ENKRIPSI DAN DEKRIPSI PESAN SUARA DENGAN METODE ALGORITMA SERPENT MENGGUNAKAN VISUAL BASIC 6.0

Mokh. Lugas Adi Patra[1]

[1,3]*Jurusan Teknik Informatika-S1, Fakultas Ilmu Komputer,*
Universitas Dian Nuswantoro Semarang
Jln. Nakula I no 5-17 Semarang 50131 INDONESIA
[1]111201005515@mhs.dinus.ac.id

Teknologi komputer yang semakin canggih dan perkembangan zaman yang semakin modern, fasilitas untuk berkomunikasi menjadi lebih nyaman. Tetapi seiring dengan perkembangan teknologi komunikasi tersbut sistem keamanan belum diperhatikan sehingga muncul pengguna yang menyalahgunakan celah keamanan sebagai peretas jaringan untuk tujuan tertentu. Usaha untuk mengamankan supaya keamanan dalam berkomunikasi dilakukan dengan cara mengamankan data yang akan dikirim kejaringan ke pengguna yang di tuju. Komunikasi suara berupa data yang telah di encode ke sinyal digital dapat di amankan supaya tidak bisa di sadap oleh pengguna yang tidak diinginkan. Dari sisi jaringan sistem sudah berjalan dengan keamanan yang memadai akan tetapi data yang dikirim masih bisa digunakan sebagai celah keamanan. Oleh karena itu pengamanan yang dilakukan dengan algoritma yang ada perlu dilakukan. Metode-metode pengamanan data bermacam-macam seperti Algoritma Rijndael, RC4, Serpent dsb. Diantara metode-metode pengamanan data Algoritma Serpent menjadi pilihan untuk mengamankan sebuah data dalam jaringan. Metode Algoritma serpent merupakan algoritma yang aman selain Algoritma Rijndael dan RC4 untuk enkripsi data sebab belum ada kasus yang membahas tentang peretasan Algoritma Serpent. Data suara yang berupa sinyal digital akan dienkripsi terlebih dahulu kemudian dikirim melalui media jaringan dan ketika data suara yang telah dienkripsi sampai ke penerima proses selanjutnya adalah mendekripsi data suara yang telah diterima dengan metode yang sama. Syarat mengenkripsi data di dalam algoritma Serpent ini adalah menggunakan key sebagai katakunci rahasia yang akan dia gunakan oleh pengirim dan penerima dalam mengenkripsi dan mendekripsi data. Key yang digunakan hanya diketahui oleh pengirim dan penerima oleh karena itu dengan adanya key untuk mengenkripsi dan mendekripsi data proses komunikasi dalam jaringan menjadi lebih aman. Dalam Metode Algoritma Serpent memuat cipher block yang berfungsi untuk mengelompokkan bit-bit sinyal digital menjadi block-block dengan ukuran bit tertentu.
Kata kunci—Voip, Metode Algoritma Serpent, Enkripsi dan Dekripsi File, Kriptografi..

The Computer Technology is advanced and the Era is become modern, Facility for Communicating becomes comfortable. but the communication security in the network is not observed. so there are many people can find the security gap. they are collecting more information to hack a network for particullar purpose.The communication is Data that converted to digital signals. so, the efforts to build the security of communication is do encryption and decryption on the data that will be sent to the recipient. There are many methods for build security such as Rijndael Algorythm, RC4 Algorythm, Serpent Algorythm etc. between the methods there is one of many that most powerfull algorythm specifically is Serpent.The signal data will be sent and accepted with the same methods. Serpent Algorythm encrypt and decrypt file with their methods, serpent change the digital signal into blocks form. so that can be applied to digital signal audio.
Keywords*—Voice Over IP, Serpent Algorythm Metode, File encryption and decryption, Cryptography.*

I. PENDAHULUAN

Pada masa sekarang ini, dimana semua peralatan sudah berbasis komputer pengguna bisa berkomunikasi lewat jaringan menggunakan komputer dengan mudah. Dalam hal ini komunikasi suara sering digunakan untuk berinteraksi dengan keluarga, sahabat dan teman-teman yang jauh bahkan sampai di seberang pulau. Banyak sekali jenis alat komunikasi yang digunakan seperti telepon dengan basis analog ataupun telepon dengan basis digital akan tetapi keamanan belum diperhatikan. maka sering terjadi kasus-kasus penyadapan melalui komunikasi suara dari pihak – pihak tertentu.

Untuk membuat sebuah pengamanan pada kasus ini perlu dilakukan enkripsi pada suara yang akan di kirimkan ke penerima supaya ketika proses pengiriman data suara tidak ada pihak ketiga yang dengan mudah ikut mendengar isi dari percakapan yang dilakukan oleh pengguna. Enkripsi biasanya dilakukan oleh alat berupa hardware ataupun software.

