JUKOMIKA - (JURNAL ILMU KOMPUTER DAN INFORMATIKA)
Volume 4, Nomor 2, Desember 2021 P-ISSN/ E-ISSN: 2655-755X/ 2723-8091

Implementasi Algoritma Grain VI Pada Pengiriman Pesan Suara

Andilala (✉)
Universitas Muhammadiyah Bengkulu, Bengkulu, Indonesia
andilala@umb.ac.id

Andilala [1], Ujang Juhardi[2]
Universitas Muhammadiyah Bengkulu, Bengkulu, Indonesia
andilala@umb.ac.id

Abstrak— Pembuatan aplikasi keamanan pesan suara dengan menggunakan algoritma Grain VI bertujuan untuk menerapkan keamanan bagi pengirim pesan suara yang penting atau rahasia. Pada penelitian ini penulis membangun sebuah sistem komunikasi dengan metode pengiriman pesan yang dilakukan memalui jaringan peer to peer. Aplikasi ini dapat membantu mempermudah dalam hal menyampaikan informasi pesan suara lintas bidang dari sub bidang kepengurusan dalam hal menyampaikan informasi pesan suara, komunikasi (Sumber pesan) harus datang langsung ke tujuan pesan. Aplikasi ini juga dapat di uji menggunakan pengujian blackbox untuk mendapatkan keberhasilan penerpan algoritma pada aplikasi ini, dengan hasil pengujian berhasil dari setiap element yang diujicobakan pada aplikasi.

Abstract— *Making voicemail security applications using the Grain VI algorithm aims to implement security for important or secret voicemail senders. In this study, the authors build a communication system with the method of sending messages through a peer to peer network. This application can help make it easier to convey voice message information across fields from the management sub-sector in terms of conveying voice message information, communication (the source of the message) must come directly to the destination of the message. This application can also be tested using blackbox testing to get the success of implementing the algorithm in this application, with the successful test results of each element being tested on the application.*

Keywords*: Grain, VI, sound, message, security.*

1 Pendahuluan

Komunikasi merupakan aspek yang cukup penting dalam kehidupan manusia. Komunikasi diperlukan untuk menyampaikan suatu informasi. Banyak ragam komunikasi, salah satunya adalah komunikasi suara. Komunikasi suara merupakan hal yang sering dilakukan dalam kehidupan sehari-hari,Seperti komunikasi suara dengan telepon yang berbasis analog dan telepon seluler yang berbasis digital [1]. Bahkan, saat ini komunikasi suara dapat dilakukan melalui jaringan internet yang lebih dikenal dengan Voice Over Internet Protokol (VoIP). Berbagai alat komunikasi suara yang ada saat ini belum tentu aman untuk digunakan,karena belum ada standar keamanan yang dapat digunakan oleh alat-alat tersebut. Oleh karena itu komunikasi ini sangat rentan terhadap serangan pihak ketiga yang merugikan sehingga diperlukan sistem keamanan komunikasi pesan suara [1][2].

Hal yang penting dalam komunikasi data antar komputer melalui jaringan adalah keamanan data Keamanan data bisa dijaga dengan berbagai cara, salah satunya adalah dengan cara melakukan enkripsi terhadap data yang dikirimkan. Dengan enkripsi, user lain tidak bisa membaca data yang kita berikan [1].

Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa di dekripsi. Proses enkripsi yaitu dengan mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Pengetahuan yang mempelajari tentang enkripsi disebut kriptografi [3].

Enkripsi simetris adalah kode hill atau lebih dikenal dengan stream chiper yang merupakan salah satu algoritma kriptografi kunci simetris. Enkripsi asimetris menggunakan dua buah kunci yang berbeda untuk enkripsi – dekripsi, yaitu kunci publik dan kunci private.Secara umum enkripsi dibagi menjadi dua jenis, yaitu enkripsi simetris dan enkripsi asimetris [4][5].

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 chiper bisa digunakan untuk digunakan enkripsi simetris maupun asimetris [5].

