RANCANG BANGUN MODUL ENKRIPSI/DEKRIPSI TEKS BERBASISKAN GPRS SEBAGAI MEDIA PENGIRIMAN DAN PENERIMAAN DATA DENGAN MENGGUNAKAN ALGORITMA ENKRIPSI *STREAM CIPHER* ATHS3

Sandromedo Christa Nugroho[1], Immanuel CH.S.[2], Arif Fachru Rozi[3]
Lembaga Sandi Negara
Jl. Harsono RM No.70 Ragunan Ps.Minggu Jakarta Selatan -12550
Telp.021-7805814, Fax.021-78844104
major.ruft@gmail.com[1], nuel.ch@gmail.com[2], arif.fachru@gmail.com[3]

ABSTRAK
Paper ini akan membahas rancang bangun modul enkripsi/dekripsi teks berbasiskan GPRS sebagai media pengiriman dan penerimaan data dengan menggunakan algoritma enkripsi stream cipher ATHS3. Perancangan modul enkripsi/dekripsi menggunakan mikrokontroler AVR AT Mega 32 sebagai pemroses data yang telah terintegrasi kedalam rangkaian DT-AVR Low Cost Micro System (LCMS). Perangkat input yang digunakan adalah rangkaian keypad 4 x 4, perangkat outputnya menggunakan Modul LCD berdimensi 16 x 2, dan perangkat pengriman, dan penerimaan datanya menggunakan Modul GSM SIM 300 C dengan memanfaatkan media komunikasi GPRS (General Packet Radio Service) sebagai media pengiriman, dan penerimaan data. Hasil dari paper ini diharapkan dapat menjadi suatu solusi alternatif pengamanan pengiriman informasi yang bersifat rahasia, serta dapat mengatasi masalah-masalah pengiriman, dan penerimaan data yang terdapat pada alat, dan peralatan yang masih menggunakan media komunikasi PSTN (wireline atau guided transmission).

Kata Kunci: Pengiriman dan Penerimaan Informasi Rahasia, Modul Enkripsi/ Dekripsi, Algoritma Enkripsi Stream Cipher ATHS3, Media Komunikasi GPRS.

1. PENDAHULUAN

Era globalisasi telah memberikan dampak perubahan yang sangat besar bagi perkembangan ilmu pengetahuan, dan teknologi saat ini. Salah satu dampak perubahan pada perkembangan ilmu pengetahuan, dan teknologi tersebut adalah pada bidang komunikasi informasi, dahulu komunikasi informasi dilakukan secara sederhana dari mulut ke mulut, selain itu penyebaran informasi juga terbatas oleh adanya jarak, dan waktu, sehingga komunikasi informasi relatif sulit untuk dilakukan. Seiring dengan perkembangan teknologi, dan tersedianya sarana, serta prasarana komunikasi, maka komunikasi informasi telah menjadi suatu hal yang mudah untuk dilakukan.

Namun tidak semua informasi dapat dikomunikasikan secara bebas, dan tanpa pengamanan, salah satu contohnya adalah informasi yang bersifat rahasia, dimana informasi yang bersifat rahasia harus diamankan terlebih dahulu sebelum dikirimkan ke tujuannya, karena jika informasi rahasia tersebut disadap atau diketahui oleh pihak-pihak yang tidak berwenang, maka bukanlah tidak mungkin hal tersebut dapat mengancam keamanan, dan stabilitas suatu bangsa, dan negara.

Dengan mengetahui kenyataan tersebut, maka dibutuhkanlah suatu metode untuk mengamankan informasi rahasia, sehingga informasi rahasia yang dikirimkan oleh pengirim dapat benar-benar sampai ke tujuan yang wewenang. Salah satu teknik untuk mengamankan informasi rahasia adalah dengan menggunakan teknik penyandian/enkripsi. Penyandian/enkripsi merupakan proses menyembunyikan atau menyamarkan suatu informasi sedemikian rupa sehingga substansinya tidak dapat diketahui oleh pihak lawan.

