SMCD: SOLUSI AMAN UNTUK KOMUNIKASI SEDERHANA

Andi Yusuf[1], Syamsi Nurdiansah[2]
Lembaga Sandi Negara
Jl. Harsono R.M. No.70, Ragunan, Pasar Minggu, Jakarta Selatan 12550
Telp. (021) 7805814 ext. 2603, Faks. (021) 78844104
E-mail: kongsibo27@yahoo.com, syam_nci3@yahoo.co.id

ABSTRAK

Morse adalah bahasa bunyi, "dit" adalah bunyi pendek dan "dah" adalah bunyi panjang. Menurut rumus noise, semakin sempit bandwidth maka akan semakin rendah level noise (N = kTB) sehingga dengan morse yang memiliki bandwidth lebih kecil dibanding PSK31 (bandwidth morse < 31 Hz) maka level noise akan semakin rendah pula. Dengan morse memungkinkan receiver untuk menerima sinyal-sinyal yang lebih lemah atau dengan kata lain untuk daya yang sama morse dapat menjangkau jarak yang lebih jauh. Morse dibangkitkan dengan cara meng-on dan off-kan pemancar/oscillator tanpa modulasi sehingga dapat dibuat dengan rangkaian yang sangat sederhana.

SMCD (Secure Morse Communication Device) merupakan alat yang dibuat untuk mengamankan informasi yang sifatnya rahasia dan memanfaatkan kode morse dalam transmisinya. Alat ini sangat efektif utamanya dalam komunikasi darurat di saat komunikasi bicara relatif sulit dilakukan karena berbagai alasan, misalnya di saat propagasi buruk, level noise yang besar atau di saat komunikasi hanya bisa dilayani dengan perangkat bercatudaya kecil sedangkan informasi yang sifatnya rahasia tetap harus ditransmisikan. Metode yang digunakan dalam mengamankan informasi rahasia pada alat ini berupa teknik penyandian. Dengan teknik ini informasi disandi menjadi suatu iformasi yang tidak dapat dibaca atau diketahui oleh pihak yang tidak berkepentingan, kecuali oleh pihak penerima yang dimaksud.

Dalam pembuatannya SMCD dibagi menjadi dua bagian yaitu pembuatan hardware dan pembuatan software. Pembuatan dari segi hardware meliputi rangkaian pengolah data, rangkaian keypad, rangkaian LCD, rangkaian morse encoder, rangkaian morse decoder dan rangkaian pengolah kunci. Sedangkan dari segi software meliputi pembuatan subrutin verifikasi pengguna, subrutin akses keypad, subrutin akses LCD, subrutin enkripsi/dekripsi, subrutin morse encoder, subrutin morse decoder dan subrutin ADC. Didapatkan hasil bahwa SMCD berhasil mengamankan informasi yang ditransmisikan melalui kode morse walaupun hanya sebatas solusi keamanan untuk komunikasi sederhana.

Kata Kunci: SMCD, DT-51 Minimum System, AVR, Vigenere, pseudo random generator dan kode morse

1. PENDAHULUAN

Komunikasi aman dengan menggunakan radio menjadi hal yang sangat penting disaat infrastruktur lain tidak dapat digunakan, sementara komunikasi yang sifatnya rahasia harus tetap dilakukan. Besarnya noise pada komunikasi radio menyebabkan terjadinnya gangguan komunikasi pada radio sehingga komunikasi tidak dapat berjalan secara optimal. Untuk itu diperlukan suatu alat komunikasi yang memiliki level noise rendah saat transmisi dan mampu memberikan solusi keamanan terhadap informasi yang di transmisikan.

Secure Morse Communication Device (SMCD) merupakan mesin yang dirancang untuk mengamankan informasi (teks) yang sifatnya rahasia dan mentransmisikan melalui komunikasi sinyal kode morse. Perancangan mesin dilakukan pada aspek perangkat lunak dan perangkat keras. Mesin hasil perancangan diharapkan dapat dijadikan solusi keamanan untuk komunikasi yang sederhana.

