PERANCANGAN PERANGKAT TRANFER DATA FILE KOMPUTER TERENKRIPSI SECARA HARDWARE MENGGUNAKAN MEDIA WRELESS DAN MIKROKONTROLER AVR ATMEGA162

Denny Ardyanto[*)], Yuli Christyono, and Ajub Ajulian Z

Jurusan Teknik Elektro, Universitas Diponegoro Semarang
Jl. Prof. Sudharto, SH, Kampus UNDIP Tembalang, Semarang 50275, Indonesia

[*)]*E-mail* :*snx_smiph@yahoo.co.id*

Abstrak

Sistem informasi jaman sekarang terdapat banyak tantangan - tantangan baru di dalam keamanan informasinya. Baik di suatu negara, perusahaan atau sebuah organisasi, keamanan data adalah salah satu hal yang penting dalam komunikasi data antar computer melalui jaringan. Banyak orang menyiasati bagaimana cara mengamankan data yang akan dikirim dan diterimanya. Keamanan data bisa dijaga dengan berbagai cara, salah satunya adalah dengan cara melakukan enkripsi terhadap data yang dikirimkan. Dalam penelitian ini, dibuat suatu alat untuk mengamankan data yang akan dikirim dan yang akan diterima dengan menggunakan enkripsi TEA. Sehingga apabila terjadi penyadapan data pada saat pengiriman ataupun penerimaan, data tersebut tidak dapat dibaca oleh penyadap tersebut karena sudah dalam bentuk enkripsi.

kata kunci: keamanan data, pengiriman data, enkripsi, TEA

Abstrak

In era information systems, there are many new challenges in the information security. Wherever in a country, company or an organization, security of data is one of the important things in the communicaton of data between one computer and the other through a network. Many people think about how to secure datawhich to be sent and to be received. Security of data can be maintained in various option, one of which is to encrypt the data transmitted. In this research, created a tool to secure data which to be sent and to be received by TEA encryption. So in case of interception of data during transmission or reception, the data can't be read by eavesdroppers because it is still in encrypted form.

Key : security data, transfer data, encripsi, TEA

1. Pendahuluan

Sistem informasi jaman sekarang terdapat banyak tantangan-tantangan baru di dalam keamanan informasinya. Baik di suatu negara, perusahaan atau sebuah organisasi karena salah satu hal yang penting dalam komunikasi data antar komputer melalui jaringan adalah keamanan datanya. Banyak orang menyiasati bagaimana cara mengamankan data yang dikirim dan data yang akan diterimanya. Keamanan data bisa dijaga dengan berbagai cara, salah satunya adalah dengan cara melakukan enkripsi terhadap data yang dikirimkan.

Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. untuk menjaga agar baik pesan atau kunci ataupun keduanya tetap terjaga kerahasiaannya dari penyadap (attacker). Penyadap pesan diasumsikan mempunyai akses yang lengkap dalam saluran komunikasi antara pengirim pesan dan penerima pesan. Penyadapan pesan sering terjadi pada komunikasi melalui internet maupun saluran telepon. Oleh karena itu maka dibuat hardware untuk meminimalisasi adanya penyadap.

Dengan enkripsi, *user* lain selain yang kita inginkan tidak bisa membaca data yang kita berikan. Secara umum enkripsi bisa dibagi menjadi dua jenis, yaitu enkripsi simetris dan enkripsi asimetris. Enkripsi dikatakan simetris bila hanya menggunakan satu buah kunci yang sama untuk melakukan enkripsi dan dekripsi. Sedangkan enkripsi asimetris menggunakan dua buah kunci yang berbeda untuk enkripsi-dekripsi, yaitu kunci publik dan kunci privat. Selain itu berdasarkan cara pengolahan data juga terdapat dua macam enkripsi, yaitu *stream cipher* dan *block cipher*. *Stream cipher* digunakan untuk enkripsi yang simetris. Sedangkan *block cipher* bisa digunakan untuk enkripsi simetris maupun asimetris. Perbedaan antara

stream cipher dan *block cipher* adalah dalam pemrosesan data, *block cipher* memproses setiap blok data sedangkan *stream cipher* memproses per-bit data.

Walaupun enkripsi bukan solusi total untuk keamanan, enkripsi merupakan *tool* yang digunakan untuk menangani ancaman-ancaman keamanan yang spesifik dan akan menjadi semakin penting, khususnya di area enkripsi data yang tersimpan.

Dalam penelitian ini dibuat suatu alat untuk mengamankan data yang akan dikirim dan yang akan diterima dengan menggunakan enkripsi TEA. agar bila terjadi penyadapan data atau file penting dikirimkan saat file atau data tersebut dikirim tidak dapat dibaca oleh penyadap tersebut karena masih dalam bentuk enkripsi.
Tujuan dari penulisan penelitian ini adalah mengatasi masalah-masalah keamanan data saat pengiriman file dari komputer yang satu ke komputer lain dengan ilmu kriptografi. Pembahasan permasalahan diharapkan tidak menyimpang dari pokok permasalahan, sehingga dalam penyelesaian masalah penelitian ini akan dibatasi pada beberapa hal berikut ini :

1. Mikrokontroller yang digunakan adalah ATmega162
2. Enkripsi datanya menggunakan metode TEA.
3. Transfer filenya secara wireless menggunakan modul wireless.
4. Interface ke komputer menggunakan konverter USB.
5. Software aplikasi berbasis Delphi7 untuk mengkonfersi file ke data heksadesimal dan data heksadesimal ke file.
6. Tidak membahas secara detail software komputer.
7. Tidak membahas secara detail interface USB.

