliki kapabilitas yang amat maju, tetapi dengan biaya ekonomis yang cukup minimal. Oleh karena itu, dipergunakan salah satu AVR produk Atmel, yaitu ATmega8535. selain karena mudah didapatkan dan murah, ATmega8535 juga memiliki fasilitas yang lengkap.

Arsitektur ATmega8535

ATmega8535 memiliki struktur bagian sebagai berikut :

a. Saluran I/O sebanyak 32 buah, yaitu Port A, Port B, Port C, dan Port D.
b. ADC 10 bit sebanyak 8 saluran
c. Tiga buah *Timer/Counter* dengan kemampuan perbandingan.
d. CPU yang terdiri atas 32 buah register.
e. *Watchdog Timer* dengan osilator internal.
f. SRAM sebesar 512 byte.
g. Memori *Flash* sebesar 8 kb dengan kemampuan *Read While Write*.
h. Unit interupsi internal dan eksternal.
i. Port antarmuka SPI
j. EEPROM sebesar 512 byte yang dapat diprogram saat operasi.
k. Antarmuka komparator analog.
l. Port USART untuk komunikasi serial.

Fitur ATmega8535

Kapabilitas detail dari ATmega8535 adalah sebagai berikut :

a. Sistem mikroprosesor 8 bit berbasis RISC dengan kecepatan maksimal 16 MHz.
b. Kapabilitas memori *flash* 8 KB, *SRAM* sebesar 512 byte, dan EEPROM (*Electrically Erasable Programmable read Only Memory*) sebesar 512 byte.
c. ADC internal dengan fidelitas 10 bit sebanyak 8 *channel.*
d. Portal komunikasi serial (USART) dengan kecepatan maksimal 2,5 Mbps.
e. Enam pilihan mode *sleep* menghemat penggunaan daya listrik.

Peta Memori

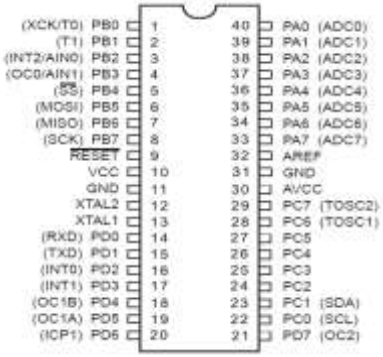
ATmega8535 memiliki 2 jenis memori utama yaitu:

a. Memori program Berfungsi untuk menyimpan program. Bersifat *non-volatile*. Memori yang digunakan adalah tipe *flash memory*. Kapasitasnya 8 kByte. Memori ini hanya digunakan untuk pemrograman.
b. Memori data Berfungsi untuk menyimpan data yang selanjutnya. Memori data masih terbagi menjadi 2 jenis lagi, yaitu jenis memori EEPROM *non-volatile*, dan data RAM *(volatile).*

Konfigurasi Pin ATmega8535

Konfigurasi pin ATmega8535 secara fungsional dapat dijelaskan sebagai berikut:

a. VCC merupakan pin yang berfungsi sebagai pin masukan catu daya.
b. GND merupakan pin *ground*
c. PORT A (PA0..PA7) merupakan I/O dua arah dan pin masukan ADC.
d. PORT B (PB0..PB7) merupakan I/O dua arah dan pin fungsi khusus, yaitu *Timer/ Counter*, komparator analog, dan SPI.
e. PORT C (PC0..PC7) merupakan pin I/O dua arah dan pin fungsi khusus, yaitu TWI, komparator analog, dan *Timer Oscilator*.
f. RESET merupakan pin yang digunakan untuk me-*reset* mikrokontroler.
g. XTAL1 dan XTAL2 merupakan pin masukan *clock* eksternal.
h. AVCC merupakan pin masukan tegangan untuk ADC.
i. AREF merupakan pin masukan tegangan referensi ADC.