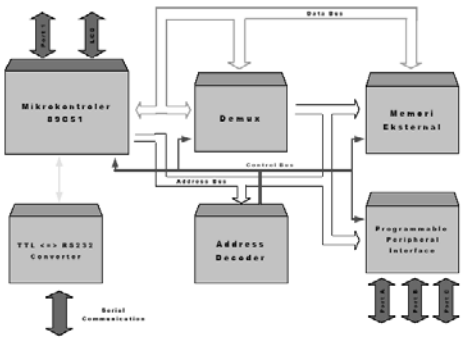
2. LANDASAN TEORI

2.1 DT51 Minimum System

DT51 merupakan development tools yang terdiri dari 2 bagian terintegrasi yaitu perangkat keras dan perangkat lunak [3]**.** Komponen utama perangkat keras DT51 ialah mikrokontroler 89C51 yang merupakan salah satu turunan keluarga MCS-51 Intel dan telah menjadi salah satu standar industri dunia. Selain mikrokontroler, DT51 dilengkapi pula dengan EEPROM yang memungkinkan DT51 bekerja dalam mode stand-alone (bekerja sendiri tanpa komputer). Selain komponen-komponen tersebut masih banyak fungsi-fungsi lain pada DT51, antara lain : timer, counter, RS-232 serial port, Programmable Peripheral Interface (PPI), serta LCD port. Perangkat lunak DT51 terdiri dari *Downloader* DT51L dan *Debugger* DT51D. Downloader berfungsi untuk mentransfer user program dari PC (Portable Computer) ke DT51, sedangkan debugger akan membantu user untuk melacak kesalahan program.

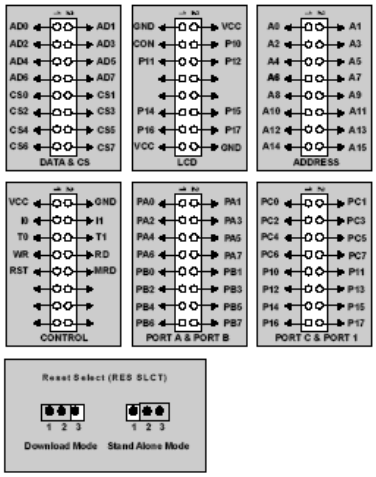
Blok Diagram DT51

Blok diagram DT51 menggambarkan beberapa bagian penting dari DT51 dapat dilihat pada Gambar 1.



Gambar 1. Blok diagram DT-51

Adapun port-port yang digunakan pada DT51 dapat dilihat pada Gambar 2.



Gambar 2. Port pada DT-51

2.2 Kode Morse

Morse adalah bahasa bunyi, "dit" adalah bunyi pendek dan "dah" adalah bunyi panjang [4]. Dalam Tabel 1 dan 2 adalah morse yang umum digunakan.

Tabel 1. Kode Morse untuk Angka

ANGKA								
	fonetik	*bunyinya*		*foneti k*	*bunyinya*		*Fonetik*	*bunyiny a*
1	one	di-dah-dah-dah-dah	**2**	two	di-di-dah-dah-dah	**3**	Three	di-di-di-dah-dah
4	four	di-di-di-di-dah	**5**	five	di-di-di-di-dit	**6**	Six	dah-di-di-di-dit
7	seven	dah-dah-di-di-dit	**8**	eight	dah-dah-dah-di-dit	**9**	Nine	dah-dah-dah-dah-dit
0	zero	dah-dah-dah-dah-dah						

2.3 ADC dan DAC

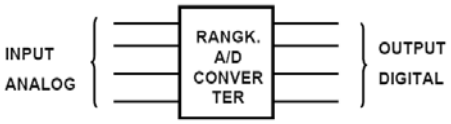
Analog to Digital Converter (ADC) adalah sebuah piranti yang dirancang untuk mengubah sinyal-sinyal analog menjadi bentuk sinyal digital [5]. Untuk perancangan *Secure Modern Morse*, IC ADC 0804 dianggap dapat memenuhi kebutuhan dari rangkaian yang akan dibuat. IC jenis ini bekerja secara cermat dengan menambahkan sedikit komponen sesuai dengan spesifikasi yang harus diberikan dan dapat mengkonversikan secara cepat suatu masukan tegangan. Gambar 3 merupakan blok umum rangkaian ADC.