2. Metode

2.1 Kriptografi

Teknik untuk mengacak suatu pesan agar tidak dapat diketahui maknanya disebut enkripsi, dan membentuk suatu bidang keilmuan yang disebut Kriptografi.Prinsip dasarnya adalah menyembunyikan informasi sedemikian rupa agar orang yang berhak saja yang dapat mengetahui isi dari informasi yang tersembunyi tersebut.Teknik ini sudah ada sejak jaman dahulu, bahkan sejak jaman sebelum Masehi pada masa perang yang digunakan untuk mengirim pesan rahasia antar sesama kawan agar apabila pesan terbaca oleh musuh ditengah jalan, isi dari pesan tersebut tidak dapat terbaca. Seiring dengan kemajuan teknik yang digunakan untuk mengenkripsi maka didalamnya terkandung unsur matematis yang membuat isi dari informasi itu semakin sulit untuk dibongkar.

2.1.1 TEA (Tiny Encryption Algorithm)

Tiny Encryption Algorithm (TEA) merupakan suatu sandi algoritma yang diciptakan oleh David Wheeler dan Roger Needham dari Computer Laboratory, Cambridge University, England pada bulan November 1994.TEA merupakan algoritma penyandian *block cipher* yang dirancang untuk penggunaan memory yang seminimal mungkin dengan kecepatan proses yang maksimal. Dekripsi Sistem penyandian TEA menggunakan proses feistel network dengan menambahkan fungsi matematik berupa penambahan dan pengurangan sebagai operator pembalik selain XOR. Hal ini dimaksudkan untuk menciptakan sifat non-linearitas. Pergeseran dua arah (ke kiri dan ke kanan) menyebabkan semua bit kunci dan data bercampur secara berulang ulang. TEA memproses 64-bit input sekali waktu dan menghasilkan 64-bit output. TEA menyimpan 64-bit input kedalam L0 dan R0 masing masing 32-bit. Sedangkan 128-bit kunci disimpan kedalam k(0), k(1), k(2), dan k(3) yang masing masing berisi 32-bit. Diharapkan teknik ini cukup dapat mencegah penggunaan teknik *exshautive search* secara efektif.

Pada sisi enkripsi ini merubah data asli menjadi data yang disandikan. Awalnya terdapat 32 bit data asli/R(0) yang kemudian bit tersebut digeser sebanyak 4 kali ke arah kiri.Setelah itu hasil bit yang telah digeser di XOR-kan dengan bit kunci K(0) yang merupakan konstanta pada proses ini. Lalu hasil dari XOR ditambahkan (ADD) dengan bit kunci K(0) kembali sehingga akan muncul 32 bit yang susunanya berbeda dengan data aslinya.

Pada bagian ini mengolah hasil dari proses enkripsi menjadi data asli. Hasil dari proses enkripsi dikurangi (SUB) dengan bit kunci K(0). Kemudian hasil dari pengurangan di XOR-kan dengan bit kunci K(0) kembali. Setelah itu digeser ke kanan sebanyak 4 bit maka akan diperoleh data asli R(0).

2.2 MikrokontrolerAT Mega 162

ATMega162 adalah CMOS 8-bit mikrokontroler berdaya rendah yang didasarkan pada AVR dengan peningkatan arsitektur RISC.Dengan menjalankan instruksi yang kuat dalam suatu *single clock cycle*, ATMega 162 dapat mecapai 1 MIPS per MHz yang memungkinkan sistem untuk mengoptimalkan daya dibandingkan kecepatan saat pemrosesan.
Core AVR menggabungkan bermacam-macam instruksi dengan 32 tujuan umum kinerja register. Ketiga puluh dua register secara langsung terhubung dengan *Arithmetic Logic Unit* (ALU), yang memungkinkan dua independen register dapat diakses dalam satu instruksi tunggal dalam satu *clock cycle*. Hasil arsitektur lebih efisien ketika mencapai sepuluh kali lebih cepat daripada mikrokontroler CISC konvensional.

2.2.1 Fitur ATmega 162

- Konsumsi daya rendah.
- Mempunyai dua buah serial komunikasi.
- Mempunyai 35 I/O.

- 16k *byte* memory *flash* ISP, 512 *bytes* EEPROM (*Electrically Erasable Programmable Read Only Memory)*, 1kb internal SRAM.
- Dua buah *timer/counter* 8 bit, satu buah *timer/counter* 16 bit.