Dalam melakukan proses enkripsi banyak sekali metode – metode yang digunakan. Algoritma yang digunakan untuk mengenkripsi file suara bermacam –macam ada algoritma Rijndael, algoritma Serpent, dan algoritma RC6. Diantara algoritma tersebut penulis menggunakan Algoritma Serpent sebagai metode yang dipakai[1]. Algoritma Serpent adalah algoritma yang cukup kuat yang hingga sekarang masih belum ada laporan serangan – serangan mengenai penyadapan dari kriptanalis yang mampu dan berhasil merusaknya. Algoritma Serpent juga tidak dipatenkan, sehingga penggunaannya untuk melakukan enkripsi tidak memerlukan adanya biaya.

Pada suatu proses komunikasi, komputer akan melakukan enkripsi pada suara sebelum dikirimkan ke penerima yang kemudian didekripsi oleh penerima menjadi sebuah suara yang utuh. Pada prosesnya ada sedikit delay yang disebabkan komputer harus melakukan perubahan dari suara yang asli menjadi suara yang terenkripsi.

Untuk mengurangi delay pada komunikasi ini, ada yang

harus dilakukan yaitu dengan penyesuaian pada algoritma serpent. Salah satunya yang dapat dilakukan adalah dengan menyesuaikan mode operasi yang digunakan. Saat ini, mode operasi yang banyak digunakan pada Algoritma Serpent adalah Cipher Block Chaining (CBC). Tetapi mode operasi ini tidak akan meningkatkan kecepatan enkripsi Serpent karena enkripsi dilakukan secara sekuensial [2].

Salah satu mode operasi yang dapat digunakan untuk mengubah kecepatan dan efisiensi enkripsi cipher blok menjadi menyerupai cipher aliran adalah mode operasi counter. Oleh karena itu, pada tugas akhir ini dipilih penerapan Algoritma Serpent dengan mode operasi yang disesuaikan menjadi mode operasi counter untuk melakukan enkripsi pada aliran pesan suara dalam dua arah [3].

II. STUDI PUSTAKA

2.1. Penelitian Terkait

Ada beberapa referensi yang diambil penulis sebagai bahan pertimbangan untuk penelitian yang dilakukan, referensi tersebut diambil dari beberapa penelitian yang dilakukan sebelumnya yang membahas tentang permasalahan yang hampir sama, antara lain :

Penelitian oleh Muhammad Fauzan Edy Purnomo, Wahyu Adi Priyono, Sapriesty Nainy Sari, Rusmi Ambarwati dan Asri Wulandari dengan judul *Implementasi Algoritma Kriptografi RC4 Pada DSP TMS320C6713 Sebagai Pendukung Sekuritas Jaringan Komunikasi Voice over Internet Protocol (VoIP)* Penelitian ini membahas tentang sebelum file suara di enkripsi ada sebuah proses untuk melakukan pengecekkan terhadap file suara apakah valid atau tidak. Proses ini dilakukan bertujuan untuk memeriksa dan memastikan sinyal suara masuka pada line input TMS320C6713 sebagai suatu sinyal informasi yang masih asli sebelum sinyal suara tersebut diacak. Pengamatan yang dilakukan pada pengujian ini adalah kekonsistensian sebuah sinyal inputan dari sisi frekuensi dan amplitude.
TMS320C6713 adalah sebuah perangkat keras yang terdiri dari system pengacak dan penerjemah sinyal suara yang akan dikirimkan lewat jaringan. Selanjutnya dari pemanfaatan perangkat keras TMS320C6713 barulah algoritma kriptografi RC4 diterapkan sehingga menjadi salah satu sistem keamanan jaringan dengan mengacak sinyal inputan sebelum dikirim supaya jika terjadi proses penyadapan dengan cara tersebut, maka yang diperoleh penyadap hanyalah sebuah sinyal yang teracak-acak.

2.2. Tinjauan Pustaka

A. Kriptografi

Kriptografi berasal berasal dari bahasa Yunani yaitu crypto berarti rahasia(secret) dan graphia berarti tulisan (writing). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika dikirim.

Sejak 4000 tahun lalu kriptografi telah dikenal oleh orang-orang Mesir lewat hieroglyph walaupun bukan dalam bentuk tulisan standard. Pada zaman Rumawi Kuno, Julius Caesar mengirimkan pesan rahasia kepada panglima perang di medan perang dengan mengganti semua susunan alfabet dari: a b c d e f g h i j k l m n o p q r s t u v w x y z, menjadi: d e f g h i j k l m n o p q r s t u v w x y z a b c.

Perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi/data secara jarak jauh. Antar kota antar wilayah antar negara bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Begitu banyak pengguna seperti departemen pertahanan, suatu perusahaan atau bahkan individu-individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau kompetitornya atau Negara lain. Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi.