Tabel 2. Kode Morse untuk Abjad

ABJAD								
A	alpha	di-dah	**B**	bravo	dah-di-di-dit	**C**	charlie	dah-di-dah-dit
D	delta	dah-di-dit	**E**	echo	dit	**F**	foxtrot	di-di-dah-dit
G	golf	dah-dah-dit	**H**	hotel	di-di-di-dit	**I**	india	di-dit
J	juliet	di-dah-dah-dah	**K**	kilo	dah-di-dah	**L**	lima	di-dah-di-dit
M	mike	dah-dah	**N**	november	dah-dit	**O**	oscar	dah-dah-dah
P	papa	di-dah-dah-dit	**Q**	quebec	dah-dah-di-dah	**R**	romeo	di-dah-dit
S	sierra	di-di-dit	**T**	tango	dah	**U**	uniform	di-di-dah
V	victor	di-di-di-dah	**W**	whiskey	di-dah-dah	**X**	x-ray	dah-di-di-dah
Y	yankee	dah-di-dah-dah	**Z**	zulu	dah-dah-di-dit			

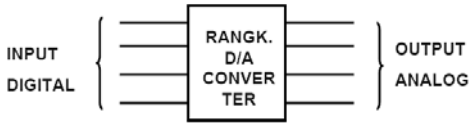
Tabel 3. Kode Morse untuk Tanda Baca

TANDA BACA										
.	titik	AAA	di-dah-di-dah-di-dah	**,**	koma	MIM	dah-dah-di-di-dah-dah	**?**	tanda tanya	IMI	di-di-dah-dah-di-dit
/	garis miring	DN	dah-di-di-dah-dit	**-**	garis datar	DU	dah-di-di-di-dah	**_**	garis bawah	IQ	di-di-dah-dah-di-dah
(	kurung buka	KN	dah-di-dah-dah-dit	**)**	kurung tutup	KK	dah-di-dah-dah-di-dah	**'**	tanda petik		di-dah-dah-dah-dah-dit
"	tanda kutip	AF	di-dah-di-di-dah-dit	**:**	titik dua	OS	dah-dah-dah-di-di-dit	**;**	titik koma	KR	dah-di-dah-di-dah-dit
+	tanda tambah	AR	di-dah-di-dah-dit	**=**	sama dengan	BT	dah-di-di-di-dah	*****	clear	SK/VA	di-di-di-dah-di-dah
$	tanda dollar	SX	di-di-di-dah-di-di-dah	**>**	tanda mulai	KA/CT	dah-di-dah-di-dah	**#**	tanda salah	HH	di-di-di-di-di-di-di-dit