Gambar 2. Konfigurasi pin ATmega8535

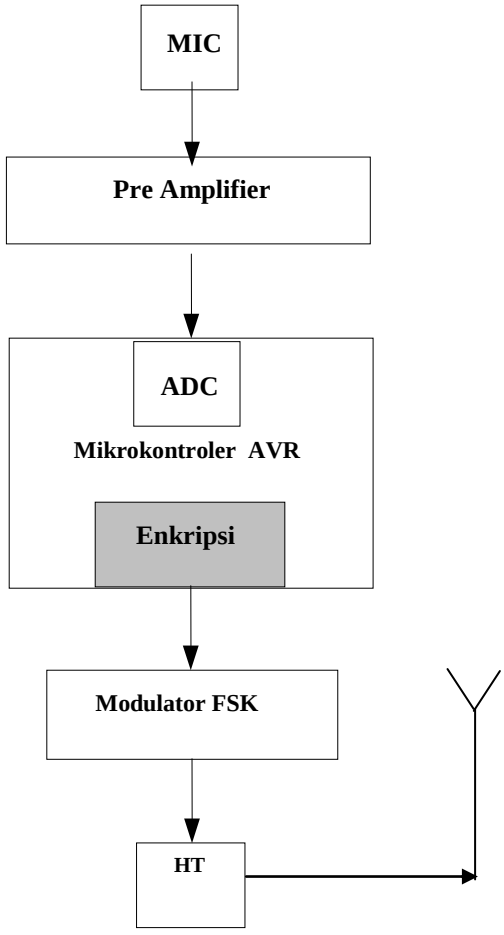
C. Metode Penelitian

Langkah-langkah Kerja Perancangan dan Realisasi Rangkaian

Langkah-langkah kerja yang dilakukan dalam perancangan dan realisasi sistem dekripsi sebagai basis *security* dan proteksi komunikasi HT menggunakan mikrokontroler AVR adalah sebagai berikut:

1. Studi literatur
2. Perancangan blok diagram rangkaian.
3. Implementasi rangkaian sistem enkripsi sebagai *security* komunikasi HT menggunakan mikrokontroler AVR seri ATmega8535.
4. Pengujian alat.
5. Analisis dan Kesimpulan

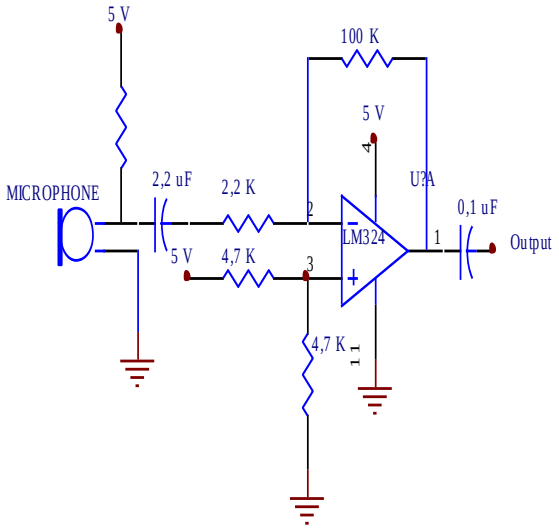
Diagram Blok Sistem Enkripsi HT



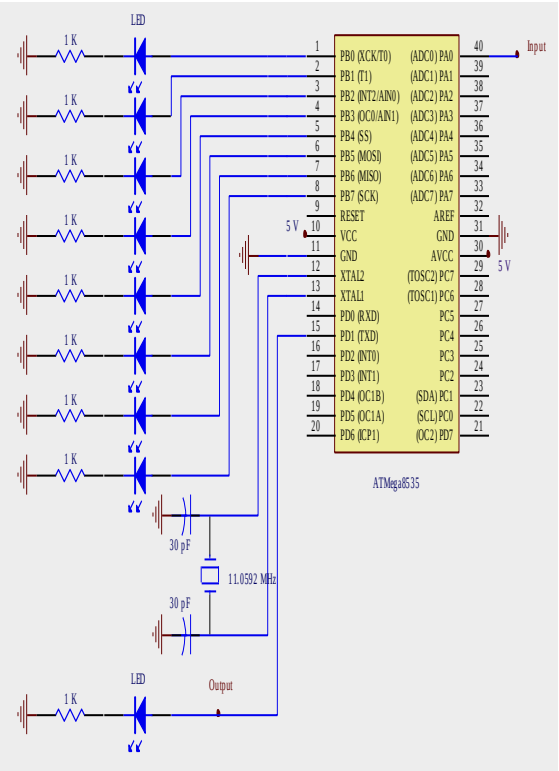
Gambar 3. Diagram blok sistem enkripsi pesawat komunikasi HT

Perancangan Rangkaian Sistem Enkripsi Pesawat Komunikasi HT

Pre-amplifier berfungsi untuk menguatkan sinyal untuk proses selanjutnya. *Input* yang digunakan pada rangkaian ini adalah sinyal analog yang berasal dari suara manusia.



Gambar 4. Rangkaian *pre-amplifier* dengan menggunakan LM324



Gambar 5. Rangkaian mikrokontroler untuk Sistem ADC dan enkripsi dengan menggunakan IC ATmega8535

Konversi ADC

Pin yang digunakan adalah PA0 yang pada mikrokontroler berfungsi sebagai input ADC. Pin ini menerima masukan dari rangkaian penguat. Keluaran dari ADC ini berupa sinyal digital yang akan dikirimkan dan diproses oleh mikrokontroler. Tegangan referensi ADC menggunakan tegangan internal mikrokontroler AVR (2,56 volt). Rentang keluaran yang dihasilkan adalah 0 sampai 255 karena ADC yang digunakan 8 bit.