Secara praktek alat, dan peralatan pengamanan informasi yang aktif beroperasi, dan digunakan di Indonesia masih memanfaatkan media komunikasi PSTN (*wireline* atau *guided transmission*) sebagai media pengiriman, dan penerimaan data, seperti misalnya mesin sandi buatan Telsy, Italy yaitu Allfax 3000i, CR-7000i, dan CR-9000i, demikian juga dengan mesin sandi buatan Hagelin Crypto, Swiss yaitu HC-4220, dan HC-4221,dan lain-lain.

Dalam melakukan pengiriman, dan penerimaan data media komunikasi PSTN memiliki beberapa kekurangan, antara lain mobilitas yang rendah, serta instalasi, dan perawatan yang kompleks baik di sisi pengguna (*user*), maupun di sisi penyedia (*provider*) jaringan media komunikasi PSTN, sehingga diperlukan biaya yang relatif bersar dalam mengoperasikan media komunisi PSTN. Selan itu pengiriman informasi rahasia dengan menggunakan media komunikasi PSTN di Indonesia sering mengalami kegagalan yang disebabkan oleh buruknya infrastruktur media komunikasi PSTN itu sendiri, dimana media komunikasi PSTN sering mengalami *drop*, jika digunakan untuk mengirimkan informasi rahasia yang telah dienkripsikan terlebih dahulu, sehingga pengiriman informasi rahasia harus dilakukan

 ISSN: 1907-5022

secara berulang-ulang, bahkan akhirnya mengalami kegagalan untuk dikirimkan.

Solusi alternatif yang dapat digunakan untuk mengatasi masalah-masalah tersebut adalah dengan menggunakan media komunikasi *wireless*, salah satunya adalah media komunikasi GPRS. GPRS (*General Packet Radio Service*) merupakan media komunikasi *wireless* yang memungkinkan suatu perangkat untuk dapat mengirimkan data ke tujuannya, dengan menggunakan paket-paket informasi. Penggunaan media komunikasi GPRS, memungkinkan pengiriman, dan penerimaan data dilakukan dengan lebih cepat, lebih efesien, dan lebih hemat biaya jika dibandingkan dengan menggunakan media komunikasi CSD (*Circuit Switch Data*), dan media komunikasi PSTN.

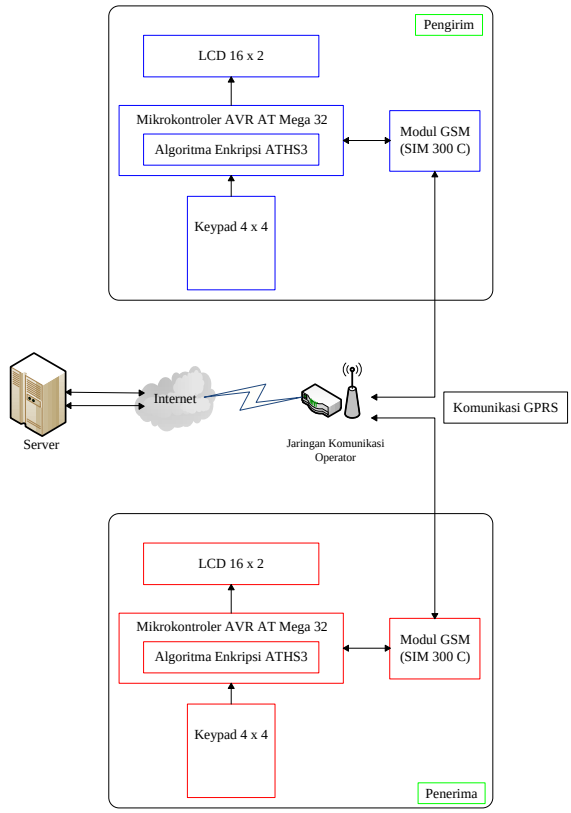
Selain itu layanan pengiriman, dan penerimaan data dengan menggunakan media komunikasi GPRS juga didukung oleh hampir seluruh *provider* jaringan komunikasi di Indonesia, sehingga dengan menggunakan media komunikasi GPRS, maka pengiriman, dan penerimaan data dapat dilakukan kapanpun, dan dimanapun tanpa terbatas adanya batas jarak, dan waktu, selama pengguna (*user*) masih memiliki pulsa, dan mendapatkan sinyal dari *provider* jaringan, atau dengan kata lain media komunikasi GPRS dapat mengatasi masalah-masalah yang terdapat pada media komunikasi PSTN (*wireline* atau *guided transmission*).