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

Manfaat dari kriptografi adalah :

a. Privacy (Kerahasiaan) yang mencegah pembacaan pesan-pesan oleh orang lain yang tidak berhak atau yang tidak berkepentingan.
b. Authenticity (Keaslian) yang membuat penerima pesan bisa mengetahui secara pasti, siapa yang mengirim pesan tersebut dan sebaliknya pengirim juga dapat mengecek kembali bahwa penerima pesan adalah orang yang benar-benar ia maksud.
c. Integrity (Keutuhan) yang meyakinkan bahwa pesan yang dikirim tidak dipalsukan atau dirubah oleh orang lain yang tidak berhak selama pengiriman pesan tersebut.
d. Non-Repudiation (Tidak adanya penolakan) mencegah penerima atau pengirim pesan mengingkari bahwa mereka pernah menerima atau mengirim pesan tersebut.

Pada penerapan teknologi yang sebenarnya, bidang-bidang utama yang digunakan untuk mencapai tujuan-tujuan tadi adalah sistem keamanan komunikasi dan keamanan komputer. Keamanan komunikasi merupakan perlindungan terhadap informasi pada saat pengiriman pesan dari sebuah sistem ke sistem lainnya. Keamanan komputer adalah perlindungan terhadap sistem informasi komputer itu sendiri, seperti pada perangkat lunak, sistem operasi komputer dan keamanan terhadap perangkat lunak manajemen basis data komputer.

B. Algoritma

Pada Kriptografi modern terdapat berbagai macam algoritma, secara umum algoritma kriptografi dibagi menjadi 3 macam yaitu :

1. Algoritma Simetris

   Algoritma Simetris adalah algoritma yang menggunakan kunci yang sama untuk melakukan enkripsi dan dekripsi. Aplikasi dari algoritma simetris digunakan oleh beberapa algoritma :

   a. Advance Encryption Standart (AES)

      AES dipublikasikan oleh NIST (National Institute of Standard and Technology) pada tahun 2001 yang digunakan untuk menggantikan algoritma DES yang semakin lama semakin mudah untuk membobol kuncinya. AES diperoleh dari hasil kompetisi yang diadakan NIST pada tahun 1997. Pada tahap pertama, 15 peserta dari 21 peserta lolos ke tahap berikutnya berdasarkan penilaian tingkat keamanan, harga, algoritma, dan karakteristik implementasi. Sepuluh dari 15 peserta tersebut gugur pada tahap berikutnya karena dianggap kurang aman dan kurang efektif.

   b. Algoritma Serpent

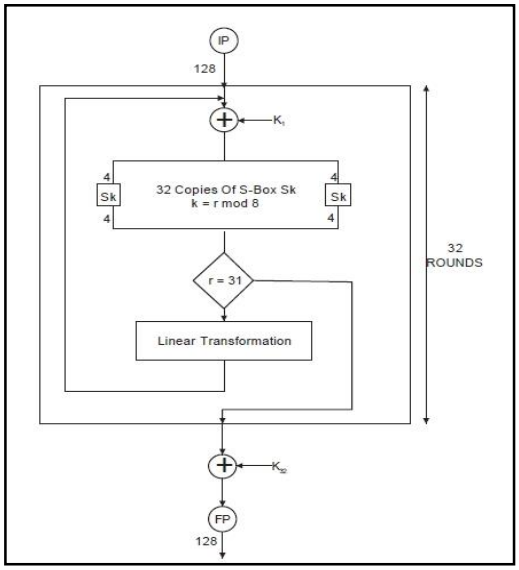
      Algoritma cipher block Serpent adalah algoritma dengan 32 putaran jaringan SP yang beroperasi pada empat word 32 bit, yang berarti ukuran bloknya adalah 128 bit. Untuk komputasi internal, semua nilai direpresentasikan dalam little-endian , di mana word pertama adalah least-significant word, dan word terakhir adalah most-significant word.

      Algoritma Serpent mengenkripsi plainteks *P* 128 bit menjadi cipherteks C 128 bit dalam 32 putaran dengan kontrol dari 33 sub-kunci 128 bit K0,...,K32. Panjang kunci masukan user 128, 192, dan 256 bit. Kunci yang lebih pendek dari 256 bit dipetakan menjadi kunci sepanjang 256 bit dengan menambahkan satu “1” bit pada akhir MSB, dan diikuti dengan “0” bit sampai mencapai 256 bit.

      Algoritma Serpent ini terdiri dari:

      1. Initial Permutation (IP)
      2. Terdiri dari 32 putaran, masing-masing terdiri dari sebuah operasi pengacakan kunci, operasi menggunakan S-Box, dan transformasi linear. Pada putaran terakhir, transformasi ini digantikan dengan penambahan operasi pengacakan kunci.
      3. Final Permutition (FP)

   Adapun untuk lebih jelasnya, struktur algoritma serpent digambarkan seperti berikut :