Rumusan untuk menghitung hasil konversi adalah

$$Dout = \frac{Vin}{Vref} x2^n$$ Dout = nilai desimal output ADC

Pengiriman data ke modulator FSK melalui serial

Pin yang digunakan untuk melakukan fungsi ini adalah pin PD0 (Rx) dan PD2 (Tx). Komunikasi yang dilakukan hanya satu arah, yaitu dari perangkat mikrokontroler ke modulator FSK. Tetapi sebelum komunikasi ini terhubung perlu membangun komunikasi terlebih dahulu.

Ada beberapa hal yang perlu diperhatikan untuk membangun hal tersebut di mikrokontroler, yaitu nilai *baud rate* yang digunakan, *setting* format data *stop* bit, dan pengaturan beberapa register seperti RXEN, TXEN, dan RXCIE. Pengaturan *baud rate* dilakukan untuk mengatur kecepatan transfer data. Pengaturan *baud rate* dilakukan dengan memberikan nilai pada register UBRR. Register UBRR adalah register 16 bit sehingga terdiri atas UBRRH (UBRR *high*) dan UBRRL (UBRR *low*). Rumus yang digunakan adalah:

$$\text{Nilai UBRR} = \frac{Frekuensi\,kristal}{(16 * baud\_rate)} - 1$$

$$= \frac{11{,}0592MHz}{16 * 1200} - 1 = 575$$

Nilai UBRR di ubah menjadi bilangan heksa yaitu menjadi 23F sehingga nilai UBRRH 2 dan UBRRL 3F.

Algoritma konversi analog ke digital

Masukan sinyal analog sebelumnya dikuatkan terlebih dahulu tegangannya sehingga sesuai dengan tegangan masukan pada ADC. Masukan ini kemudian akan dikonversi ke sinyal digital.

Sebelum melakukan proses konversi ADC perlu dilakukan pengaturan register ADMUX dan ADCSRA. ADMUX merupakan register 8 bit yang berfungsi menentukan tegangan referensi ADC, format data keluaran, dan saluran ADC yang digunakan. Nilai konfigurasi ADMUX yang digunakan seperti tertera pada tabel 2.

Tabel 2. Nilai register ADMUX.

REFS1	**REFS0**	**ADLAR**	**MUX4**	**MUX3**	**MUX2**	**MUX1**	**MUX0**
1	1	1	0	0	0	0	0

Sedangkan konfigurasi ADCSRA ditunjukkan pada tabel 3 berikut :

Tabel 3. Konfigurasi register ADCSRA.

ADEN	**ADCS**	**ADATE**	**ADIF**	**ADIE**	**ADPS2**	**ADPS1**	**ADPS0**
1	0	0	0	0	1	1	0

Register ADCSRA berfungsi untuk melakukan pengaturan sinyal kontrol dan status dari ADC. Dengan konfigurasi ADMUX dan ADCSRA di atas, tegangan referensi yang digunakan sama dengan tegangan VCC mikrokontroler, data keluaran ADC *left adjust*, ADC yang digunakan adalah ADC0, dan prescalar 64 serta mode konversi *single mode.*

Setelah register ADMUX dan ADCSRA dikonfigurasi, ADC sudah dapat melakukan konversi sinyal analog. Ketika akan melakukan konversi, ADC melakukan pemeriksaan terhadap bit ADATE. Jika bernilai satu maka konversi dapat dilakukan jika tidak konversi akan ditunda hingga ADATE sama dengan satu. Konversi selesai apabila bit ADIF = 1. Jika ADIF = 1 dan ADSC = 0 maka mikrokontroler siap untuk melakukan konversi lagi. Hasil konversi ADC disimpan pada register ADCH.

Algoritma Komunikasi Serial

Untuk mengirimkan data yang diperoleh dari mikrokontroler ke modulator FSK perlu dilakukan komunikasi. Komunikasi yang digunakan adalah komunikasi serial. Agar terjadi komunikasi maka dilakukan pengaturan *baud rate*, paritas, data bit, dan bit *stop* pada mikrokontroler dan modulator FSK dengan nilai yang sama. Nilai dari pengaturan *baud rate*, data bit, paritas, dan *stop* bit berturut-turut adalah 1200, 8, none, dan 1.

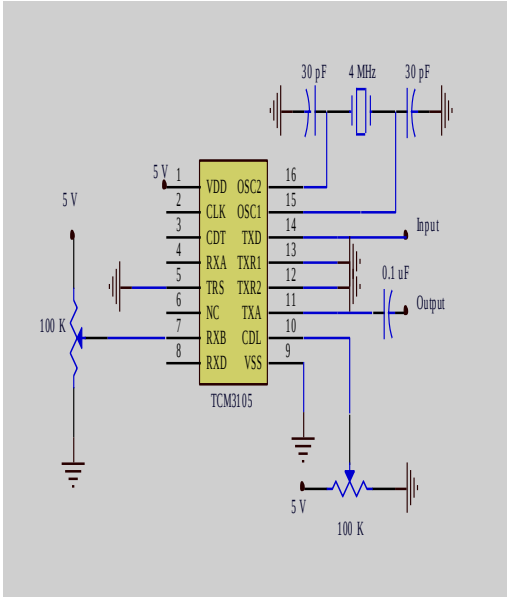
Pengaturan komunikasi serial pada mikrokontroler dilakukan dengan menentukan nilai atau melakukan konfigurasi beberapa register, yaitu:

i. UBRR (*USART Baud Rate Register*), register ini digunakan sebagai bit penyimpan konstanta kecepatan komunikasi serial. Register ini dibagi menjadi dua, yaitu UBRRL dan UBRRH, nilai kedua register ini adalah 3F dan 2.
ii. UCSRB (*USART Control and Status Register B*) merupakan register 8 bit pengatur aktivasi penerima dan pengirim Tx = 1.
iii. UCSRC (*USART Control and Status Register C*) merupakan register 8 bit yang digunakan untuk mengatur mode dan kecepatan komunikasi serial yang

dilakukan. Bit yang diatur adalah bit UCSZ0 = 1.

Modulator Pengunci Pergeseran Frekuensi (*Frequency Shift Keying*/ FSK)

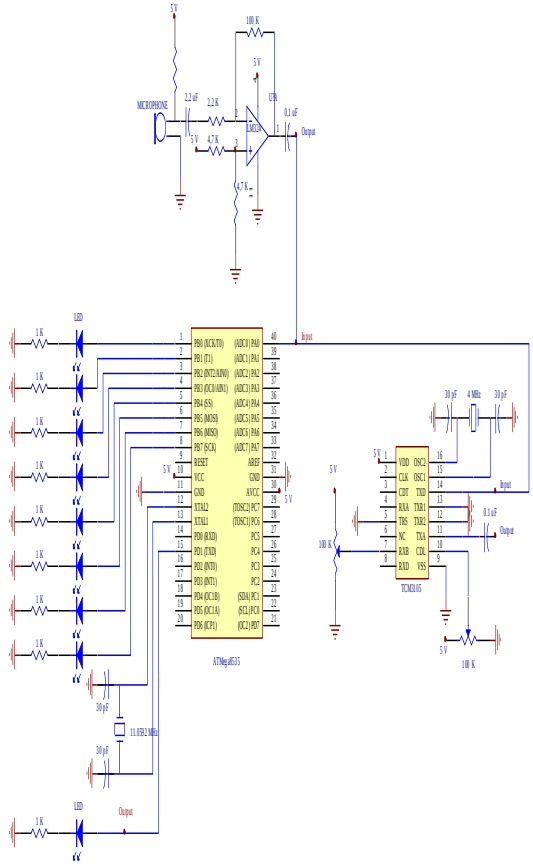
Untuk mengirimkan bit-bit digital maka diperlukan suatu sistem modulasi digital agar dapat mengkonversi bit-bit tersebut ke dalam bentuk sinyal analog. Modulasi digital yang dipakai ialah sistem FSK. Pada Tugas Akhir ini digunakan IC TCM 3105Ne sebagai IC FSK dengan nilai *baud rate* maksimal yang dimiliki adalah 1200bps. Pengaturan *baud rate* pada IC ini di atur pada kaki IC yang bernomor 5, 11 dan 12 yang semuanya dihubungkan langsung ke *ground*.



Gambar 6. Rangkaian modulator FSK dengan menggunakan TCM 3105NE

D. Hasil dan Pembahasan

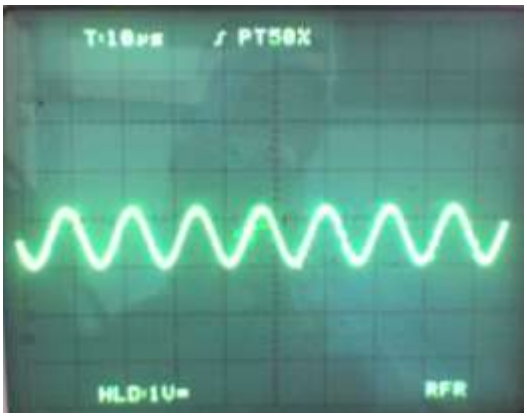
Pengujian dan analisis dilakukan untuk mengetahui kemampuan atau kinerja sistem enkripsi yang dibuat pada pesawat HT, apakah rangkaian yang dibuat sesuai dengan yang diharapkan. Pengujian dilakukan pada tiap blok rangkaian sehingga apabila terjadi suatu kesalahan akan dapat diketahui secara pasti.