2.3 Modul Wireless

Wireless atau *wireless network* merupakan sekumpulan komputer yang saling terhubung antara satu dengan lainya sehingga terbentuk sebuah jaringan komputer dengan menggunakan media udara / gelombang sebagai jalur lintas datanya. Pada dasarnya *wireless* dengan LAN merupakan sama-sama jaringan komputer yang saling terhubung antara satu dengan lainya, yang membedakan antara keduanya adalah media jalur lintas data yang digunakan, jika LAN masih menggunakan kabel sebagai media lintas datanya, sedangkan *wireless* menggunakan media gelombang radio/udara. Penerapan dari aplikasi *wirelessnetwork* ini antara lain adalah jaringan *nirkabel* diperusahaan, atau *mobile communication* seperti *handphone*dan HT. Adapun pengertian lainya adalah sekumpulan standar yang digunakan untuk jaringan *local nirkabel* (*Wireless Local Area Network* – WLAN) yang didasari pada spesifikasi IEEE 802.11.Terdapat tiga varian terhadap *standard* tersebut yaitu 802.11b atau dikenal dengan WIFI (*Wireless Fidelity*), 802.11a (WIFI5), dan 802.11. ketiga *standard* tersebut biasa disingkat 802.11a/b/g. Versi *Wireless* LAN 802.11b memiliki kemampuan *transfer* data kecepatan tinggi hingga 11Mbps pada *band* frekuensi 2,4 Ghz. Versi berikutnya 802.11a, untuk *transfer* data kecepatan tinggi hingga 54 Mbps dengan frekuensi 2,4 Ghz.

2.3.1 Deskripsi *Wireless* nRF905

nRF905 adalah *chip* tunggal radio *transceiver* yang bekerja pada frekuensi 433/868/915MHz ISM *band*. *Transceiver* terdiri dari *synthesizer* terintegrasi frekuensi, rantai penerima dengan *demodulator*, *power amplifier*, *osilator Kristal* dan, *modulator*.Fitur *ShockBurst* secara otomatis menangani pembukaan dan CRC dapat dengan mudah mengkonfigurasi nRF905 melalui SPI.Konsumsi saat ini sangat rendah, hanya mengirimkan 9mA pada *output*-10dBm, dan pada penerima 12.5mA.

2.4 *Interface* USB (*Universal Serial Bus*)

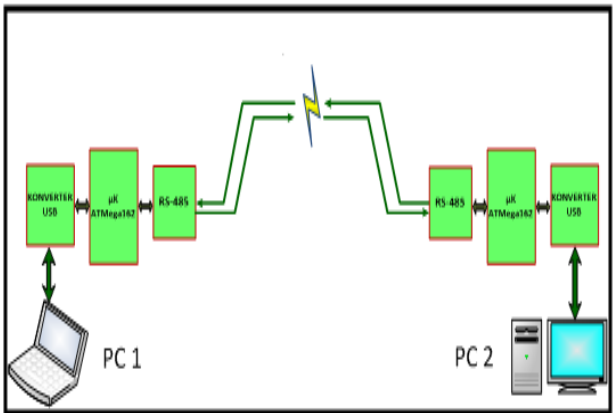
Universal Serial Bus (USB) adalah suatu protokol untuk pemindahan data ke dan dari alat digital, dan secara perlahan menggantikan RS-232 yang merupakan protokol komunikasi *peripheral*.USB menyediakan *bandwidth* yang luas, arus 500 mA, dan mengurangi pendukung pada PC yang berhubungan dengan permintaan perangkat keras.Untuk pengembangan sejumlah perangkat *peripheral*.Lebih dari 20 tahun, metoda komunikasi yang utama antara komputer dan perangkat pendukung dihubungkan dengan menggunakan protokol komunikasi RS-232. Sering dikenal sebagai *serial port*, RS-232 secara khas diterapkan sebagai 9 pin kabel yang memancarkan data secara berurutan, yakni TX (*Transmit data*) dan RX (*Receive data*) yang mengirimkan dan menerima data secara berurutan.

2.5 IC FT 232R USB - UART TTL

FT232R adalah USB ke perangkat *interface serial* UART yang menyederhanakan USB dengan desain serial dan mengurangi jumlah komponen eksternal dengan sepenuhnya mengintegrasikan EEPROM eksternal, USB resistor terminasi dan sirkuit jam terintegrasi yang tidak memerlukan kristal eksternal, ke dalam perangkat. Ini telah dirancang untuk beroperasi secara efisien dengan pengontrol *host* USB dengan menggunakan sesedikit mungkin dari total USB *bandwidth* yang tersedia.