2. PERANCANGAN MODUL ENKRIPSI/ DEKRIPSI

Perancangan modul enkripsi/dekripsi dalam paper ini menggunakan mikrokontroler AVR AT Mega 32 sebagai pemroses data, dimana mikrokontroler AVR AT Mega 32 tersebut telah terintegrasi kedalam rangkaian DT-AVR *Low Cost Micro System* (LCMS) atau yang lebih dikenal juga dengan sebutan *minimum system* (*minsys*). Perangkat input yang digunakan dalam perancangan perangkat keras modul enkripsi/dekripsi ini adalah rangkaian *keypad* 4 x 4, perangkat outputnya menggunakan Modul LCD berdimensi 16 x 2, dan perangkat pengriman, dan penerimaan datanya menggunakan Modul GSM SIM 300 C dengan memanfaatkan media komunikasi GPRS (*General Packet Radio Service*) sebagai media pengiriman, dan penerimaan data.

Perancangan modul enkripsi/dekripsi teks berbasiskan mikrokontroler AVR yang dapat melakukan proses pengiriman, dan penerimaan data dengan menggunakan media komunikasi GPRS (*General Packet Radio Service*), setidaknya membutuhkan 2 (dua) buah modul enkripsi/dekripsi yang sama, yaitu 1 (satu) modul sebagai pihak pengirim, dan 1 (satu) modul lainnya sebagai pihak penerima. Modul enkripsi/dekripsi akan bekerja secara *stand alone* atau bekerja tanpa membutuhkan perangkat-perangkat tambahan lainnya. Namun perlu diketahui bahwa, modul enkripsi/dekripsi tersebut membutuhkan *power supply* sebagai sumber tegangan, dan *server* GPRS sebagai pihak ketiga yang berfungsi untuk meneruskan pengiriman data dari pihak pengirim data ke pihak penerima data.

Proses pengiriman, dan penerimaan data pada modul enkripsi/dekripsi ini akan bekerja secara 1 (satu) arah (*halfduplex*) atau dengan kata lain jika pihak A sedang mengirimkan data ke pihak B, maka pihak A tidak akan dapat menerima data dari pihak lainnya, demikian juga sebaliknya, jika pihak pihak B sedang menerima data dari pihak A, maka pihak B tidak akan dapat mengirimkan data ke pihak lainnya. Proses *halfduplex* tersebut diimplementasikan agar memudahkan pengguna (*user*) dalam melakukan pengiriman, dan penerimaan data ke pihak lainnya, serta mencegah adanya 'tumpang tindih' proses yang harus dikerjakan oleh modul enkripsi/dekripsi. Gambar 1. dibawah menunjukkan blok diagram perancangan modul enkripsi/dekripsi.

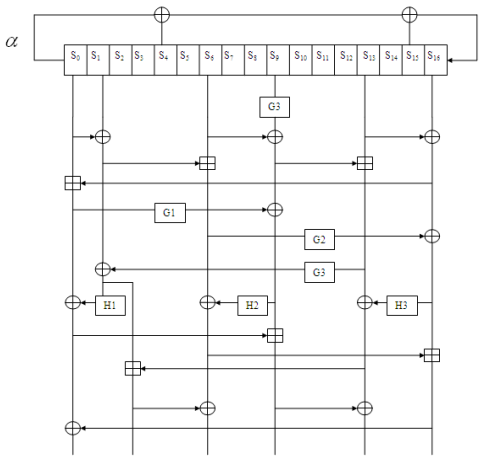


Gambar 1. Blok Diagram Perancangan Modul Enkripsi/Dekripsi.