Algoritma Grain VI merupakan algoritma stream cipher. Stream cipher beroperasi dalam bentuk per-bit, yang dalam hal ini rangkaian bit dibagi menjadi per-bit yang panjangnya sudah ditentukan sebelumnya sehingga harus dilakukan penyesuaian pada algoritma ini Salah satu cara yang dapat digunakan dalampenyesuaian mode operasi yang digunakan yaitu dengan mengubah kecepatan dan efisiensi enkripsi cipher blok menjadicipheraliran mode operasi counter [6][7]. Penerapan Algoritma Grain VI dengan mode operasi counter untuk melakukan enkripsi pada aliran pesan suara dalam satu arah dan mempresentasikan enkripsi stream cipher,sehingga pembicaraan yang bersifat khusus dan rahasia tidak dapat dilacak atau diketahui oleh pihak lain yang tidak bertanggung jawab. Dengan demikian komunikasi suara yang dilakukan dapat berlangsung lebih aman dan nyaman karena pengguna tidak khawatir terhadap keamanan pembicaraan yang sedang dilakukan.

2 Studi Literatur

2.1 Enkripsi

Terdapat beberapa teknik enkripsi yang digunakan dalam suatu komunikasi data pada jaringan komputer yang artinya tersembunyi atau suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa di dekripsi (kebalikan dari proses enkripsi) dahulu. Encryptionberasal dari bahasa yunani kryptos yang artinya tersembunyi atau rahasia. Enkripsi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi yang aman, terutama untuk memastikan integritas dan autentikasi dari sebuah pesan. Contohnya, Message Authentication Code (MAC) atau digital signature. Penggunaan yang lain yaitu untuk melindungi dari analisis jaringan [1]

2.2 Grain VI

Grain VI adalah termasuk dalam enkripsi stream chiper yang memiliki kunci simetris. Grain chiper adalah bit oriented synchronous stream ciper. Pada synchronous strem chiper, kunci yang dibangkitkan secara terpisah dari plain text. Grain chiper sebuah fungsi penyaringan (filter) AlgoritmaGrain VI merupakan algoritma stream cipher. Stream cipher beroperasi dalam bentuk per-bit, yang dalam hal ini rangkaian bit dibagi menjadi per-bit yang panjangnya sudah ditentukan sebelumnya. Sehingga harus dilakukan penyesuaian pada algoritma ini.[8].

Ada juga yang berpendapat Grain VI adalah stream cipher,Grain VIdirancang terutama untuk lingkungan hardware terbatas.Ia menerimakunci 80-bit dan 64-bit.Spesifikasi tidak direkomendasikan panjang maksimum output perpasangan. Sejumlah potensi kelemahan dalam cipher telah diidentifikasi 160-bit keadaan internal Grains terdiri dari 80-bit baris register geser umpan balik dan 80-bit non linear register geser umpan balik [9].

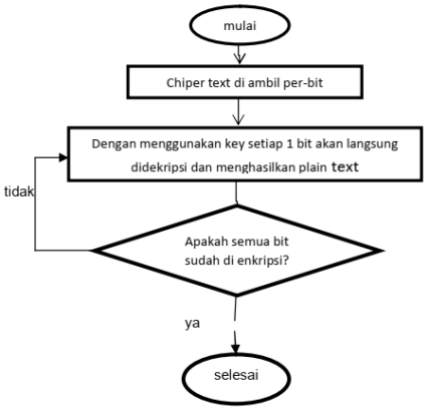

Fig.1. Flowchart proses Enkripsi menggunakanAlgoritmaGrain VI (Dimas Zulhasmi Wigraha)

3 Metodologi

Fig.2. Alur Penelitian

Pengumpulan Data
Data penelitian dihimpun melalui dua metode pengumpulan data yaitu:

- Metode Studi Pustaka
  Studi pustaka dilakukan dengan mengumpulkan teori, konsep dan data dari buku-buku mengenai bahasa pemrograman komputer.sistem keamanan, dan algoritma pemrograman. Data juga diperoleh dari artikel dan jurnal yang berasal dari internet.
- Metode Observasi
  Data penelitian dikumpulkan dengan melakukan pengamatan atau observasi secara langsung terhadap sistem pengiriman pesan suara
  Metode Perancangan Sistem

Analisa Sistem Aktual
Sebelum melakukan pengembangan sistem, maka perlu dilakukan pengamatan terhadap sistem yang berjalan. Penulis memperoleh informasi dari PT. Telkom Catel Bengkulu bahwa saat ini mereka masih menggunakan menggunakan cara sederhana dalam hal menyampaikan informasi seperti halnya orang yang akan menyampaiakan informasi atau sebaliknya harus bertemu pada suatu waktu dengan tujuan menyampaikan informasi dan belum memiliki program tersendiri untuk menyampaikan informasi sehingga membutuhkan waktu yang cukup banyak untk pengerjaan hal tersebut