2.6 Desain *Hardware*.

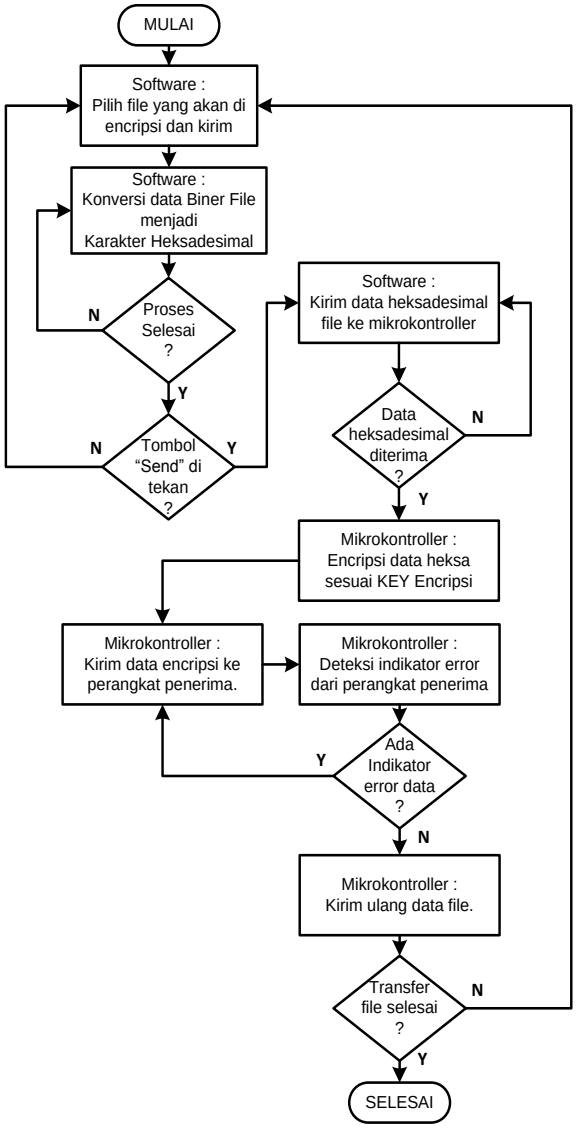
Beberapa perangkat keras yang tergabung membentuk suatu sistem yang dikendalikan oleh mikrokontroler ATMega162 sebagai pengendali utama pada pengacak data (enkripsi) dan mikrokontroler ATmega162 sebagai penerjemah atau mengembalikan data seperti semula (deskripsi). Pada blok diagram PC 1 dan PC 2 terdiri dari rangkaian penyesuai tegangan FT232RL mengubah level tegangan USB – UART TTL, AVR ATMega162, dan NRF905 sebagai pengirim dan penerima data, seperti yang terlihat pada blok diagram berikut ini :



Gambar 1. Blok Diagram Keseluruhan

Pada perencanaan dan pembuatan alat enkripsi data dibagi menjadi dua bagian utama, dimana pada bagian PC 1 terdiri dari pengirim data dari PC kemudian dienkripsi oleh mikrokontroler ATmega162 lalu di kirimkan melalui modul nRF905. setelah modul nRF 905 pada PC 2 menerima data maka akan dideskripsi oleh mikrokontroler ATmega162 menjadi data semula dan ditampilkan ke monitor. Begitu pula sebaliknya yang dikirim dari PC 2 diacak oleh mikrokontroler ATmega162 selanjutnya diterjemahkan kembali oleh mikrokontroler ATmega162

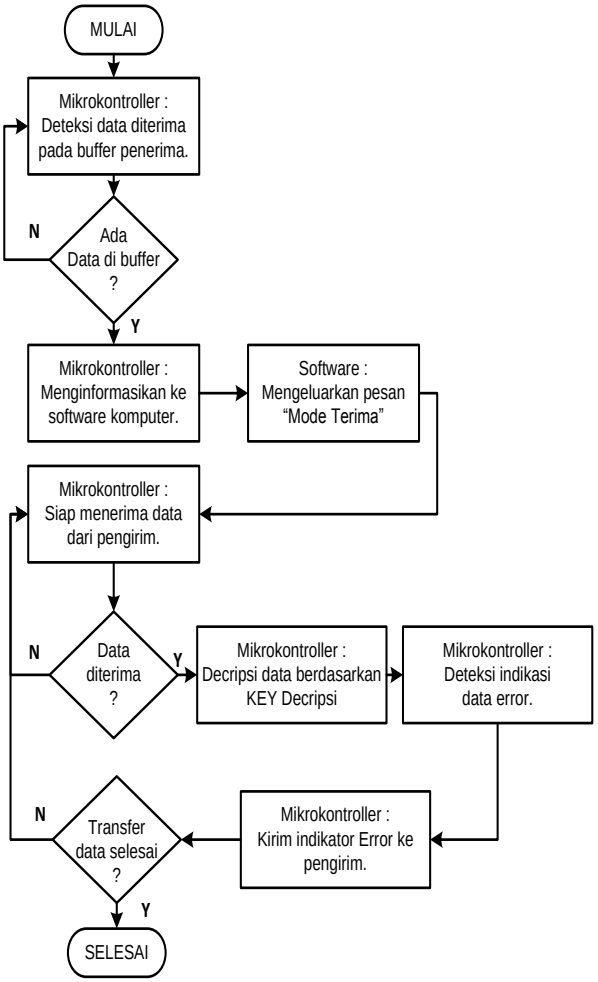
pada PC 1, sehingga terjadi saling komunikasi pertukaran data dimana data yang sudah teracak tersebut sulit untuk dipecahkan apabila terjadi penyadapan pada saat transmisi melalui wireless diantara bagian PC 1 dan bagian PC 2 setelah melewati rangkaian NRF905.
Untuk memudahkan dalam pembuatan piranti lunak terlebih dahulu dibuat definisi dari masing-masing *port* dan alur pikir dari rencana program yang dibuat.



