**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNOLOGI INFORMASI**

**INSTITUT TEKNOLOGI SEPULUH NOPEMBER**

**USULAN TUGAS AKHIR**

# **IDENTITAS PENGUSUL**

Nama : **Bayu Bagus Satryo**

NRP : **5108 100 035**

Dosen Wali : **Dr. Agus Zainal Arifin, S.Kom, M.Kom**

1. **JUDUL TUGAS AKHIR**

***“Keamanan Pesan pada Audio dengan Metode Enhancement Least Significant Bit (LSB), Vigenere dan Tiny Encryption Algorithm (TEA)”***

1. **LATAR BELAKANG**

Perkembangan teknologi yang semakin pesat menjadikan manusia semakin bergantung dengan adanya teknologi. Salah satu hasil perkembangan teknologi yang berpengaruh cukup besar terhadap kegiatan sehari-hari manusia adalah pengiriman pesan, baik berupa data, gambar, audio ataupun video. Bagi sebagian orang pengiriman data ini menjadi penting, sehingga membutuhkan keamanan dan kerahasiaan dalam proses pengirimannya.

Diperlukan metode khusus untuk menjaga keterjaminan kerahasiaan data. Dimana metode ini hanya mampu dipahami dengan baik oleh si pengirim pesan dan pihak yg menerima pesan. Metode yang umum digunakan dalam menjaga kerahasiaan data ini adalah metode kriptografi. Kriptografi sendiri adalah ilmu yang berguna untuk mengacak data sedemikian rupa sehingga tidak bisa dibaca oleh pihak ketiga. Tetapi pengacakan data dengan cara steganografi saat ini cenderung mudah dikenali dikarenakan data yang diacak gampang dicurigai serta kemampuan kriptanalisis (pemecah kriptografi) yang semakin canggih.

Kemudian, dipakailah metode steganografi untuk menyembunyikan data. Steganografi sendiri memiliki pengertian sebuah seni dan ilmu untuk menulis pesan tersembunyi atau menyembunyikan suatu pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak seorangpun yang menyadari. Adapun nantinya yang akan digunakan adalah audio untuk mendukung steganografi.

Untuk kriptografi disini akan menggunakan 2 metode yaitu metode Vigenere dan Tiny Encrytion Algorithm. Yang mana metode vigenere ini adalah proses menyandikan teks alphabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. Sandi vigenere sendiri merupakan bentuk sederhana dari sandi subtitusi polialfabetik.

Sementara 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.

Enhanced Least Significant Bit merupakan salah satu metode steganografi yang merupakan pengembangan dari metode sebelumnya. Metode paling dasar dalam ilmu kriptografi.

1. **RUMUSAN MASALAH**

Berdasarkan latar belakang yang telah diuraikan diatas, terdapat permasalahan yang dapat dirumuskan, yaitu:

1. Bagaimana membuat kriptografi dengan metode Vigenere dan Tiny Encryption Algorithm.
2. Bagaimana menyisipkan data hasil kriptografi ke dalam file audio dengan Enhanced Least Significant Bit.
3. Bagaimana mendekripsi file audio untuk dapat membaca isi pesan di dalamnya.
4. **BATASAN MASALAH**

Permasalahan yang dibahas dalam Tugas Akhir ini memiliki beberapa batasan yakni,

1. Metode Kriptografi yang digunakan adalah Vigenere dan Tiny Encryption Algorithm.
2. Metode steganografi yang digunakan adalah Enhanced Least Significant Bit.
3. File yang dienkripsi adalah file txt.
4. File untuk steganografi adalah file wav.
5. Menggunakan bahasa pemrograman Java.
6. **TUJUAN TUGAS AKHIR**

Tujuan Tugas Akhir ini yaitu mengembangkan aplikasi yang dapat,

1. Mampu menggabungkan dua model kriptografi yang berbeda.
2. Mampu menyimpan data yang bersifat rahasia ke dalam file audio.
3. **MANFAAT TUGAS AKHIR**

Manfaat yang diharapkan dengan mengimplementasikan pengamanan data dengan kriptografi dan steganografi ini adalah terciptanya jaminan keamanan bagi pengiriman pesan melalui media audio yang telah disisipi pesan sehingga tidak mudah terbaca oleh pihak lain dan tidak mudah dilacak isi pesannya.