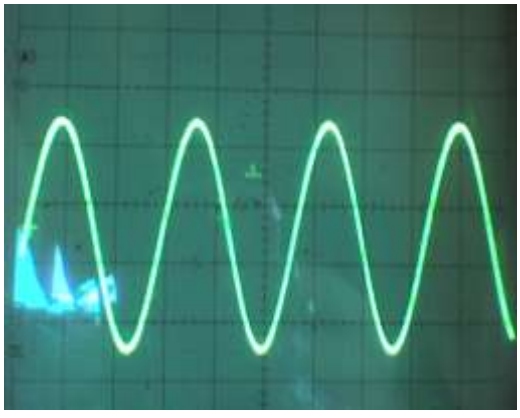
Gambar 7. Rangkaian sistem enkripsi pesawat komunikasi HT

Pengujian Rangkaian *Pre-Amplifier* dengan Menggunakan LM324

Pre-amplifier berfungsi untuk menguatkan sinyal untuk proses selanjutnya. Pengujian rangkaian ini dilakukan dengan cara memberi *input* yang berasal dari *function generator* sedangkan *output* dari rangkaian ini dihubungkan dengan osiloskop. Dari hasil yang didapat dilihat dari osiloskop sinyal yang diberikan berubah seiring dengan bertambahnya frekuensi yang diberikan oleh *function generator*. Amplitudo yang didapat semakin tinggi frekuensi suara maka semakin tinggi pula amplitudo yang dihasilkan. Berikut gambar sinyal *pre-amplifier* dengan input yang berasal dari *function generator*



Gambar 8. Sinyal *input pre-amplifier* dari *function generator*



Gambar 9. Sinyal *output pre-amplifier*

Pengujian juga dilakukan dengan menggunakan speaker sebagai *output* rangkaian, didapat hasil bahwa dari *input* yang diberikan maka *output*nya bisa terdengar suara pada speaker sesuai dengan suara masukan yang diberikan pada mikropon. Setelah dilakukan pengujian ini dapat dinyatakan bahwa rangkaian ini telah dapat berfungsi dengan baik untuk selanjutnya bisa dihubungkan dengan rangkaian berikutnya sehingga bisa membentuk rangkaian sistem enkripsi yang diinginkan.

Pengujian ADC dan Sistem Enkripsi pada Mikrokontroler AVR Seri ATmega8535.

Program konversi ADC mikrokontroler ATmega8535 digunakan untuk mengubah data/masukan analog menjadi keluaran digital. Pada proses ADC ini dilakukan proses *sampling* dan kuantisasi untuk setiap sinyal analog yang masuk yang dalam hal ini berupa suara manusia yang mempunyai *range* frekuensi 20 – 3400 Hz. Pada rangkaian mikrokontroler di *setting* pinA0 sebagai *input* ADC dan *output* rangkaian di *setting* pada portB yang mana pada rangkaiannya digunakan LED sebagai indikator sinyal hasil konversi ADC. Adapun pengujian yang dilakukan terhadap rangkaian ADC yaitu dengan memasukkan tegangan analog (Vi) pada ADC dengan nilai tertentu kemudian mencatat data digital (D_{out}) keluaran ADC.

Tahapan berikutnya adalah menambah program pada mikrokontroler yaitu program pengiriman data serial. *Baud rate* yang digunakan sesuai dengan *baud rate* yang telah diatur pada modulator FSK yaitu 1200 bps. Dari data digital yang parelel maka di ubah menjadi serial sehingga bisa dikirim sebagai masukan untuk modulator FSK. Adapun pengujian pengiriman data ADC secara serial dilakukan dengan cara menggunakan rangkaian penerima *(receiver)* yang telah diprogram juga penerimaan serialnya.

Selanjutnya pengujian dilanjutkan dengan menambahkan program enkripsi pada mikrokontroler pengirim. Adapun sistem enkripsi yang dibuat berdasarkan kriptografi Vigenere, dan kunci yang digunakan dalam perancangan alat ini berdasarkan kesepakatan antara pengirim dan penerima adalah menggunakan tiga kunci yaitu G, A dan S.

Proses yang dilakukan pada mikrokontroler pengirim ini adalah setelah sinyal yang diterima dikonversikan menjadi sinyal digital maka data tersebut langsung di enkripsi. Dalam hal ini, kunci keamanan informasi yang digunakan adalah $GAS_{alphabetic}$. Karena mikrokontroler AVR ATmega8535 hanya menggunakan bilangan biner dan heksa,