Gambar 2. *Flowchart* pada proses pengiriman data

Tahap dalam perancangan system ini. Pertama memilih file yang akan kirimkan, data yang masih dalam bentuk file akan dikonversikan terlebih dahulu ke bentuk heks-bin karena proses enkripsi yang dilakukan harus pada bentuk heksadesimal. setelah proses selesai maka hasilnya akan dikirim ke mikrokontroler dan data heksadesimal yang telah diterima mikrokontroler akan langsung dienkripsi sesuai dengan key yang telah ditentukan di dalam mikrokontroler. Setelah data heksadesimal berhasil di enkripsi maka akan diteruskan ke nRF905 yang kemudian di transmisikan ke perangkat lain melalui gelombang wireless seperti pada gambar 2

Lalu pada gambar 3 terlihat bahwa mikrokontroler akan mendeteksi data telah diterima melalui modul NRF905dan akan menginformasikanya pada software komputer yang akan terlihat pada layar monitor. Setelah data diterima mikro kontroler akan mendiskripsikan berdasarkan key yang telah ditentukan.



Gambar 3. *Flowchart* pada proses penerimaan data

3. Hasil dan Analisa

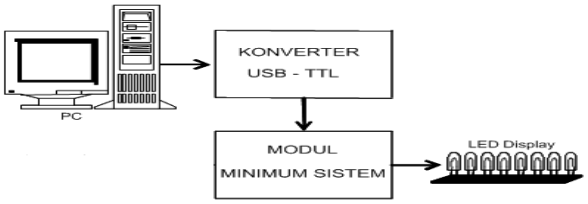
3.1 Sistem Mikrokontroler ATMEGA 162

Pada pengukuran Sistem Minimum Mikrokontroler ATMEGA 162 ini meliputi tegangan masing-masing *port* yaitu *port* A, *port* B, *port* C, dan *port* D, pada kondisi logika tinggi dan logika rendah. Langkah–langkah yang dilakukan untuk mengukur sistem minimum Mikrokontroler ATMega 162 adalah sebagai berikut:

1. Menghubungkan tegangan masukan pada catu daya 5 Volt dengan sistem minimum Mikrokontroler ATMega 162.

2. menggnduh program pengukuran yang sederhana dengan memberikan inputan masing-masing *port* pada kondisi logika tinggi.
3. Menjalankan program dengan ISP *programmer*.
4. Mengukur tegangan masing-masing *port*.
5. Ulangi langkah 2, 3, dan 4 untuk kondisi logika rendah.
6. Mencatat hasil pengukuran tegangan masing – masing *port*, baik pada kondisi logika tinggi maupun logika rendah.

3.2 Pengujian Rangkaian Konverter USB-UART TTL.



Gambar 4. Pengujian Konverter USB

Pengujian ini untuk mengetahui apakah rangkaian konverter USB-TTL dapat berfungsi sebagaimana yang direncanakan. Pengujian ini menggunakan alat bantu system ATMega162 dan Term95 sebagai program bantu pada PC. Satu *byte* kode (15H) dikirimkan dari minimum *system* ATMega162 lewat rangkaian konverter USB-TTL untuk menguji rangkaian dapat mengirimkan data dan satu *byte* selanjutnya akan diterima oleh minimum *system* ATMega162 untuk menguji rangkaian dapat menerima data dengan keluaran dalam level TTL yang hasilnya akan ditampilkan pada LED di Port 1.

3.3 Pengujian Pengujian Power Supply

Gambar 5. Pengujian power supply

3.4 Pengujian Wireless nRF905

Pengujian modul *wireless* bertujuan untuk mengetahui jarak jangkauan modul *Tranciever* nRF905. Dari data sheet nRF905 dikatakan bahwa modul ini mampu digunakan hingga mencapai jarak 3000 meter atau 3 Km. Pengujian dilakukan dengan cara memprogram perangkat *slave* untuk mengirim karakter "ABCDEFGH" kepada perangkat *master* setiap 1 detik, lalu data tersebut selanjutnya oleh *master* ditampilkan ke LCD serta dikirim ke komputer. Selanjutnya perangkat *slave* ditaruh pada jarak tertentu untuk mengetahui jarak maksimal transmisi datanya. Jika data yang diterima *master* tidak sama dengan data yang dikirim oleh *slave* atau tidak ada data yang diterima oleh *master* maka dikatakan jarak maksimal modul nRF905 telah tercapai. Tabel 1 menunjukkan hasil yang didapatkan setelah pengujian modul wireless nRF905.