3. IMPLEMENTASI ALGORITMA *STREAM CIPHER* ATHS3 PADA MODUL ENKRIPSI/DEKRIPSI

Algoritma enkripsi yang akan di*download*kan kedalam memori mikrokontroler AVR AT Mega 32 adalah algoritma enkripsi *stream cipher* ATHS3. Algoritma enkripsi *stream*

cipher ATHS3 merupakan algoritma berbasis *synchronous stream cipher*, dimana proses penyandiannya adalah dengan menggunakan operasi XOR *(exclusive-OR)* antara teks terang (*plainteks*) dengan rangkaian kunci output (*key stream*), sehingga menghasilkan teks sandi (*cipherteks*). Algoritma enkripsi *stream cipher* ATHS3 menggunakan kunci input (*seed*) sepanjang 128 bit, dan IV (*Initial Vector*) sepanjang 128 bit, dan pada setiap iterasinya, algoritma tersebut akan menghasilkan rangkaian kunci output (*key stream*) sepanjang 192 bit. Algoritma enkripsi *stream cipher* ATHS3 terdiri atas 3 (tiga) proses utama, yaitu proses inisialisasi awal, proses pembangkitan rangkaian kunci output (*key stream*), dan proses enkripsi/dekripsi. Algoritma enkripsi *stream cipher* ATHS3 terdiri atas 2 (dua) komponen utama yaitu : LFSR yang merupakan LFSR pada algoritma SOBER-128, dan fungsi F yang merupakan salah satu fungsi pada algoritma Dragon. Gambar 2. dibawah merupakkan algoritma *stream cipher* ATHS3.



Gambar 2. Algoritma *Stream Cipher* ATHS3.

Algoritma enkripsi *stream cipher* ATHS3 setidaknya membutuhkan alokasi memori sebesar 3172 Byte (sekitar 3 KiloByte), dengan rincian penggunaan memori sebagai berikut :

1. Kunci input *(Seed)* sebesar 128 bit (16 Byte).
2. IV (*Initial Vector*) sebesar 128 bit (16 Byte).
3. Fungsi-fungsi :
   a. Fungsi LFSR.
      i. 17 *stage*, setiap *stage* terdiri atas 32 bit (17 *stage* x 32 bit = 68 Byte).
      ii. Tabel Multab, terdiri dari 256 *entry* dengan setiap *entry* bernilai 32 bit (256 *entry* x 32 bit = 1024 Byte).
      iii. Sehingga total kebutuhan memori untuk fungsi LFSR adalah 68 Byte + 1024 Byte = 1092 Byte.
   b. Fungsi F (merupakan 6 (enam) *word* berukuran 32 bit yang berasal dari fungsi LFSR).
      i. 2 (dua) buah S-Box, terdiri dari 256 *entry* dengan setiap *entry* bernilai 32 bit (2 S-Box x 256 *entry* x 32 bit = 2048 Byte).
      ii. Sehingga total kebutuhan memori untuk fungsi F adalah 2048 Byte.
4. Berdasarkan perhitungan kebutuhan memori diatas, maka dapat diasumsikan kebutuhan memori untuk mengimplementasikan algoritma enkripsi *stream cipher* ATHS3 kedalam memori mikrokontroler AT Mega 32 adalah sebesar 16 Byte + 16 Byte + 1092 Byte + 2048 Byte = 3172 Byte (sekitar 3 Kilo Byte).

4. PENGUJIAN MODUL ENKRIPSI/ DEKRIPSI

Pengujian terhadap modul enkripsi/dekripsi dilakukan untuk dapat mengetahui apakah modul enkripsi/dekripsi tersebut dapat berfungsi dengan baik, dan benar. Tahap pengujian dilakukan dengan cara mengambil data, dan fakta yang terdapat pada hasil pengujian modul enkripsi/dekripsi, kemudian melakukan analisis terhadap data, dan fakta tersebut, untuk mengetahui kebenaran atau kesalahan proses, dan kinerja dari modul enkripsi/dekripsi.