Perancangan Aplikasi
Sistem pengiriman data suara yang akan di rancang dengan memasukan suara melalui microphone kemudian diubah menjadi bit digital. Untuk memperkecil ukuran data suara yang akan diproses, dilakukan proses kompresi. Hasil dari kompresi ini nantinya akan enkripsi dengan algoritma Grain VI dan dikirimkan melalui kabel jaringan. Penerima akan melakukan dekripsi terhadap data suara yang dikirimkan. Hasil dekripsi kemudian di didekompresi dan dikeluarkan melalui speaker agar dapat didengarkan kembali.

Langkah awal yang dilakukan yaitu dengan memasukan file audio oleh pengguna pertama. Data suara di digitalisasi sehingga menghasilkan file audio digital yang dapat diolah oleh komputer. Langkah berikutnya adalah kompresi (pengecilan ukuran) file audio digital sehingga memiliki ukuran yang lebih kecil sehingga lebih mudah untuk dianalisis. Hasil kompresi file audio kemudian dienkripsi sebelum dikirimkan melalui jaringan.

Penggunaan kedua juga melakukan prosedur yang sama dengan pengguna pertama untuk mengirimkan file dan audio, sehingga proses pengiriman dan penerimaan dan penerimaan suara dalam dilakukan secara aman karena telah melalui tahap enkripsi dan dekripsi. Proses digitalisasi suara adalah tahapan pengubahan sinyal suara analog menjadi digital. Sinyal suara analog didapat dari microphone sedangkan perangkat digitalisasi suara adalah soundcard. File hasil digitalisasi suara terdapat dalam berbagai format, yaitu wav. File wav memiliki ukuran yang cukup besar, sehingga kurang efisen apabila langsung dikirim melalui jaringan, karena dapat membebani jaringan dan menambah waktu pengiriman data, oleh karena itu file ini perlu dikompres dalam mp3 atau sejenisnya yang memiliki ukuran yang lebih kecil.

File hasil kompresi kemudian dienkripsi sehingga tidak dapat dibaca oleh pengguna lain, kecuali komputer yang memiliki program dekripsi yang sesuai. Program dekripsi bertugas untuk mengembalikan pola file menjadi seperti sebelum enkripsi.

4 Hasil dan Pembahasan

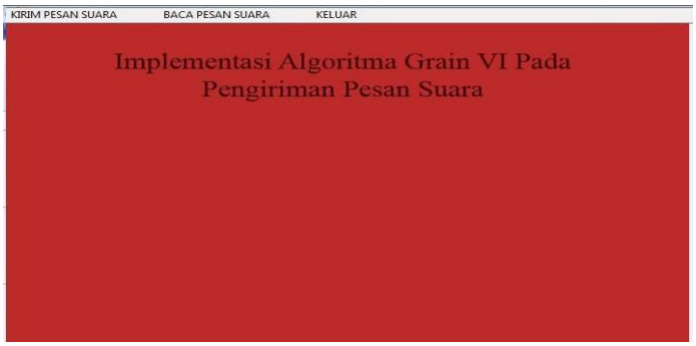

Fig.3. Tampilan Awal Apliaksi

Menu Kirim Suara

Menu ini merupakan fasilitas pengiriman pesan suara yang ada di rancangan sofware ini, Untuk memasuki menu ini anda bisa mengeloik tombol Kirim pesan suara yang ada di menu utama.

Setelah menekan tombol kirim pesan suara maka anda di minta untuk mengisi pasword, silahkan isi pasword anda. Kalau anda berhasil memasukan pasword anda maka anda dapat mengirimkan pesan suara di fasilitas pengiriman pesan suara pada rancangan sofware ini.