Tabel 1. hasil pengujian modul nRF905

No.	Jarak	Hasil Data diterima *Master*
1	5 meter	ABCDEFGH
2	10 meter	ABCDEFGH
3	15 meter	ABCDEFGH
4	20 meter	ABCDEFGH
5	25 meter	ABCDEFGH
6	30 meter	ABCDEFGH
7	35 meter	Data kacau
8	40 meter	Kadang kacau , Kadang hilang
9	45 meter	Data hilang

Tabel 1. menunjukkan bahwa ketika jarak antara 5 meter hingga 30 meter data yang dikirim oleh *slave* dan data yang diterima oleh *master* sama, stabil, dan tanpa kehilangan data 1 *byte*. Akan tetapi ketika mencapai jarak 35 meter komunikasi data mulai kacau dan mulai kehilangan data ketika mencapai jarak 40 meter. Pada jarak 45 meter data benar-benar hilang dan pada perangkat *master* tidak terdeteksi data dari *slave*. Hal ini menunjukkan bahwa jarak maksimal agar komunikasi data menggunakan modul nRF905 dapat terjadi yaitu pada jarak 30 meter.

Hal yang menyebabkan jarak komunikasi modul *wireless* nRF905 tidak mampu mencapai jarak maksimalnya yaitu 3000 meter bisa disebabkan beberapa hal antara lain: Perangkat *power supply* yang tidak stabil dan daya yang tidak mencukupi, antena yang tidak sesuai dengan frekuensi kerjanya, perangkat atau rangkaian lainnya yang menkonsumsi daya lebih besar dari modul nRF905.

3.5 Enkripsi

Pada proses ini merubah data asli menjadi data yang disandikan. Awalnya terdapat 32 bit data asli/R(0) yang kemudian bit tersebut digeser sebanyak 4 kali ke arah kiri.Setelah itu hasil bit yang telah digeser di XOR-kan dengan bit kunci K(0) yang merupakan konstanta pada proses ini. Lalu hasil dari XOR ditambahkan (ADD) dengan bit kunci K(0) kembali sehingga akan muncul 32 bit yang susunanya berbeda dengan data aslinya.

Data :0001 0010 0011 0100 0101 0110 0111 1000

Shift :0010 0011 0100 0101 0110 0111 1000 0001
Hasil geser

Key :0001 0010 0011 0100 0101 0110 0111 1000

XOR :0011 0001 0111 0001 0011 0001 1111 1001
Hasil XOR

KEY :0001 0010 0011 0100 0101 0110 0111 1000

ADD :0100 0011 1010 0101 10001000 01110001
Hasil penjumlahan

3.6 Dekripsi

Pada bagian ini mengolah hasil dari proses enkripsi menjadi data asli. Hasil dari proses enkripsi dikurangi (SUB) dengan bit kunci K(0). Kemudian hasil dari pengurangan di XOR-kan dengan bit kunci K(0) kembali. Setelah itu digeser ke kanan sebanyak 4 bit maka akan diperoleh data asli R(0).

Data :0100 0011 1010 0101 10001000 01110001

KEY :0001 0010 0011 0100 01010110 01111000

SUB :0011 0001 0111 0001 00110001 11111001
Hasil Pengurangan

KEY :0001 0010 0011 0100 01010110 01111000

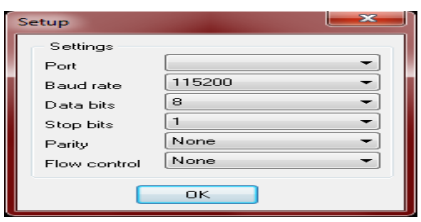
XOR :0010 0011 0100 0101 0110 0111 1000 0001
Hasil XOR

Shift : 0001 0010 0011 0100 01010110 011111000
Hasil Geser ke Kanan 4 bit

3.6 Pengujian Program

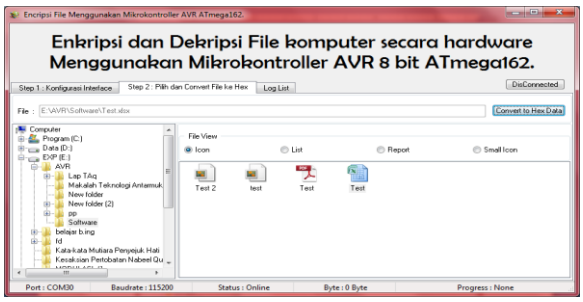
Gambar 6. Tampilan awal program

Pada gambar 6. diatas merupakan tampilan awal pada program yang berjalan di PC selanjutnya klik tombol *configuration.*



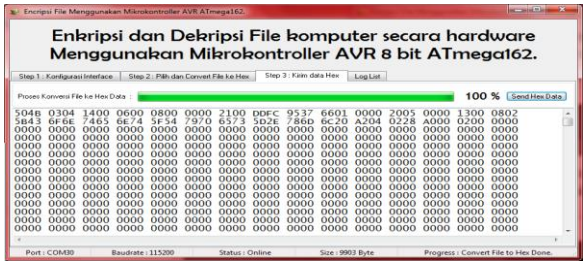
Gambar 7. Pilihan menu pada tombol *configuration*

Pada gambar 7 terdapat beberapa settingan yang bisa diubah, yang pertama memilih *port* USB yang digunakan oleh *hardware*. Kemudian memilih *baud rate* pada angka 115200 dikarenakan settingan *baud rate* pada mikro telah disetting di angka tersebut. Dan untuk *data bit, stop bit, parity*, dan *flow control* diikuti seperti gambar diatas. Setelah selesai menentukan *port* dan *baud rate* maka klik *connect* pada menu utama untuk menghubungkan alat dengan PC.