Gambar 2.1 Alur Algoritma enkripsi serpent

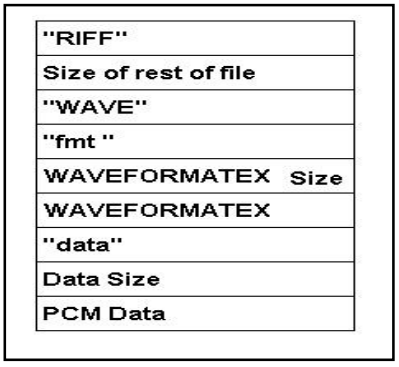
C. Aplikasi Messenger

Aplikasi Mensenger ini adalah sebuah aplikasi yang digunakan untuk berkomunikasi dengan pengguna aplikasi mesengger lain dalam jarak yang tak ditentukan karena komunikasi ini dilakukan via Internet. Aplikasi Messenger biasanya disediakan oleh penyedia layanan perpesanan seperti Yahoo! Messenger, Gmail (GTalk), Skype dsb. Aplikasi tersebut menyediakan layanan panggilan suara dimana pengguna bisa melakukan percakapan secara realtime layaknya kita berbicara di telepon. Biasanya pengguna menambahkan sebuah kontak yang berupa alamat Email dari pengguna lain yang dia kenal.

D. File WAV

WAV atau Waveform. File Audio WAV mirip dengan PCM, namun bisa terkompresi maupun tidak terkompresi. File Wav juga mirip dengan file AIFF yaitu file Audio yang digunakan komputer Mac. Format WAV banyak digunakan oleh handphone, sehingga popularitas bisa menyamai file MP3.

Struktur file WAV adalah sebagai berikut :



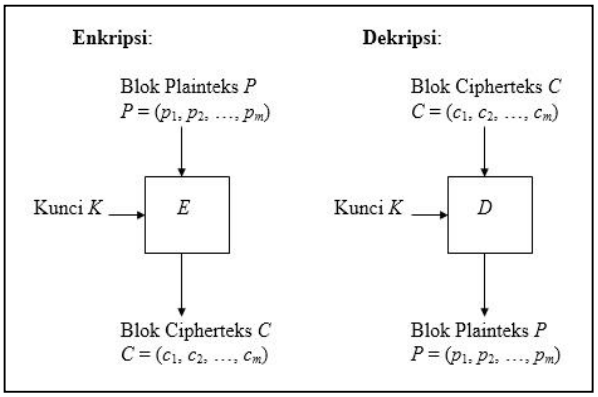
Gambar 2.2 : Layout File WAV

a. “RIFF” Merupakan sebuah header awal file wav. tiap karakternya mempunyai penjang 1 byte.
b. Size of rest of file (integer) merupakan ukuran untuk semua file dalam wav per 8 byte, di tiap bitnya adalah 32 – bit integer. Ukuran ini akan dibuat setelah file tercipta.
c. “WAVE” Type file header.
d. “fmt ” Penanda Chunk format. Termasuk chunk yang berisi nilai null
e. WAVEFORMATEX Size Untuk menandakan panjang data yang terdaftar dan format type
f. WAVEFORMATEX Berisi sampel rate – 32 bit integer. Berisi nilai 44100(CD) dan memuat bit sampel rate
g. “data” Header chunk “dsata”.penanda awal data segmen
h. PCM Data Ukuran dari segmen data

E. Cipher Block

Salah satu kriptografi simetrik adalah Block Cipher. Block Cipher melakukan enkripsi dan dekripsi terhadap sebuah data yang masuk, membaginya dalam blok – blok data terlebih dahulu, lalu proses enkripsi dilakukan secara terpisah terhadap masing – masing blok data. Dalam matematis, Block Cipher merupakan pemetaan blok – blok plaintext ke blok – blok ciphertext . Ambil bahwa dalam suatu teks sandi sepanjang n-bit, terlebih dahulu kita bagi dalam beberapa blok – blok dengan ukuran panjang yang sama. Dengan kunci yang sama dan dengan algoritma tertentu, blok – blok ini dienkripsi, dan hasil outputnya pun berupa blok – blok sandi yang terenkripsi dan berukuran sama.

Block cipher memiliki beberapa keuntungan, yaitu mudahnya implementasi algoritma Block Cipher ke dalam software – software. Error Propagation yang terjadi pun tidak merambat ke ciphertext lainnya karena enkripsi masing – masing bloknya independen. Namun, Block Cipher sangat mudah dianalisis karena blok – blok yang dienkripsi saling independen dan kuncinya sama, maka hal ini memudahkan kriptanalis untuk mengetahui kunci yang digunakan.

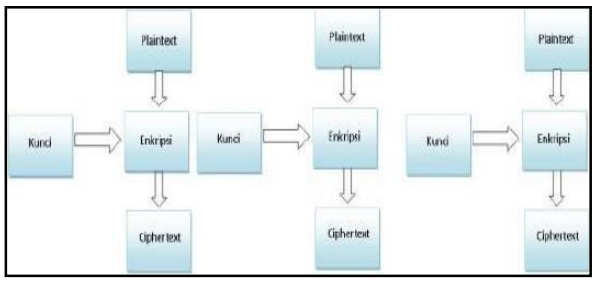


Gambar 2.3 Enkripsi dan Dekripsi dengan Chiper Block

Ada beberapa method dalam pengenkripsian, yaitu metode Electronic Code Book, Cipher Block Chaining, Cipher Feedback, Outer Feedback, dan Counter.