Baca Pesan Suara

Untuk membaca atau mendengarkan pesan suara yang dikirim anda bisa mengelik tombol baca pesan suara, akan tampil seperti gambar dibawah ini:

Fig.4. Dengar Pesan Suara

Pengujian software

Menggunakan metode black box. Metode ini digunakan untuk mengetahui apakah perangkat lunak berfungsi dengan benar. Adapun hal-hal yang akan diujikan menggunakan metode black box ini adalah sebagai berikut :

a. Pengujian Login

Berikut ini adalah hasil pengujian sistem menggunakan metode black box berdasarkan requiment pada rencana pengujian :

Table.1. Blacbox Testing Login

Data yang dimasukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
User name dan password terisi dengan benar	Akan menampilkan form utama	Menampilkan form utama	[√] Diterima [ ] Ditolak
User name dan Password kosong atau user name dan Passwor salah	Akan menampilkan "Kode yang anda masukan salah"	Akan menampilkan "Kode yang anda masukan salah"	[√] Diterima [ ] Ditolak

b. Pengujian Data

Table.2. Blacbox Testing Data

Kasus dan Hasil Uji (Data Normal)			
Data yang dimasukan	**Yang diharapkan**	**Pengamatan**	**Kesimpulan**
Klik "Tambah"	Tombol yang aktif hanya tombol "Kirim" dan "Batal"	Dapat mengisi tiap field sesuai yang diharapkan	[√] Diterima [ ] Ditolak

Mengisi textbox tiap field Klik "Simpan"	Data tersimpan	Tombol "Kirim" dapat berfungsi sesuai dengan yang digharapkan	[√] Diterima [ ] Ditolak

5 Kesimpulan

Aplikasi keamanan pesan suara dengan menggunakan algoritma Grain VI ber-tujuan untuk menerapkan keamanan bagi pengirim pesan suara yang penting atau rahasia sistem komunikasi dengan metode pengiriman pesan yang dilakukan memalui jaringan peer to peer. Aplikasi ini dapat membantu mempermudah dalam hal menyampaikan informasi pesan suara lintas bidang dari sub bidang kepengurusan dalam hal menyampaikan informasi pesan suara, komunikasi (Sumber pesan) ha-rus datang langsung ke tujuan pesan. Aplikasi ini juga dapat di uji menggunakan pengujian blackbox untuk mendapatkan keberhasilan penerpan algoritma pada ap-likasi ini, dengan hasil pengujian berhasil dari setiap element yang diujicobakan pada aplikasi

6 Daftar Pustaka

[1] Anggi, (2009). Tugas Akhir : Studi dan Implementasi Enkripsi Pengiriman Suara Menggunakan Algoritma Twofish. Jurusan Teknik Informatika, Fakultas Teknologi Industri, Institut Teknologi Bandung.
[2] Herlambang, dkk. (2010). Tugas Akhir: Analisis Algoritma Enkripsi ElGamal, Grain VI, dan AES dengan Studi Kasus Aplikasi Resep Makanan.
[3] Meier, W.(2005) A Stream Cipher Proposal: Grain-128. estream, ECRYPT Stream Cipher Project. http://www.ecrypt.eu.org/stream.
[4] Martin Hell, (2005). Grain - A Stream Cipher for Constrained Environments Rudi, 2011. Keamanan Jaringan dan Enkripsi Data, IPB, Bandung
[5] Supriyanto, (2007),Komunikasi Jaringan Komputer Enkripsi Deskripsi Tamatjita, 2006. Kriptografi Untuk Perlindungan Data
[6] Wigraha, Dimas Zulhazmi. (2012). Tugas Akhir : Analisi Algoritma Enkripsi Elgamal Grain VI dan Aes Dengan Studi Kasus Aplikasi Resep Makanan. Jurusan Teknik Informatika, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh November.
[7] Syahifudin Shahid (2018) Implementasi Algoritme Grain V1 Dan 128 Bit Pada Raspberry PI, Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, Vol. 2, No. 4, April 2018, hlm. 1572-1581
[8] FAIQ NAJIB AL-AZIZ (2020). Analisis Algoritma Enkripsi Grain V1 Dan Espresso Pada Iot Dengan Studi Kasus Aplikasi Rfid, Universitas Telkom Indonesia. Jakarta
[9] Mohammad Ubaidullah Bokhari. 2014. A Detailed Analysis of Grain family of Stream Ciphers. I.J. Computer Network and Information Security

7 Penulis

	Andilala, M.Kom Fakultas Teknik Program Studi Sistem Informasi Universitas Muhammadiyah Bengkulu
	Ujang Juhardi, M.Kom Fakultas Teknik Program Studi Teknik Informatika Universitas Muhammadiyah Bengkulu