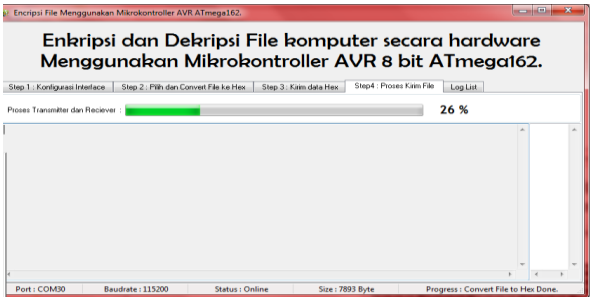
Gambar 8. Tampilan eksplorer pada OS

Setelah PC dan *hardware* terhubung maka dilanjutkan pada langkah kedua yaitu memilih file yang akan di enkripsi dan dikirimkan di tampilan explorer windows. Setelah file dipilih terus di *convert* terlebih dahulu ke bentuk heksadesimal baru bisa di transmisikan ke perangkat lain.



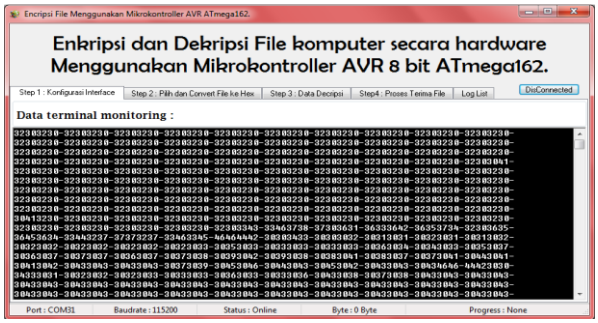
Gambar 9. Proses konversi data yang berupa file ke heksadesimal

Pada gambar 9. menunjukan hasil konversi yang berupa data heksadesimal yang selanjutnya dilakukan langkah berikutnya yaitu mengirim data heksadesimal ke perangkat PC yang lain melalui *wireless* sekaligus terinkripsi pada *hardware*.



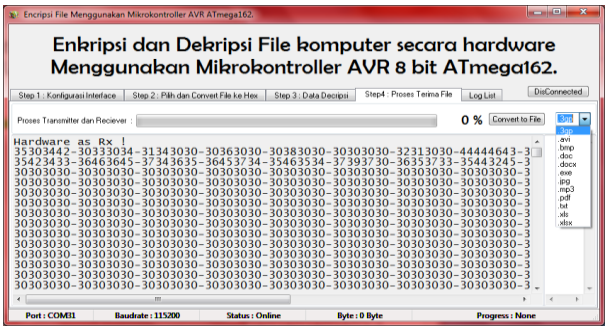
Gambar 10 Proses pengiriman file

Pada gambar 10 menunjukan proses pengiriman data melalui *hardware* yang di enkripsi terlebih dahulu sebelum di transmisikan oleh modul *wireless*



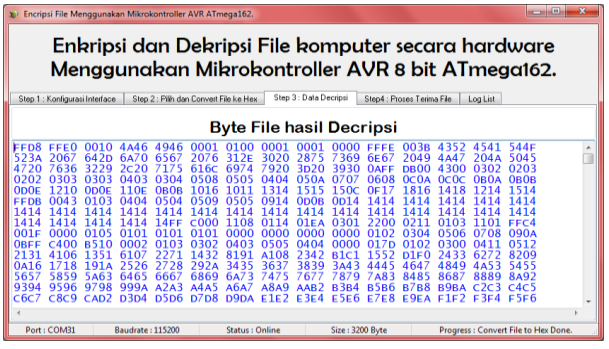
Gambar 11. Proses penerimaan data yang terenkripsi

Pada gambar 11. adalah menu utama program pada PC penerima, terlihat beberapa angka yang terkirim dan berjalan sampai semua file diterima.



Gambar 12. Adalah tampilan pada PC penerima saat file selesai diterima

Setelah semua file diterima maka langkah selanjutnya adalah mengkonvert file tersebut sesuai dengan format file yang dikirimkan.