1. Electronic Code Book

Pada mode ini, setiap blok plainteks dienkripsi secara individual dan independen. Secara matematis, enkripsi dengan mode ECB dinyatakan sebagai $Ci = Ek(Pi)$ dan dekripsi sebagai $Pi = Dk(Ci)$ yang dalam hal ini, Pi dan Ci masing-masing blok plainteks dan cipherteks ke-i.



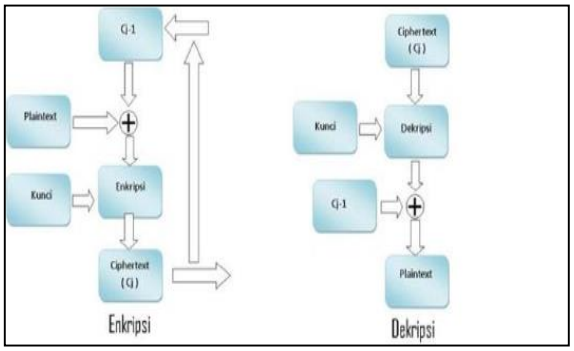
Gambar 2.4 Skema Buku Kode Elektronik

2. Chiper Block Chaining

Mode ini menerapkan mekanisme umpan-balik (*feedback*) pada sebuah blok, yang dalam hal ini hasil enkripsi blok sebelumnya di-umpan-balikkan ke dalam enkripsi blok yang *current*. Caranya, blok plainteks yang *current* di-XOR-kan terlebih dahulu dengan blok cipherteks hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi.

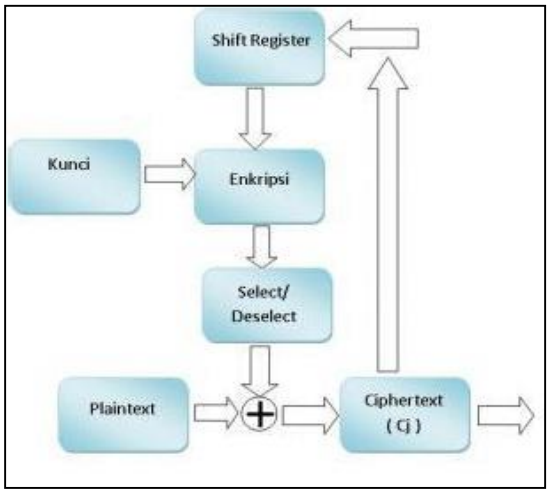
Dengan mode *CBC*, setiap blok cipherteks bergantung tidak hanya pada blok plainteksnya tetapi juga pada seluruh blok plainteks sebelumnya. Dekripsi dilakukan dengan memasukkan blok cipherteks yang *current* ke fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok cipherteks sebelumnya. Dalam hal ini, blok cipherteks sebelumnya berfungsi sebagai umpan-maju (*feedforward*) pada akhir proses dekripsi.

Secara matematis, enkripsi dengan mode *CBC* dinyatakan sebagai $Ci = Ek(Pi \oplus Ci - 1)$ dan dekripsi sebagai $Pi = Dk(Ci) \oplus Ci - 1$



Gambar 2.5 Skema Chiper Block Chaining

3. Chiper Feedback



Gambar 2.6 Skema Feedback Chiper

Metode Cipher Feedback menggunakan sistem Shift Register, dimana yang diproses terlebih dahulu adalah Initialization Vector dalam algoritma Enkripsi dengan Kunci. Setelah diproses, bit yang dihasilkan akan melalui proses seleksi bit, biasanya bit – bit yang paling kiri, untuk selanjutnya dienkripsi dengan Plaintext untuk menghasilkan Ciphertext. Bit hasil seleksi yang digunakan tergantung besarnya bit blok plaintext yang diinput. Selanjutnya, setelah mendapatkan blok ciphertext, selain di output, blok ciphertext tersebut dimasukkan ke IV yang sebelumnya, dan IV digeser sebanyak bit blok ciphertext sebelumnya, yang selanjutnya IV yang telah digeser bersama blok ciphertext yang digabung bersama IV tersebut diproses kembali oleh algoritma Enkripsi tersebut.

4. Output Feedback

Perbedaan mendasar OFB, yang membedakannya dengan CFB adalah input yang digunakan dalam proses enkripsi. Kalau dalam CFB, input yang digunakan adalah ciphertext yang selanjutnya dishift bersama IV, dalam OFB yang digunakan adalah output bit hasil dari proses seleksi yang kemudian dishift bersama IV yang sebelumnya. Hasil Seleksi tetap diguanakan dalam proses enkripsi Plaintext untuk mendapatkan Ciphertext.