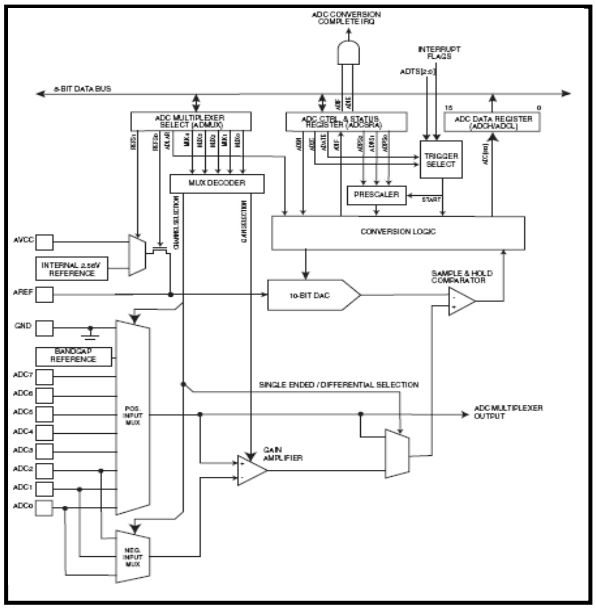
Gambar 3. Blok rangkaian adc

Digital to Analog Converter (DAC) adalah sebuah piranti yang dirancang untuk mengubah sinyal digital menjadi bentuk sinyal analog [5]. Untuk perancangan *Secure Modern Morse*, proses DAC diperlukan untuk mengkonversi data digital menjadi ketukan (kode sinyal) morse. Penggunaan DAC hanya menggunakan rangkaian relay dan jack CW, tidak memerlukan IC DAC secara khusus. Gambar 4 merupakan blok umum rangkaian DAC.



Gambar 4. Blok rangkaian dac

Pada pihak penerima menggunakan ADC dengan memanfaatkan AVR. ADC-AVR merupakan ADC yang memiliki resolusi 10 bit. Berikut adalah skema dari ADC-AVR.

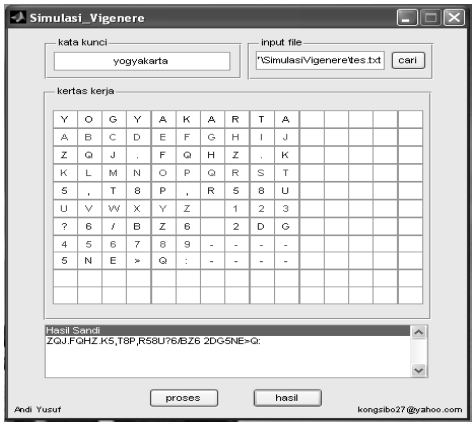


Gambar 5. skematik adc-avr

2.4 Kriptografi

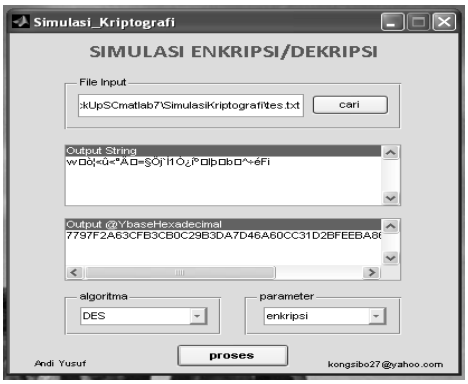
Kriptografi adalah ilmu untuk menjaga kerahasiaan informasi dengan metode dan teknik matematika yang mencakup *confidentiality*, *data integrity*, *entity authentication*, dan *data origin autehtication* [9]. Kriptografi mempelajari sistem sandi (seperangkat prosedur, protokol, instruksi, algoritma kriptografis, dan sebagainya). Dalam SMCD algortima kriptografi yang digunakan adalah vigenere dan *Data Encryption Standard* (DES).

Vigenere merupakan sistem penyandian klasik yang ditemukan oleh seorang Perancis, Blaise de Viginere (1523-1596). Sistem ini memiliki rumus: S=T+K dimana S adalah hasil sandi; T adalah teks asli; dan K adalah kunci. Gambar 6 merupakan contoh simulasi dari sistem viginere.



Gambar 6. simulasi algoritma vigenere

DES merupakan algoritma standar yang pertama dikeluarkan oleh *National Bureau standard* Amerika Serikat untuk konsumsi public. Algoritma ini melakukan proses enkripsi/dekripsi dengan ukuran blok 64-bit. Proses enkripsi setiap blok terdiri 16 round, ditambah dengan fungsi permutasi. Gambar 7 merupakan contoh hasil simulasi dari Agoritma DES.