1. **RINGKASAN TUGAS AKHIR**

Pada tugas akhir ini penulis mengusulkan sebuah aplikasi yang melakukan enkripsi pada file plainteks (.txt) dengan menggunakan metode Vigenere. Setelah dilakukan enkripsi dengan metode Vigenere kemudian dilakukan enkripsi dengan metode Tiny Encryption Algorithm, pesan tersebut lalu di sembunyikan di file audio (steganografi). Setelah dilakukan enkripsi (kriptografi) dan penyembunyian pesan (steganografi) maka pesan yang telah di steganografi tersebut harus dapat di ekstraksi, setelah dilakukan ekstraksi maka selanjutnya akan dilakukan dekripsi dari pesan tersebut sehingga dapat didapatkan kembali pesan aslinya.

Vigènere cipher sangat dikenal karena mudah dipahami dan diimplementasikan. Cipher menggunakan bujursangakar Vigènere untuk melakukan enkripsi seperti ditunjukkan pada (gambar 2.1). Kolom paling kiri dari bujursangkar menyatakan huruf-hurf kunci, sedangkan baris paling atas menyatakan huruf-huruf plainteks. Setiap baris dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar cipher, yang mana jumlah pergesaran huruf plainteks ditentukan nilai numerik huruf kunci tersebut ( yaitu, A = 0, B = 1, C = 2,…, Z = 25).

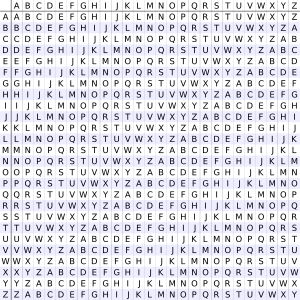


Table Vigenere Square

Untuk contoh tersebut maka untuk pendekripsiannya adalah sebagai berikut. Key nya akan berpindah posisi menjadi kolom plaintext. Contoh :

Plainteks : THIS PLAINTEXT

Kunci : SONY SONYSONYS

Cipherteks : LVVQ HZNGFHRVL

Dari hasil enkripsi diatas tersebut, maka proses dekripsinya untuk mencari plaintextnya adalah :

Kunci : SONY SONYSONYS

Cipherteks : LVVQ HZNGFHRVL

Untuk karakter yang pertama, huruf S maka akan dicari seluruh isi karakter yang berada pada kolom huruf S ke bawah, dimana terdapat karakter ciphertext huruf L, maka dilihat pada pada kolom kunci yang menunjukkan bahwa huruf L tersebut berada pada baris huruf T. Begitu juga dengan karakter yang ke dua huruf O, maka akan dicari seluruh isi karakter yanga berada pada kolom huruf O ke bawah, dimana terdapat karakter ciphertext huruf V, maka dilihat pada kolom kunci yang menunjukkan bahwa huruf V tersebut berada pada baris huruf H, dan seterusnya. Demikianlah cara kerja proses dekripsinya untuk mencari plainteks.

TEA merupakan algortima enkripsi blok, dengan blok-blok sebagai berikut:

* 64-bit input L0 dan R0 @32-bit.
* 128-bit kunci k[0], k[1], k[2], k[3] @32-bit.

Dan menggunakan Delta (golden number) = (√5 -1)231 = $9e3779b9 H dengan Round sebanyak 32 kali.

**Rumus Enkripsi**:

SUM = n \* Delta

Ln = L(n-1)+((R(n-1) Shl 4)+K[0]) XOR (R(n-1)+SUM) XOR ((R(n-1) Shr 5)+K[1]))

Rn = R(n-1) + ((Ln Shl 4)+K[2]) XOR (Ln+SUM) XOR ((Ln Shr 5)+K[3])

**Rumus Dekripsi**:

Rn = R(n-1) – ((L(n-1) Shl 4)+k[2]) XOR (L(n-1)+SUM) XOR ((L(n-1) Shr 5)+k[3])