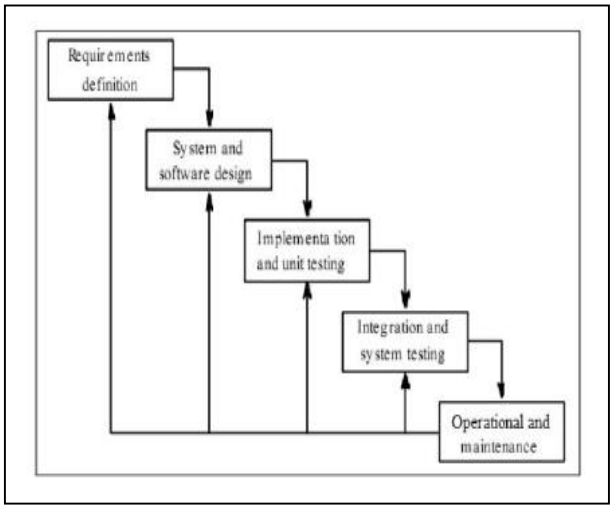
III. METODOLOGI PENELITIAN

3.1 Pengumpulan Data

Survei dilakukan untuk memperoleh data yang akurat berdasarkan pemakai terbanyak. Dan mereka memiliki keluhan-keluhan ketika menggunakan layanan komunikasi suara. Banyak penyalah-gunaan terhadap celah keamanan yang ada pada komunikasi suara sehingga memicu terjadinya penyadapan oleh para peretas. Saat ini, sudah banyak sekali layanan email yang menyediakan fasilitas komunikasi suara. Pengguna yang dulu hanya bisa menggunakan layanan email untuk mengirim dan menerima pesan saja, sekarang pengguna sudah bisa melakukan panggilan suara kepada pengguna-pengguna lain.

3.2 Metode

Metode yang digunakan dalam penelitian ini adalah Metode Waterfall. Model ini merupakan model yang umum digunakan oleh para peneliti.



Gambar 3.1 : Metode Waterfall.

3.3 Pengujian Metode

a. Memastikan fungsionalitas perangkat lunak dapat berjalan dengan baik sesuai dengan spesifikasi perangkat lunak yang telah ditentukan.
b. Memastikan funsionalitas user interface agar berfungsi dengan baik pada waktu penggunaan aplikasi.

Pengujian ini meliputi 2 hal antara lain sebagai berikut :

1. Blackbox Testing

Black-Box Testing merupakan pengujian yang berfokus pada spesifikasi fungsional (coding) dari perangkat lunak, tester dapat mendefinisikan kumpulan kondisi input dan melakukan pengetesan pada spesifikasi fungsional program untuk memastikan bahwa fungsi-fungsi pada perangkat lunak telah berjalan dengan benar.

2. Whitebox Testing

Pengujian perangkat lunak perlu dilakukan untuk mengevaluasi baik secara manual maupun otomatis untuk menguji apakah perangkat lunak sudah memenuhi persyaratan atau belum, dan untuk menentukan perbedaan antara hasil yang diharapkan dengan hasil sebenarnya.

IV. HASIL PENELITIAN DAN PEMBAHASAN

4.1 Kebutuhaan

Pada penelitian ini, akan dijelaskan mengenai langkah-langkah implementasi dan analisis hasil penelitian *Enkripsi dan Dekripsi Pesan Suara dengan Metode Serpent menggunakan Visual Basic 6.0*.

Kebutuhan Hardware :

a. Ram 2GB
b. Harddisk 500GB
c. Processor Dual Core 1,2 GHz
d. Microphone
e. Speaker/Headphone
f. Internet Connection

Kebutuhan Software :

a. OS Windows 7
b. Software Microsoft Visual Basic 6.0
c. HexEditor

4.2 Prosedur persiapan pembuatan aplikasi

a. Mengumpulkan materi –materi yang dibutuhkan
   1. Data awal yang dibutuhkan untuk penelitian yang dilakukan adalah berupa kode Hexa hasil dari pembacaan melalui aplikasi HexEditor atau yang di buat sendiri dengan bahasa pemrograman Visual Basic 6.0.
   2. Referensi tentang perhitungan algoritma serpent
   3. Menentukan library – library yang akan di gunakan di bahasa pemrograman visual basic 6.0

b. Melakukan pembatasan terhadap materi tersebut
c. Mempersiapkan dan melakukan instalasi perangkat keras
d. Memperisapkan dan melakukan instalasi perangkat lunak sesuai dengan spesifikasi kebutuhan