4.1. Uji Vektor

Pengujian ini dilakukan dengan tujuan untuk mengetahui apakah pembangkitan rangkaian kunci output (*key stream*) pada algoritma enkripsi *stream cipher* ATHS3 yang telah diimplementasikan ke dalam *hardware* sama dengan pembangkitan rangkaian kunci output (*key stream*) pada algoritma enkripsi *stream cipher* ATHS3 dalam bentuk *software*. Tabel 1. dan 2. dibawah menunjukkan hasil uji vektor algoritma enkripsi *stream cipher* ATHS3.

Tabel 1. Hasil Uji Vektor Algoritma Enkripsi *Stream Cipher* ATHS3 Dalam Bentuk *Software*.

No.	Kunci Input dan IV	Kunci Output
1.	Kunci = 0x00000000000000000000000000000000	0x97fc1e5b0f4c63e7fa2510a25c95f5c2c772af955dea8050
	IV = 0x00000000000000000000000000000000	

Tebel 2. Hasil Uji Vektor Algoritma Enkripsi *Stream Cipher* ATHS3 yang Telah Diimplementasikan ke Dalam *Hardware*.

No.	Kunci Input dan IV	Kunci Output
1.	Kunci = 0x00000000000000000000000000000000	0x97fc1e5b0f4c63e7fa2510a25c95f5c2c772af955dea8050
	IV = 0x00000000000000000000000000000000	

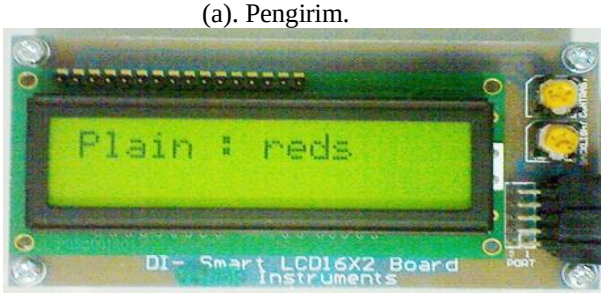
 ISSN: 1907-5022

Berdasarkan tabel hasil uji vektor diatas, dapat diketahui bahwa rangkaian kunci output (*key stream*) yang dihasilkan oleh algoritma enkripsi *stream cipher* ATHS3 yang telah diimplementasikan ke dalam *hardware* sama dengan rangkaian kunci output (*key stream*) yang dihasilkan oleh algoritma enkripsi *stream cipher* ATHS3 dalam bentuk *software*, dimana rangkaian kunci output (*key stream*) yang dihasilkan oleh algoritma enkripsi *stream cipher* ATHS3 terdiri dari 48 (empat puluh delapan) heksadesimal.

4.2. Pengujian Proses Enkripsi dan Dekripsi Data

Pengujian ini dilakukan dengan tujuan untuk mengetahui apakah mikrokontroler AVR AT Mega 32 dapat menjalankan program algoritma enkripsi *stream cipher* ATHS3 yang telah di*download*kan ke dalamnya, serta melakukan proses enkripsi, dan dekripsi terhadap data. Gambar 3.(a)., dan (b). dibawah menunjukkan hasil pengujian proses enkripsi, dan dekripsi data.

(a). Pengirim.



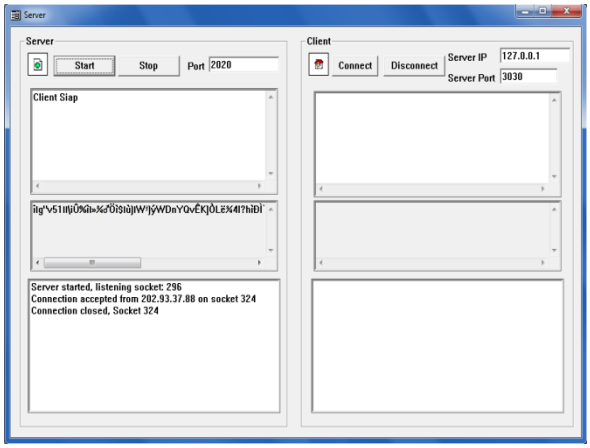
(b). Penerima.