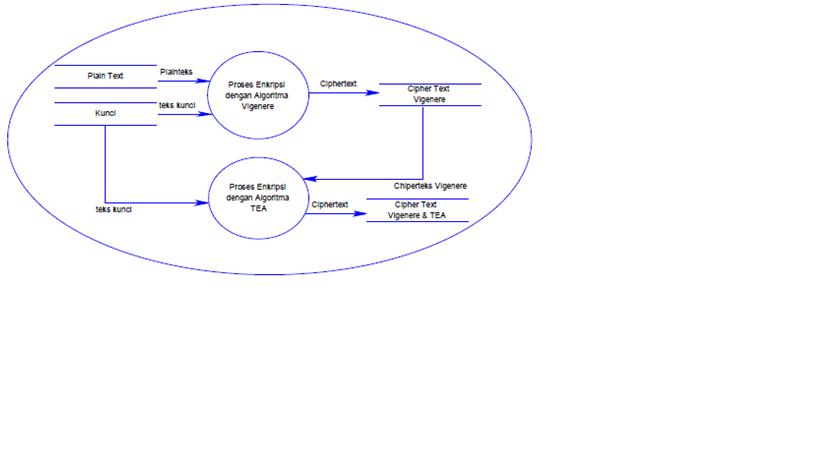
Ln = L(n-1) – ((Rn Shl 4)+k[0]) XOR (Rn+SUM) XOR ((Rn Shr 5)+k[1]) )

SUM = SUM - Delta (SUM = Delta X 32 )

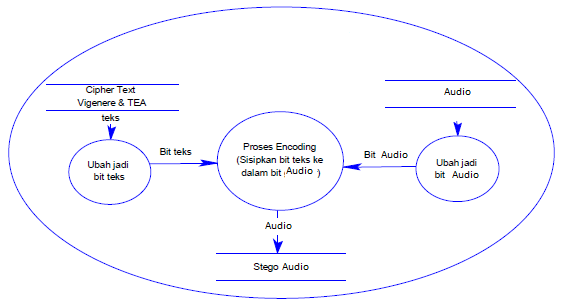
Di mana : Delta = (√5 -1)231 = (2654435770)D = (9e3779b9)H

n = Round ke

Proses kerja kriptografi dapat dilihat pada gambar berikut



Sedangkan proses steganografi pada gambar di bawah



Proses steganografi akan menggunakan metode Enhanced Least Significant Bit (LSB) yang mana pada metode ini digunakan *randomize bit number* untuk menyusupkan pesan pada audio. Metode ini akan melihat MSB (Most Significant Bit) sebelum menyusupkan bit. Dimana apabila 2 MSB pertama bernilai 00 maka yang berubah adalah LSB ke 3. Jika 2 MSB pertama bernilai 01 maka yang berubah adalah LSB ke 2 dan bila 2 MSB pertama bernilai 10 atau 11 maka yang berubah adalah LSB ke 2

Media yang akan digunakan sebagai media penyembunyian pesan adalah file audio. File audio digunakan karena memiliki ukuran yang besar sehingga pengirim pesan dapat menyisipkan pesan yang lebih besar pula di dalam media steganografi. File audio dipilih juga dikarenakan metode penyisipannya yang lebih modern daripada menyisipkan sebuah pesan ke file gambar/image.

1. **METODOLOGI**
2. **Analisis Kebutuhan dan Studi Literatur**

Pada tahap ini dilakukan pengumpulan dan penggalian informasi dan literatur yang diperlukan dalam tahap perancangan sistem. Literatur yang dicari meliputi artikel kriptografi dengan metode Vigenere dan Tiny Encryption Algorithm*,* menyisipkan data hasil kiptografi ke dalam file audio dan cara memecah file audio. Literatur yang dipelajari dan digunakan meliputi buku referensi dan dokumentasi internet

1. **Perancangan Perangkat Lunak**

Pada tahap ini dilakukan analisa awal dan pendefinisian kebutuhan sistem untuk mengetahui masalah yang sedang dihadapi. Pada tahapan ini dilakukan perancangan tentang tampilan GUI dari program. Dan juga dirancang tentang OOP dari implementasi metode Vigenere dan Tiny Encryption Algorithm.