Gambar 7. simulasi algoritma des

3. DESKRIPSI DAN PENGGUNAAN SMCD

3.1. Deskripsi Mesin

Secara garis besar *Secure Modern Morse* dibagi menjadi 2 bagian :

1. SMCD untuk pengirim

   Berupa modul perangkat keras yang digunakan untuk mengenkripsi pesan dan secara otomatis mengkonversi menjadi kode morse. Dapat dikatakan bahwa modul ini berfungsi sebagai *encryptor* dan *encoder*.

Gambar 8. SMCD pengirim

2. SMCD untuk penerima

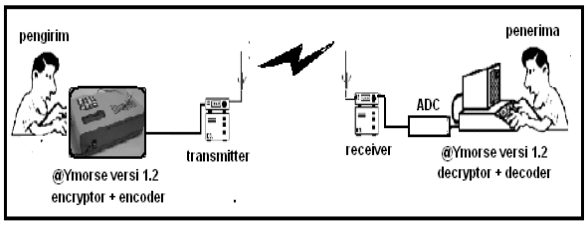
   Berupa modul perangkat lunak yang digunakan untuk mengkonversi kode morse menjadi pesan terenkripsi dan secara otomatis mendekripsi mejadi pesan asli sesuai pengiriman. Dapat dikatakan bahwa modul ini berfungsi sebagai *decryptor* dan *decoder*.

Gambar 9. SMCD penerima

3.2. Penggunaan Mesin

Penggunaan SMCD dapat dipadukan dengan radio ICOM HF/VHF/UHF all mode transceiver IC – 706 MKIIG sebagai transmitter dan receiver pada prototype komunikasi awal.

Alat ini sangat cocok digunakan dalam komunikasi darurat di saat komunikasi bicara relatif sulit dilakukan karena berbagai alasan, dalam hal ini komunikasi di perairan Indonesia. Skema penggunaan mesin ini digambarkan pada gambar 10.



Gambar 10. Penggunaan SMCD

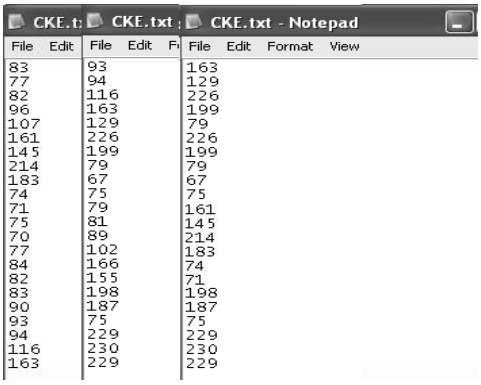
3.3. Cara Kerja Mesin

Hal penting yang perlu diketahui bahwa disisi pengirim terdapat 2 buah alat yaitu modul perangkat keras SMCD pengirim dan radio transmitter, sedangkan disisi penerima terdapat 3 buah alat yaitu laptop yang menyimpan modul perangkat lunak SMCD penerima, modul konversi analog-digital dan radio receiver. Adapun cara kerja alat ini mulai dari pengiriman sampai dengan penerimaan dijelaskan sebagai berikut :

1. Pengirim menginput pesan melalui keypad dan akan tampil pada layar dari modul SMCD pengirim;
2. Tekan tombol kirim pada modul SMCD pengirim dan secara otomatis pesan akan dienkripsi untuk kemudian dikonversi menjadi kode-kode morse. Kode morse yang dihasilkan akan dikirimkan secara otomatis pada radio transmitter melalui koneksi pada port CW;