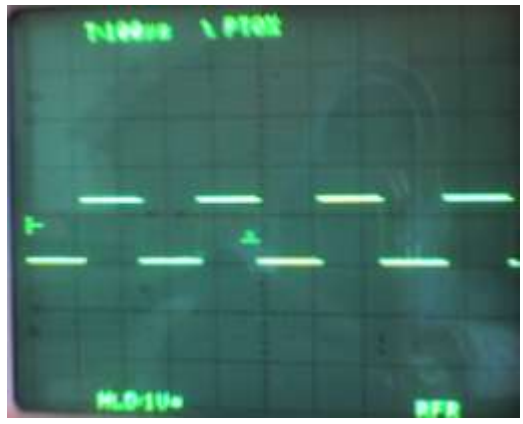
maka kunci *alphabetic* yang digunakan akan terlebih dahulu dikonversikan dalam bilangan biner. Dengan demikian, kunci $GAS_{alphabetic}$ akan menjadi:
$G_{alphabetic}$: 0b00000110(6) Kunci I
$A_{alphabetic}$: 0b 0000 0000 (0) Kunci II
$S_{alphabetic}$: 0b 0001 0010 (18) Kunci III
dan selanjutnya data yang telah di enkripsi akan dikirm secara serial ke mikrokontroler penerima. Adapun penggunaan kunci digunakan berdasarkan urutan data yang masuk, jika data pertama maka yang digunakan adalah kunci pertama yaitu G selanjutnya data ke dua akan digunakan kunci ke dua yaitu A begitu juga dengan data ke tiga yaitu menggunakan kunci ke tiga, S. Jika ada data yang masuk lagi maka kunci yang digunakan kembali ke kunci pertama begitu seterusnya.

Pengujian Rangkaian FSK menggunakan TCM 3105NE

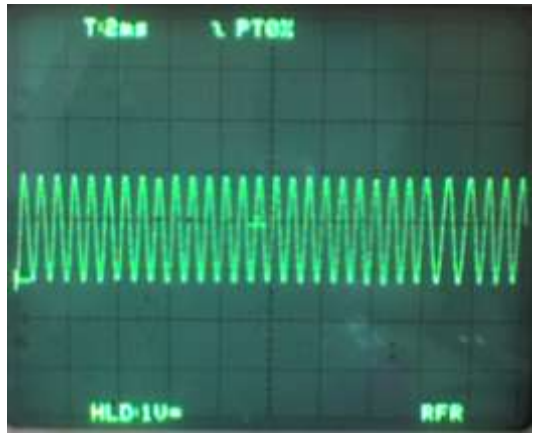
Rangkaian FSK yang digunakan terdiri dari dua bagian yakni modulator FSK yang terdapat pada bagian pemancar (*transmitter*) dan demodulator FSK pada bagian penerima (*transmitter*). Dalam perancangan ini, rangkaian modulator dan demodulator FSK menggunakan *baud rate* yang sama yaitu 1200 bps. Hal ini dikarenakan pin TRS, TXR1, dan TXR2 berada dalam logika *low* (terhubung *ground*).
Modulator FSK pada *transmitter* dirancang untuk mengubah data biner (data digital serial hasil enkripsi) menjadi dua buah sinyal/gelombang yang merepresentasikan data biner tersebut, berupa informasi yang siap dikirimkan melalui pemancar FM pada pesawat komunikasi HT.

Pengujian Rangkaian Power Supply

Rangkaian *power supply* berfungsi untuk menyediakan daya bagi rangkaian sistem enkripsi pada komunikasi HT. Dalam perancangan ini, tegangan yang diberikan ke rangkaian antara lain bernilai -15 volt, 0 volt, 5 volt, dan 15 volt.



Gambar 10. *Input* rangkaian modulator FSK dari *function generator*



Gambar 11. *Output* rangkaian modulator FSK

Kondisi ideal yang diharapkan pada keluaran IC *regulator* LM7805 adalah 5 V dan tegangan pada IC *regulator* LM7815 adalah +15 volt dan LM7915 menghasilkan tegangan -15 volt. Dalam hal ini, rangkaian *power supply* memperoleh masukan tegangan AC dari transformator *step-down* yang menurunkan tegangan AC 220 volt menjadi tegangan yang sesuai untuk masukan rangkaian *power supply.*

Pengujian Seluruh Blok Rangkaian

Setelah semua blok rangkaian di uji selanjutnya adalah pengujian untuk seluruh rangkaian yaitu dari *input pre-amplifier* berupa suara manusia (sinyal analog) yang

selanjutnya dikonversi menjadi sinyal digital melalui ADC yang telah diprogram pada mikrokontroler dan di enkripsi lalu dikirim secara serial ke modulator FSK yang kemudian dihubungkan ke PTT bagian mikrofon pada HT.

Dari hasil pengujian ternyata hasil yang didapat tidak sesuai dengan yang diharapkan. Suara yang dikirim tidak dapat diterima dengan jelas oleh sistem penerima, yang terdengar hanyalah suara bass saja. Hal ini dikarenakan modulator FSK dan demodulator FSK menggunakan *baud rate* 1200 bps. Dengan *baud rate* 1200 bps berdasarkan hasil perhitungan frekuensi yang bisa ditransmisikan adalah hanya 60 Hz saja. Yaitu dengan cara:

a. Data serial yang dikirim adalah 10 bit (8 bit informasi serial dan 1 bit *start* dan 1 bit *stop*).
   Jadi, data yang dikirim setiap detik adalah = $\frac{1200bps}{10bit} = 120Bps$
b. Waktu yang dibutuhkan untuk setiap pengiriman data secara serial adalah $\frac{1}{120Hz} = 8{,}33ms$.
c. Berdasarkan Nyquist, bandwidth yang dikirim = 2 x frekuensi sampling.
   Dengan demikian, frekuensi maksimum yang bisa dikirim adalah: $\frac{120Hz}{2} = 60Hz$