4.3 Unit bahasa dan pemodelan

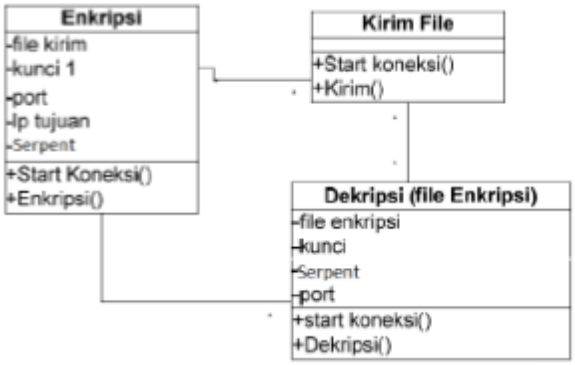
a. Use Case Diagram

Gambar 4.3.1 UCase Diagram

b. Skenario

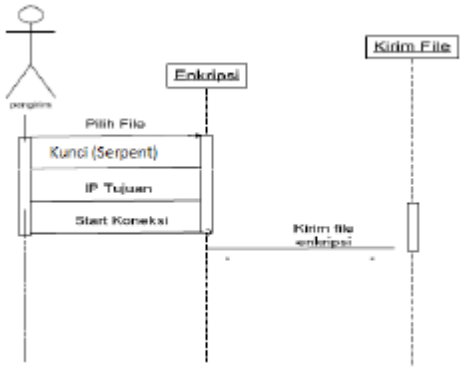
Gambar 4.3.2 Skenario Global

c. Class Diagram

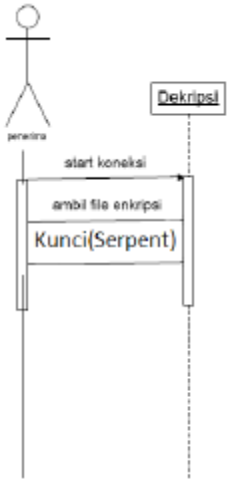


Gambar 4.3.3 Class Diagram

d. Sequence Diagram

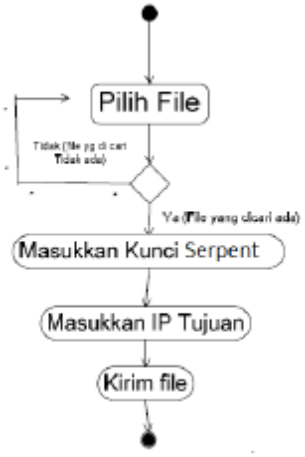


Gambar 4.4.4 Sequence Diagram

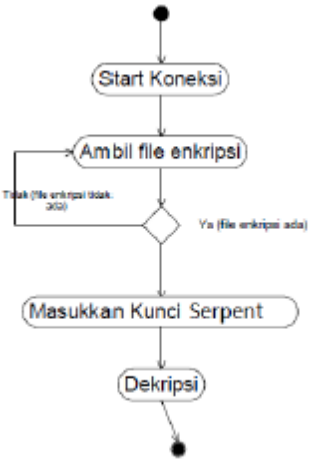


Gambar 4.3.5 Sequence Diagram Detail

e. Activity Diagram



Gambar 4.3.6 Activity Diagram



Gambar 4.4.7 Activity diagram dekripsi

4.4 Analisa Algoritma Serpent

Algoritma Serpent adalah algoritma dengan 32 putaran jaringan SP yang beroperasi pada empat word 32 bit, yang berarti ukuran bloknya adalah 128 bir. Semua nilai yang digunakan direpresentasikan sebagai bitstream. Untuk komputasi internal, semua nilai direpresentasikan dalam little-endian, di mana word pertama adalah least-significant word, dan word terakhir adalah most-significant word. Secara eksternal, setiap blok dituliskan sebagai plain hexadesimal 128 bit . Serpent mengenkripsi plainteks P 128 bit menjadi cipherteks C 128 bit dalam 32 putaran dengan kontrol dari 33 sub-kunci 128 bit K0,...,K32. Panjang kunci masukan user fleksibel, namun untuk memenuhi persyaratan AES, maka ditetapkan 128, 192,dan 256 bit. Kunci yang lebih pendek dari 256 bit dipetakan menjadi kunci sepanjang 256 bit dengan menambahkan satu “1” bit pada akhir MSB, dan diikuti dengan “0” bit sampai mencapai 256 bit.

S-Box Serpent adalah permutasi 4 bit dengan ketentuan sebagai berikut:

1. Masing-masing karakteristik diferensial memiliki probabilitas maksimal ¼, dan sebuah input dengan perbedaan satu bit tidak akan meghasilkan output dengan perbedaan satu bit
2. Masing-masing karakteristik linear memiliki probabilitas antara ½ ± ¼, dan hubungan linear antara sebuah bit pada input dan sebuah bit pada output memiliki probabilitas ½ ±1/8
3. Urutan non-linear bit output sebagai fungsi dari bit input maksimal 3 Pembangkitan S-Box terinspirasi dari EC4, yaitu menggunakan matriks dengan 32 array yang masing-masing memiliki 16 entri.

Matriks diinisialisasi dengan 32 baris S-Box DES dan ditransformasikan dengan menukar entri pada array ke-r bergantung pada nilai entri ke-(r+1) array dan pada inisial string yang merepresentasikan kunci. Jika array hasilnya memenuhi ketentuan yang telah disebutkan sebelumnya, maka simpan array sebagai Serpent S-Box. Ulangi prosedur tadi sampai 8 S-Box berhasil dibangkitkan.