Gambar 13. Proses dekripsi setelah semua file terkirim

Pada gambar 14 Menunjukan proses dekripsi dan hasil dari file yang sudah diterima sempurna

Gambar 15 Penerimaan file pada hardware yang tidak terdapat proses dekripsi

Pada gambar 15 Adalah hasil file yang diterima PC 3 yang diasumsikan sebagai attacker yang akan mencuri data saat file di kirimkan, tetapi tidak mengetahui proses enkripsinya. Jadi file yang diterima PC3 tidak bisa dibaca dan di konversikan ke bentuk file karena bit yang diterima telah teracak. Hal ini menjadi bukti bahwa file yang dikirim melalui hardware berupa file terenkripsi. Dan file terenkripsi tersebut dapat terdekripsi saat penerimaan file.

4.7 Pengujian Bit Rate

Pengujian ini untuk mengetahui berapakah kecepatan transfer file yang dijalankan dengan gelombang wireless yang dilakukan oleh modul nRF905. Langkah dari pengujian adalah dengan mencatat besarnya file yang akan dikirim dan juga mencatat waktu yang diperlukan saat pengiriman dari PC1 ke PC2 sampai file tersebut terkirim sepenuhnya.

Tabel 4.7 Percobaan bit rate

NO.	Besar File	Waktu Pengiriman	Transfer Rate
1.	4KB	28 s	1,14 Kbps
2.	8KB	64 s	1 Kbps
3.	10KB	78 s	1,02 Kbps
4.	11KB	88 s	1 Kbps
5.	17,7KB	147 s	0,93 Kbps
6.	25KB	198 s	1,01 Kbps

Menurut tabel 4.7 maka dapat diketahui bahwa semakin besar file yang dikirimkan maka waktu yang diperlukan akan semakin lama. Transfer rate akan didapatkan dengan membagi besarnya file yang dikirimkan dengan waktu yang dibutuhkan dari PC1 sampai PC2. Dari percobaan yang dilakukan nilai bit rate selalu berbeda. Contoh perhitungan bit rate sebagai berikut :

$$\text{Bit rate} = \frac{\text{Besar file}}{\text{Waktu}}$$

$$= \frac{8\ \text{KB}}{64\ \text{s}}$$

$$= 1\text{Kbps}$$

Dari beberapa percobaan yang dilakukan maka diperoleh waktu rata-ratanya sebagai berikut :

Bit rate rata2 = $\frac{(1{,}14 + 1 + 1{,}02 + 1 + 0{,}93 + 1{,}01)\ \text{Kbps}}{6}$

= 1,017 Kbps

4. Kesimpulan

1. Mikro kontroler 8 bit ATMega162 dapat digunakan untuk melakukan proses enkripsi dan dekripsi dengan baik.
2. Enkripsi jenis TEA efektif dalam pengamanan file.
3. Perangkat wireless tidak dapat menjadi pengirim sekaligus penerima pada waktu yang bersamaan.
4. Menurut ransfer percobaan yang dilakukan bit rate yang dihasilkan 1,017 Kbps.
5. Saat pengiriman file, Tx harus menerima report dari Rx terlebih dahulu setiap bitnya agar tidak terjadi kesalahan sehingga diperlukan waktu 2 kali lebih lama.

Saran

Adapun saran yang dapat diberikan sehubungan dengan pelaksanaan penelitian ini adalah :

1. Untuk mempercepat proses pengiriman data dapat dipasang 2 modul wireless pada 1 alat sehingga saat mengirimkan data bisa sekaligus sebagai penerima.
2. Dimungkinkan untuk membuat perangkat yang langsung bisa mendekripsikan file tanpa harus tau format pada data yang dikirim.

Referensi

[1]. Antea. **WiFi Transformasi Teknologi Data Digital.** New's PONSEL, Edisi 43, hal 28 – 29, Agustus 2005

[2]. Budiharto, Widodo & Gamayel Rizal. 2006. **Belajar Sendiri 12 Proyek Mikrokontroler Untuk Pemula**. Bekasi: Elex Media Komputindo.

[3]. Budiharto, Widodo & Sigit Firmansyah. 2004. **Elektronika Digital dan Mikroprosesor**. Jakarta: Penerbit Andi

[4]. Gunawan, A.H., Andi Putra, (2004), **Komunikasi Data via IEEE 802.11**, Dinastindo

[5]. Mulyanta, E., (2005), **Pengenalan Protokol Jaringan Wireless Komputer**, ANDI, Yogyakarta.

[6]. Sadikin, Rifky (2012). Kriptografi Untuk Keamanan Jaringan. Yogyakarta: Penerbit Andi

[7]. Sari, Yunita. 2009. **Perancangan Dan Implementasi Sistem Keamanan Data Menggunakan Algoritma Simetri TEA Dengan Bahasa Pemrograman Delphi 7.0.** Universitas Sumatera Utara.

[8]. Wheeler, David J. and Needham, Roger M. *TEA, a Tiny Encryption Algorithm*. ComputerLaboratory, Cambridge University, England. November, 1994.

[9]. Williams, D. 2008. **The Tiny Encryption Algorithm (TEA),** CPSC 6128 – **Network Security**, Columbus State University.

[10]. www.ftdichip.com/Documents/DataSheets/ICs/DS_**FT232R**.pdf