1. **Implementasi**

Pada tahap pengimplementasian ini aplikasi sudah mulai dibuat secara menyeluruh berdasar pada desain sistem dan tampilan perangkat lunak. Bahasa pemrograman yang digunakan untuk membangun aplikasi ini adalah JAVA untuk pengolahan antarmuka pengguna.

1. **Uji Coba dan Evaluasi**

Pada tahap ini implementasi yang sudah selesai dikerjakan, akan diuji dengan cara melakukan berbagai skenario. Pengujian ini kemungkinan juga akan melibatkan orang lain untuk membantu penilaian terhadap keakuratan perangkat lunak dalam menjawab kebutuhan yang tercantum pada rumusan masalah. Pada tahap ini juga akan dilakukan perbaikan apabila aplikasi dinilai kurang sesuai dengan tujuan awal pembuatan program.

1. **Penyusunan Buku Tugas Akhir**

Pada tahap ini melakukan pendokumentasian dan laporan dari seluruh konsep, dasar teori, implementasi, proses yang telah dilakukan, dan hasil-hasil yang telah didapatkan selama pengerjaan tugas akhir. Buku tugas akhir ini bertujuan untuk mendapatkan gambaran dari pengerjaan tugas akhir ini dan diharapkan dapat berguna untuk pembaca yang tertarik untuk melakukan pengembangan lebih lanjut.

Secara garis besar, buku tugas akhir nantinya terdiri atas beberapa bagian yaitu :

1. Pendahuluan
   1. Latar Belakang
   2. Permasalahan
   3. Batasan Tugas Akhir
   4. Tujuan
   5. Metodologi
   6. Sistematika Penulisan
2. Tinjauan Pustaka
3. Desain dan Implementasi
4. Uji Coba dan Evaluasi
5. Kesimpulan dan Saran
6. Daftar Pustaka
7. **JADWAL PEMBUATAN TUGAS AKHIR**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Tahapan | Bulan (Tahun 2012) | | | | | | | | | | | | | | | | | | | | |
| Februari | | | | Maret | | | | April | | | | | Mei | | | | Juni | | | |
| Analisa kebutuhan dan studi literatur |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Perancangan sistem |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Implementasi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Uji coba dan evaluasi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Penyusunan buku |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. **DAFTAR PUSTAKA**

[1] Administrator (2006). Dasar Kriptografi, (online),

(http://ilmukomputer.org/2006/08/25/dasar-kriptografi/, diakses tanggal 27 Februari 2012)

[2] Antoni Andre (2012). Apa itu Steganografi, (online),

(http://elmoony.wordpress.com/2012/01/08/apa-itu-steganografi/, diakses tanggal 27 Februari 2012)

[3] Wulandari, Ratna, (2010). Pembuatan Aplikasi Steganografi pada File Audio Mp3 dengan Metode Parity Coding dan Enkripsi Rijndael.(Online),

(http://digilib.its.ac.id/ITS-Undergraduate-3100010040361/14550, diakses pada tanggal 27 februari 2012)

[4] Girsang, Truman Tuah. (2010). Analisis Kerahasiaan Data Menggunakan Algoritma Vigenere Cipher Dalam Sistem Pengamanan Data. (online), (http://repository.usu.ac.id/handle/123456789/20100, diakses tanggal 27 Februari 2012)

1. Hidayat Akik. 2008. *Kriptografi dan Stenografi Menggunakan Algoritma Vigenere dan Tea (Tiny Encryption Algorithm)*.
2. Asad, Muhammad. Gilani Junaid. Khalid, Adnan. 2011. *An Enhanced Least Significant Bit Modification Technique for Audio Steganography*.

**LEMBAR PENGESAHAN**

###### Surabaya, 29 Februari 2012

Menyetujui,

|  |  |
| --- | --- |
| Dosen Pembimbing I,  **Henning Titi Ciptaningtyas, S. Kom, M. Kom.**  NIP. 198407082010122004 | Dosen Pembimbing II,  **Hudan Studiawan, S. Kom, M. Kom.**  NIP. |