Gambar 11. Koneksi SMCD pengirim dengan Radio Transmitter

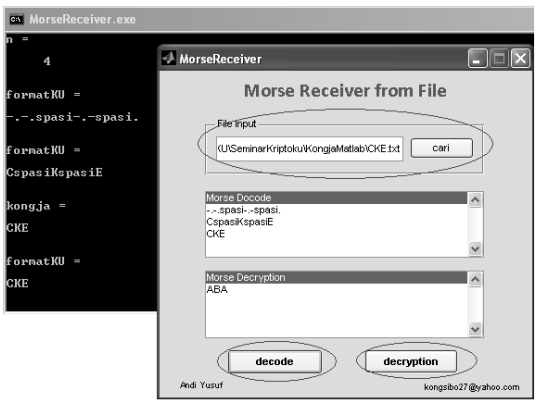
3. Radio transmitter akan menerima kode morse tersebut dan secara otomatis mengirimkan kepada radio receiver dalam bentuk sinyal morse;
4. Disisi penerima, radio receiver akan menerima sinyal morse yang dikirimkan radio transmitter. Kemudian sinyal morse dalam hal ini bunyi morse dikonversi menjadi data digital oleh modul ADC yang terkoneksi pada port audio pada radio receiver;
5. Data digital hasil konversi dari modul ADC secara otomatis dikirimkan pada computer melalui hyperterminal untuk kemudian data digital tersebut disimpan dalam suatu file;



Gambar 12. Data Digital hasil konversi modul ADC

6. Penerima menjalankan modul SMCD penerima dan menginputkan file yang menyimpan data digital pada proses 5. Langkah selanjutnya penerima melakukan proses *decode* dan dekripsi yang sudah disediakan pada aplikasi tersebut;
7. Pesan dapat dibaca oleh penerima pada modul

SMCD penerima di "textfield Morse Decryption" yaitu form terbawah pada aplikasi.



Gambar 13. Pesan yang dihasilkan pada Modul SMCD penerima

4. PERANCANGAN SMCD

Perancangan mesin SMCD version dibagi menjadi dua yaitu perancangan perangkat keras dan perancangan perangkat lunak.

4.1 Perancangan perangkat keras

Adapun perangkat keras yang harus dirancang pada mesin SMCD dapat dijelaskan secara detail dibawah ini.

Rangkaian pengolah data

Merupakan rangkaian bawaan dari DT51 minimum system.

Rangkaian keypad

Merupakan konfigurasi koneksi keypad dengan port pada DT51.

Rangkaian LCD

Merupakan konfigurasi koneksi LCD dengan port pada DT51.

Rangkaian Morse Encoder

Merupakan rangkaian DAC untuk pengiriman automatis, merubah keyer morse menjadi relay yang dikontrol DT51. Secara spesifik rangkaian ini merupakan relay yang terkoneksi dengan DT51 dan radio.

Rangkaian Morse Decoder

Merupakan rangkaian ADC, memanfaatkan IC ADC0804 yang memanfaatkan input audio dari radio dan mengirimkan 8 bit output pada DT51.

Rangkaian pengolah kunci

Merupakan konfigurasi koneksi USB dengan port pada DT51.

4.2 Perancangan perangkat lunak

Adapun perangkat lunak yang harus dirancang pada mesin SMCD dapat dijelaskan secara detail dibawah ini.

Subrutin verifikasi pengguna

Sub rutin dibuat untuk fungsi verifikasi pengguna dalam penggunaan mesin. Verifikasi berupa inputan enam digit pin pengguna, jika pin sesuai maka akses diterima untuk menggunakan mesin. Sedangkan pin yang tidak sesuai maka akses ditolak dan mesin kembali pada tampilan *default*.

Subrutin akses keypad

Sub rutin dibuat untuk memberikan respon dari keypad yang ditekan oleh pengguna. Setiap tombol pada keypad dapat merepresentasikan 3-4 karakter yang digunakan sebagai inputan pada mesin yang dirancang.

Subrutin akses LCD

Sub rutin dibuat untuk dapat menampilkan karakter input dari penekanan keypad ataupun karakter output hasil proses enkripsi/dekripsi.

Subrutin enkripsi/dekripsi sederhana

Sub rutin enkripsi dan dekripsi merupakan program utama. Sub rutin enkripsi digunakan untuk menyandi pesan terang menjadi suatu pesan tersandi. Sedangkan sub rutin dekripsi digunakan untuk membuka pesan tersandi menjadi suatu pesan terang.

Subrutin enkripi/dekripsi Lanjutan

Subrutin enkripsi dan dekripsi untuk algoritma yang lebih kompleks seperti DES atau AES. Sehingga memiliki nilai keamanan yang lebih tinggi.