Gambar 3.(a)., dan (b). Hasil Pengujian Proses Enkripsi, dan Dekripsi Data.

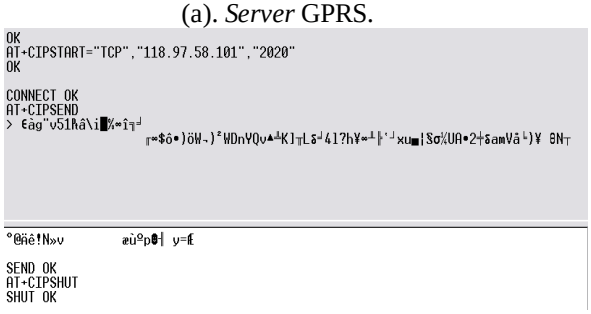
Berdasarkan gambar hasil pengujian proses enkripsi, dan dekripsi data diatas, dapat diketahui bahwa mikrokontroler AVR AT Mega 32 yang digunakan dapat menjalankan program algoritma enkripsi *stream cipher* ATHS3 yang telah di*download*kan ke dalamnya, serta melakukan proses enkripsi, dan dekripsi data, dengan menggunakan algoritma tersebut.

4.3. Pengujian Pengiriman dan Penerimaan Data

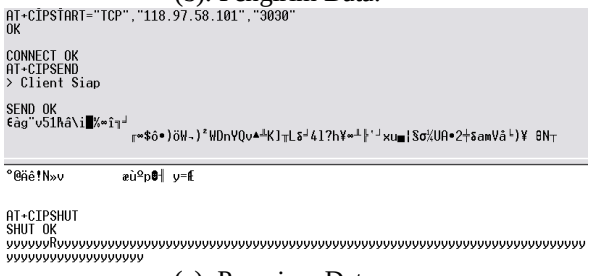
Pengujian ini dilakukan dengan tujuan untuk mengetahui apakah keseluruhan perangkat pada modul enkripsi/dekripsi yang telah diintegrasikan dapat bekerja, dan berfungsi sesuai dengan yang diharapkan, serta untuk mengetahui apakah media komunikasi GPRS dapat digunakan sebagai media pengiriman, dan penerimaan data terenkripsi pada modul enkripsi/dekripsi. Selain itu pengujian ini juga bertujuan untuk mengetahui seberapa jauh jarak pengiriman, dan penerimaan data yang dapat dilakukan oleh modul enkripsi/dekripsi tersebut. Gambar 4.(a)., (b)., dan (c). dibawah menunjukkan hasil pengujian pengiriman, dan penerimaan data dari pihak pengirim ke pihak penerima. Sedangkan tabel 3. dibawah menunjukkan hasil pengujian pengiriman, dan penerimaan data dengan menggunakan modul enkripsi/dekripsi di beberapa lokasi berbeda.



(a). *Server* GPRS.



(b). Pengirim Data.



(c). Penerima Data.

Gambar 4.(a)., (b)., dan (c). Pengiriman, dan Penerimaan Data Dengan Menggunakan Modul Enkripsi/Dekrispsi.

Tabel 3. Hasil Pengiriman, dan Penerimaan Data Dengan Menggunakan Modul Enkripsi/Dekripsi di Beberapa Lokasi Berbeda.