Selanjutnya untuk lebih membuktikan bahwa kendala yang terjadi karena pengaruh *baud rate*, maka dilakukan pemograman lagi dengan menggunakan frekuensi masukan 8KHz dan *baud rate* yang digunakan adalah 115,2 Kbps. Pengujian dilakukan tanpa menggunakan modulator FSK dan demodulator FSK, sehingga rangkaian yang digunakan hanya *pre-amplifier* → mikrokontroler (ADC+enkripsi) → HT *transmitter* → HT *receiver* → rangkaian penerima.

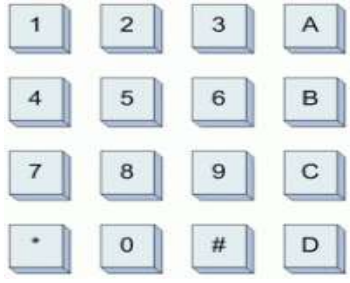
a. Data serial yang dikirim adalah 10 bit (8 bit informasi serial dan 1 bit *start* dan 1 bit *stop*).
   Jadi, data yang dikirim setiap detik adalah = $\frac{115{,}2Kbps}{10bit} = 11{,}52KBps$
b. Waktu yang dibutuhkan untuk setiap pengiriman data secara serial adalah $\frac{1}{11{,}52KHz} = 87\mu s$.
c. Berdasarkan Nyquist, frekuensi maksimum yang bisa dikirim adalah: $\frac{11{,}52KHz}{2} = 5{,}76KHz$

Dari hasil pengujian, suara yang dikirim dapat diterima dengan jelas di sisi penerima. Dengan demikian terbukti bahwa kendala penelitian ini adalah ada pada IC FSK yang tidak mendukung dengan frekuensi suara manusia.

Agar penelitian yang dilakukan lebih baik maka penelitian dilanjutkan dengan mengubah *input* yang digunakan pada rangkaian yaitu mengganti sinyal suara menjadi data digital yang berasal dari *keypad*.

Pengujian Rangkaian keypad sebagai input data yang akan di enkripsikan

Keypad 4x4 memiliki 16 buah tombol sebagai saklar. Model *push button, normally open*, artinya dalam kondisi normal (tidak ditekan) saklar terbuka.



Gambar 12. *Keypad switch layout*

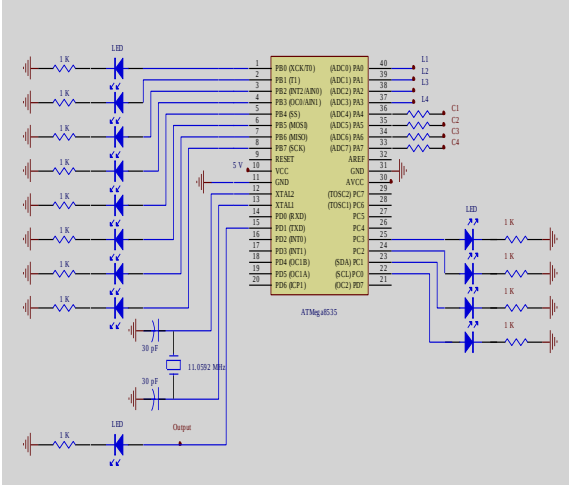
Switches menghubungkan bersama antara baris dan kolom (gambar di bawah).

Dengan menekan *keypad*, *switch* akan menghubungkan satu baris ke satu kolom tertentu. Sebagai contoh, dengan menekan tombol 3, maka baris 1 dan kolom 3 akan terhubung.

Cara kerja *keypad* adalah sebagai berikut: AVR mengkonfigurasikan pin 0-3 Port A (PA0-PA3) sebagai *input*, dan pin 4-7 Port A (PA4-PA7) sebagai *output*. Mula-mula pin *output* dan *input* di*set* seluruhnya pada kondisi H (1).

Selanjutnya dilakukan *scanning* per kolom. *Scanning* ini dilakukan dengan menjadikan *low* kolom yang dimaksud. Misal, *scanning* kolom I, maka PA4 diset low. Jika saklar tidak ditekan, logika mengambang, tidak ada data yang dikirim.

Scanning dilanjutkan ke kolom selanjutnya dengan cara PA5 (L) lainnya *High*. Jika di kolom 2 ini ada saklar/tombol yang ditekan maka pin *input* yang terhubung ke saklar yang bersangkutan akan bernilai logika 0. Data ini diteruskan untuk proses selanjutnya dtampilkan pada lampu LED untuk mengindikasikan *input* yang dimasukan sama dengan *output* yang ditampilkan. Dan *scanning* dilanjutkan lagi, demikian seterusnya.