Subrutin Morse Encoder

Sub rutin dibuat untuk merubah pesan tersandi menjadi kode – kode morse yang dapat dikirim melalui transmisi morse pada radio.

Subrutin Morse Decoder

Sub rutin dibuat untuk merubah sinyal kode morse (bunyi morse) yang berasal dari radio menjadi data digital untuk dilakukan proses dekripsi.

Subrutin Analog to Digital Converter

Subrutin ini dibuat pada mikrokontroler AVR yang memiliki fungsi untuk merubah data analog menjadi data digital.

5. REALISASI RANCANGAN PADA SMCD

Mesin SMCD ini masih memungkinkan untuk dikembangkan lebih lanjut. Rencana kedepan SMCD *versi 1.2* memungkinkan untuk pengolahan file dengan algoritma yang lebih kompleks dan manajemen kunci yang baik. Untuk rencana pengembangan perlu dilakukan pembuatan rencana komponen seperti dilihat pada Tabel 4 dan Tabel 5.

Tabel 4. Realisasi perangkat keras

No.	*Perangkat Keras*	*Realisasi*
1.	Rangkaian pengolah data	Sudah terealisasi
2.	Rangkaian keypad	Sudah terealisasi
3.	Rangkaian LCD	Sudah terealisasi
4.	Rangkaian Morse Encoder	Sudah terealisasi
5.	Rangkaian Morse Decoder	Sudah terealisasi
6.	Rangkaian pengolah kunci	Sedang direalisasikan

Tabel 5. Realisasi perangkat lunak

No.	*Perangkat Lunak*	*Realisasi*
1.	Subrutin verifikasi pengguna	Sudah terealisasi
2.	Subrutin akses keypad	Sudah terealisasi
3.	Subrutin akses LCD	Sudah terealisasi
4.	Subrutin enkripsi/dekripsi	Sudah terealisasi
5.	Subrutin Morse Encoder	Sudah terealisasi
6.	Subrutin Morse Decoder	Sudah terealisasi

6. KESIMPULAN

Kesimpulan yang bisa diambil dari proses perancangan SMCD ini adalah :

1. Masih ditemukan kendala noise pada saat melakukan proses ADC sehingga perlu dilakukan penambahan filter yang sesuai.
2. Realisasi perancangan perangkat lunak terkait enkripsi/dekripsi yang lebih kompleks dan penyimpanan kunci mempunyai tingkat kesulitan yang lebih tinggi dibandingkan perangkat lunak yang lain.
3. Realisasi untuk pengolahan dari teks menjadi file sangat memungkinkan untuk dilakukan. Dengan menambahan suatu aplikasi pada sisi pengirim.

PUSTAKA

Innovative Electronics. (2005). *AT89S51/52 Development Tools DT-51 MinSys*.

Andi Yusuf, (2005). *Rancang Bangun Mesin Sandi Teks untuk Pengamanan pada Transmisi Morse*, Jurnal Seminar Tugas Akhir.

Innovative Electronics. (2005). *89C51 Development Tools DT51 vesion 3*.

Orari Pusat. *Aktif CW*. Diakses pada 3 Januari 2009 dari http://mirror.unej.ac.id/onnowpurbo/orari-diklat/pemula/teknik-operasi/operating-procedures/Aktiv-CW.htm.

STT TELKOM. (2003). *Modul Praktek Microcontroller*, Bandung.

ATMEL, *Datasheet ATMEL AVR ATmega32*. Diakses pada 20 januari 2008 dari http://www.atmel.com.

Bejo Agus. (2008). *C & AVR Rahasia Kemudahan Bahasa C dalam Mikrokontroler ATmega8535*. Yogyakarta : Graha Ilmu

Tim Penyusun. (2007). Jelajah Kriptologi. Jakarta : Lembaga Sandi Negara

Roger J. Sutton. (2002). *SECURE COMMUNICATION Application and Management*, Wiley Series 81-86.