No.	*Server*	Lokasi	Titik	Lokasi	Titik	Lokasi	Estimasi Jarak Kirim Terima Data (Dalam KM)	Keterangan
1		Ciseeng		Pondok Gede		Pondok Gede	0	Sukses
2		Ciseeng		Pondok Gede		Kp. Gedong	2.8	Sukses
3		Ciseeng		Pondok Gede		Cililitan	3.1	Sukses
4	*Server*	Ciseeng	A	Pondok Gede	B	Cijantung	4.6	Sukses
5	GPRS	Ciseeng		Pondok Gede		Depok	14.6	Sukses
6		Ciseeng		Pondok Gede		Sawangan	18.1	Sukses
7		Ciseeng		Pondok Gede		Parung	21.6	Sukses
8		Ciseeng		Pondok Gede		Ciseeng	26.7	Sukses

Keterangan Tabel 3. :
Kondisi sukses = Kondisi dimana tidak terdapat kegagalan pengiriman data, dan *error* dari data yang diterima.
Kondisi *error* = Kondisi dimana terdapat kegagalan pengiriman data atau *error* dari data yang diterima.

Berdasarkan gambar pengiriman, dan penerimaan data dengan menggunakan modul enkripsi/dekripsi diatas, dapat diketahui bahwa seluruh perangkat yang telah diintegrasikan menjadi modul enkripsi/dekripsi dapat bekerja, dan berfungsi sesuai dengan yang diharapkan, serta dapat diketahui juga bahwa media komunikasi GPRS dapat digunakan sebagai media pengiriman, dan penerimaan data pada modul enkripsi/dekripsi. Namun perlu diperhatikan bahwa terdapat 1 (satu) buah *error* pada *plainteks* ke 7 (tujuh) hasil dekripsi karena, *cipherteks* hasil enkripsi yang berupa ASCII NULL (00000000_2), dan CTRL+Z (00011010_2) dikonversikan menjadi ASCII 1 (00000001_2), hal tersebut dilakukan agar tidak menggangu proses pengiriman, dan penerimaan data pada modul enkripsi/dekripsi, dimana dalam operasi string ASCII NULL merupakan akhir dari string, sedangkan ASCII CTRL+Z merupakan perintah eksekusi pengiriman data pada AT+CIPSEND. Selain itu dapat diketahui bahwa jarak yang memisahkan antara *server* GPRS, titik A, dan titik B tidak memberikan pengaruh terhadap hasil pengiriman, dan penerimaan data, dimana proses pengiriman, dan penerimaan data pada modul enkripsi/dekripsi dipengaruhi oleh sinyal yang berhasil ditangkap oleh Modul GSM yang terdapat pada modul enkripsi/dekripsi tersebut.

5. KESIMPULAN

Terdapat beberapa kesimpulan yang dapat diambil, terkait dengan dengan modul enkripsi/dekripsi pada paper ini, antara lain :