4.5.Desain Input Output

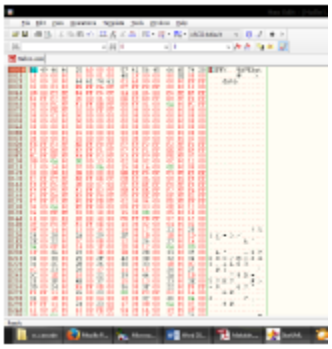
Gambar 4.5.1 Menu Utama

4.6 Implementasi

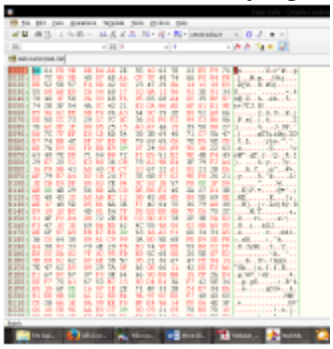
Pada tugas akhir ini, perangkat lunak yang dikembangkan untuk melakukan pengiriman pesan suara memiliki batasan sebagai berikut:

1. Perangkat lunak hanya melibatkan paling sedikit dua komputer.
2. Proses digitalisasi dan kompresi sinyal suara yang dilakukan tidak diimplementasikan dengan source code yang dibuat sendiri, tetapi dengan memanfaatkan library yang ada pada software developer microsoft visual basic 6.0.
3. Untuk format audio yang di masukan adalah sebagai berikut :
   a. Sample rate 8000Hz.
   b. Ukuran sample 16 bit.
   c. Channel yang digunakan adalah mono bukan stereo.
4. Jenis masukan file berasal dari dua sumber yaitu :
   a. Pesan suara yang direkam langsung yang kemudian dienkripsi
   b. File audio yang di eknripsi lalu di kirim ke pengguna lain

4.7 Analisa Percobaan



Gambar 4.7.1 Kode Hex File yang belum di enkripsi



Gambar 4.7.2 Kode Hex File yang telah dienkripsi

4.8 Pengujian program

a. Blackbox testing

Kelebihan dan kelemahan Blackbox Testing

1. Dapat memilih subset test secara efektif dan efisien

2. Dapat menemukan cacat

3. Memaksimalkan testing investmen

4. Tidak pernah yakin apakah perangkat lunak tersebut benar-benar lulus uji

b. Whitebox testing

Kelebihan whitebox testing

1. Kesalahan logika. Digunakan pada sintaks ‘if’ dan pengulangan. Dimana White Box Testing akan mendeteksi kondisi-kondisi yang tidak sesuai dan mendeteksi kapan proses pengulangan akan berhenti.
2. Ketidaksesuaian asumsi. Menampilkan asumsi yang tidak sesuai dengan kenyataan, untuk di analisa dan diperbaiki.
3. Kesalahan ketik. Mendeteksi bahasa pemrograman yang bersifat case sensitive.
4. Untuk perangkat lunak yang tergolong besar, White Box Testing dianggap sebagai strategi yang tergolong boros, karena akan melibatkan sumber daya yang besar untuk melakukannya.

REFERENSI

[1] Schneier, Bruce. 1996. Applied Cryptography 2nd. John Wiley & Sons.

[2] Tanenbaum, Andrew S. 2001. *Modern Operating Systems 2nd*. Prentice Hall.

[3] Bora, Piotr, Tomasz Czakka. Implementation of Serpent Algorithm Using Altera
FPGA Devices. Military Communication Institute.

[4] Agus dan A. Asmara, *Meraih Untung Memelihara Ikan Koi*. Bandung: Titian Ilmu, 2007.

[5] Anonym. (2014, Maret) content-based image retrieval. [Online]. http://en.wikipedia.org/wiki/Content-based_image_retrieval. [Diakses 24 Maret 2014].

[6] P. I. Hastuti, M. Hariadi dan I K. Eddy, "Content Based Image Retrieval Berdasarkan Fitur Bentuk Menggunakan Metode Gradient Vector Flow Snake," in *Seminar Nasional Informatika* , Yogyakarta, 2009.

[7] Freez-kun. (2012, April) Teknologi yang Digunakan Sehari-hari: Desain Database. [Online]. http://adnanfritzdomaulana.blogspot.com/2012/04/desain-database.html. [25 Maret 2014].

[8] H. F. Atlam, G. Attiya dan N. El-Fishawy, "Comparative Study on CBIR based on Color Feature," *International Journal of Computer Applications*, vol. 78, no. 16, pp. 0975-8887, September 2013.

[9]Tyo. (2012, Maret) Sistem Pengenalan Wajah Menggunakan Webcam Untuk Absensi dengan Metode Template Matching. [Online]. http://07351486-indra.blogspot.com/2012/03/sistem-pengenalan-wajah-menggunakan.html.

[10] L. Makarti, A. Basuki dan T. Karlita, "Aplikasi Identifikasi Flora Indonesia pada Platform Android," *Jurnal Informatika dan Komputer PENS*, vol. 2, no. 2, 2013.
[11] R. Kaur, dan S. Jindal, "Digital Image Watermaking Technique using High Frequency Band based on Discrete Wavelet Transform and Singular Value Decomposition," *International Journal of Computer Applications*, vol. 89, no. 19, pp. 0975-8887, Maret 2014.