Gambar 13. Rangkaian skematik *keypad* sebagai *input* mikrokontroler

Pada rangkaian yang digunakan dua buah *output* pada mikrokontroler yaitu port C sebagai *output* hasil *scanning keypad* dan port B digunakan sebagai *output* hasil pengiriman data serial. Adapun port yang difungsikan sebagai *output* dipasang LED sebagai indikator untuk menampilkan data biner hasil *scanning* dari *keypad.*
Setelah semua blok rangkaian diuji satu persatu maka selanjutnya dilakukan uji rangkaian secara keseluruhan secara lengkap dari sisi pengirim maupun penerima. pengujian yang dilakukan sama dengan uji rangkaian yang dilakukan sebelumnya hanya saja input data yang digunakan berbeda, yaitu *keypad.* Urutan proses pengiriman data adalah: *keypad* → *Scanning keypad*+sistem enkripsi (mikrokontroler) → HT *transmitter* → HT *receiver* → rangkaian penerima. Berikut data hasil pengujian:

Dari hasil pengujian dapat dilihat data yang dikirim yang berasal dari *keypad* dapat diterima dengan baik di sisi penerima walaupun data yang diterima telah diacak dengan sistem enkripsi yang ada. Hal ini terjadi karena pada sisi penerima data tersebut di dekripsi kembali sehingga data yang diterima sama dengan data yang dikirim. Dengan demikian dapat disimpulkan bahwa hasil perancangan sistem enkripsi pada HT ini telah dapat berfungsi dan bekerja sesuai dengan kerangka pemikiran dan desain penelitian.

E. Kesimpulan dan Saran

Kesimpulan

Setelah dilakukan berbagai pengujian dan analisa terhadap sistem enkripsi pada komunikasi HT (*Handie-Talkie*) baik perangkat keras maupun perangkat lunak, dapat diambil beberapa simpulan antara lain:

1. Perangkat sistem enkripsi pada komunikasi HT sudah dapat bekerja dalam mengkonversikan sinyal analog menjadi digital dan mengacak data

hasil konversi tersebut untuk ditransmisikan ke sistem penerima.
2. *Baud rate* yang digunakan dalam komunikasi serial yaitu 1200 bps (sesuai dengan spesifikasi IC FSK) akan tetapi dengan *baud rate* tersebut hanya bisa mendukung frekuensi sebesar 60 Hz.
3. Agar frekuensi suara dapat diacak dan ditransmisikan dengan baik maka digunakan *baud rate* yang mendukung frekuensi suara manusia yaitu sebesar 115,2 Kbps.
4. Data yang berasal dari *keypad* dapat ditransmisikan dengan baik dengan menggunakan *baud rate* 1200 bps pada IC FSK (TCM 3105NE).

Saran

Saran yang bisa diberikan kepada pengguna maupun para peneliti selanjutnya adalah:

1. Untuk pengembangan selanjutnya, hendaknya menambahkan sistem *Fase Shift Keying* yang memiliki *baud rate* yang mendukung untuk komunikasi suara manusia.
2. Penggunaaan kunci pada sistem enkripsi dan dekripsi diupayakan seminimal mungkin agar informasi yang diterima lebih akurat.

Daftar Pustaka

[1] Iswanti Suprapti. 2003. *Studi Sistem Keamanan Data dengan Metode Public Key Cryptography*. ITB. Bandung.

[2] P.H Smale. 1996. *Sistem Telekomunikasi I Edisi Kedua*. Terjemahan Ir. Chris Timoteus. Erlangga. Jakarta.

[3] Roger L. Freeman. 1996. *Telecommunication System Engineering 3rd Edition*. John Willey & Sons. Inc. New York.

[4] Stallings, William. 2001. *Dasar-Dasar Komunikasi Data*. PT. Salemba Teknika. Jakarta.

[5] Suhana. 1984. *Buku Pegangan Teknik telekomunikasi*. Pradnya Paramita. Jakarta.

[6] Suhata. 2003. *Aplikasi Mikrokontroler Sebagai Pengendali Peralatan Elektronik*. PT. ElekMediaKomputindo. Jakarta.

[7] Sukiswo. 2006. *Perancangan Telemetri Suhu dengan Modulasi Digital FSK-FM*. FT Undip. Semarang.

[8] Sutadi, Dwi. 2003. *I/O BUS & Motherboard*. ANDI. Yogyakarta.

[9] Thomas L Floyd. 1996. *Electronics Fundamental Cicuit, Devaices and Applications 4th Edition*. Prentice-Hall, Inc. New Jersey

[10] Wardhana, Lingga. 2006. *Balajar Sendiri Mikrokontroler AVR seri ATMega8535*. ANDI OFFSET. Yogyakarta. 187 hlm.