1. Algoritma enkripsi *stream cipher* ATHS3 dapat diimplementasikan ke dalam mikrokontroler AVR AT Mega 32.
2. Mikrokontroler AVR AT Mega 32 dapat digunakan sebagai pemroses data, yang terhubung dengan perangkat-perangkat input, dan output, serta Modul GSM pada modul enkripsi/dekripsi.
3. Media komunikasi GPRS dapat digunakan sebagai media pengiriman, dan penerimaan data pada modul enkripsi/dekripsi yang telah dirancang.
4. Dalam melakukan pengiriman, dan penerimaan data dengan menggunakan modul enkripsi/dekripsi yang telah dirancang, dibutuhkan sinyal yang baik, serta catu daya yang cukup besar, yaitu 5 Volt 2 Ampere, selain itu dibutuhkan sebuah *server* GPRS yang harus terhubung dengan internet, sebagai pihak ketiga untuk meneruskan data yang dikirim dari pihak pengirim ke pihak penerima, dimana jika *server* GPRS mengalami kerusakan atau *down* maka pengiriman, dan penerimaan data tidak dapat dilakukan, sehingga dibuuhkan operator untuk menjaga atau *memaintenance* kinerja dai *server* GPRS.
5. Data maksimal yang dapat dikirimkan dengan menggunakan media komunikasi GPRS, dalam 1 (satu) kali proses pengiriman adalah sebanyak 1 KB atau 1000 Byte.
6. Pihak penyadap yang melakukan kegiatan penyadapan terhadap pengiriman data dari pihak pengirim ke pihak penerima, hanya akan mendapatkan data dalam bentuk terenkripsi (*cipherteks*), sehingga data yang dikirimkan oleh pihak pengirim ke pihak penerima relatif aman terhadap ancaman kegiatan penyadapan yang dilakukan oleh pihak ketiga (pihak penyadap).
7. Jarak yang memisahkan antara *server* GPRS, titik A (pihak pengirim), dan titik B (pihak penerima) tidak memberikan pengaruh terhadap hasil pengiriman, dan penerimaan data, dimana proses pengiriman, dan penerimaan data pada modul enkripsi/dekripsi dipengaruhi oleh sinyal yang berhasil ditangkap oleh Modul GSM yang terdapat pada modul enkripsi/dekripsi tersebut, jika kondisi sinyal dalam keadaan baik, dan berhasil ditangkap oleh Modul GSM, maka pengiriman, dan penerimaan data akan berlangsung dengan baik (sukses), sedangkan jika kondisi sinyal dalam keadaan buruk, dan tidak berhasil ditangkap oleh Modul GSM, maka pengiriman, dan penerimaan data tidak akan berlangsung dengan baik (*error*).
8. Modul enkripsi/dekripsi yang telah dirancang dapat bekerja secara *half duplex* atau dapat menjadi pengirim data (*Tx*), dan penerima data (*Rx*), namun harus dilakukan secara bergantian.

DAFTAR PUSTAKA

Atmel Corporation. *Atmel AVR ATmega32 Datasheet.*

Balch, Mark. (2003). *Complete Digital Design.* McGraw-Hill Companies, Inc.

Delta Electronics. *DGSM-300.*

ETSI (*European Telecommunication Standards Institute*). (1998). *Cellular telecommunication system (Phase 2+); AT Command set for GSM Mobile Equipment (ME); GSM 07.07 version 7.4.0.*

Gunawan, Fransiskus. *AN (Application Note) 70*.

Hawke, Philip., Paddon, Michael., Rose, Gregory G. *Primitive Specification for SOBER-128*.

Innovative Electronics. (2005). *Quick Start DT-IO 4 x 4 Keypad*.

K. Chen, M. Henricksen, W. Millan, J. Fuller, L.Simpson, E. Dawson, H. Lee, S. Moon. *Dragon : A Fast Word Based Stream Cipher*.

Kurniawan Usman, Uke. *GPRS (General Packet Radio Service)*.

Menezes, Alfred J., Ooschot, Paul C. Van. & Vanstone, Scott A. (1997). *Handbook of Applied Cryptography*. Boca Raton : CRC press LLC.

Schneier, Bruce. (1996). *Applied Cryptography : Protocol, Algorithms and Source Code in C*. John Willey & Sons, Inc.

Simcom. *Sim 300 C GSM/GPRS Modul*.

Simcom. (2004). *AT command (for TCPIP) SIM100S Versi 4.0.8*.

Simcom. (2007). *TCP/IP AN (Application Notes) Versi 1.02*.

Simcom. (2009). *Sim 300 C Hardware Design Versi 2.08*.

Stalling, Wiliams. (1999). *Cryptography and Network Security : Principles and Practice 4nd Edition*. New Jersey : Prentice Hall, Inc.

Sumarkidjo, dkk. (2007). *Jelajah Kriptologi*. Buku tidak diterbitkan. Jakarta. Lembaga Sandi Negara Republik Indonesia.

Tommy PM. (2003). *Pengantar Konsep dan Aplikasi TCP/IP Pada Windows NT Server*.

Ula, Mutammimul. (2008). *Sistem Pengingat Ujian Mahasiswa Berbasis SMS*. Yogyakarta. Universitas Islam Indonesia.

Undang-undang Nomor 32 Tahun 2002 Tentang Penyiaran.