

BAB I

PENDAHULUAN

I.1. Latar Belakang

Penyandian data berupa multimedia salah satunya adalah gambar. Semakin rumit metode yang digunakan, maka tingkat keamanan yang dihasilkan pun akan semakin baik pula. Gambar digunakan dalam berbagai bidang seperti keamanan, medis, ilmu, teknik, seni, hiburan, iklan, pendidikan serta pelatihan. Dengan bertambahnya penggunaan teknik digital bagi transmisi dan penyimpanan gambar, masalah mendasar untuk melindungi kerahasiaan, keutuhan dan keaslian gambar memang perlu diperhatikan.

Enkripsi gambar menggunakan algoritma 3DES adalah cara untuk menyembunyikan informasi gambar asli dan dibuat gambar tersebut tidak tampak seperti gambar aslinya. Menentukan gambar apa yang akan disembunyikan informasinya beserta kunci. Kemudian langkah selanjutnya melakukan proses enkripsi, bagaimana cara memetakan tiap piksel dari gambar tersebut. DES ditetapkan sebagai standard untuk melindungi data dan informasi. Tetapi, DES dianggap sudah tidak aman lagi, karena dengan perangkat keras khususnya kuncinya dapat ditemukan dalam waktu beberapa hari. Kemudian IBM yang membuat algoritma DES mengembangkan DES menjadi 3DES.

3DES juga banyak digunakan dan penggunaannya lebih aman dibandingkan DES. Dalam paper ini dibahas tentang enkripsi dan dekripsi data dengan algoritma 3DES, dengan lama waktu yang diperlukan dan kecepatannya, serta

kekuatan 3DES terhadap serangan *brute force*. Hal ini dikarenakan kerahasiaan suatu informasi sangatlah penting dan bersifat pribadi.

Oleh karena itulah, penulis terdorong dan berinisiatif untuk mengambil judul “**Perancangan Aplikasi Enkripsi File Gambar Dengan Algoritma Triple Des**” dalam penyusunan skripsi ini.

I.2. Ruang lingkup Permasalahan

Adapun beberapa tahap yang dilakukan dalam membuat ruang lingkup permasalahan adalah :

I.2.1. Identifikasi Masalah

Berdasarkan penelitian penulis sehubungan dengan materi yang penulis angkat dalam skripsi ini, penulis menemukan beberapa masalah antara lain :

1. Minimnya mengenkripsi suatu gambar dengan menggunakan algoritma 3DES (*Triple Data Encryption Standard*).
2. Belum diketahuinya besar ukuran file gambar yang dapat dienkripsi dengan menggunakan algoritma 3DES dalam waktu satu detik.
3. Sulitnya menerapkan kekuatan algoritma 3DES terhadap serangan *brute force*.

I.2.2. Rumusan Masalah

Berikut rumusan masalah yang akan dicari pemecahannya melalui penulisan skripsi ini :

1. Bagaimana cara mengenkripsi suatu gambar dengan menggunakan algoritma 3DES (*Triple Data Encryption Standard*) ?
2. Berapa besar ukuran file yang dapat dienkripsi dengan menggunakan algoritma 3DES dalam waktu satu detik ?
3. Mengetahui kekuatan algoritma 3DES terhadap serangan brute force ?

I.2.3. Batasan Masalah

Adapun batasan masalah yang penulis berikan dalam pembuatan skripsi ini adalah sebagai berikut :

1. Ukuran gambar yang digunakan pada uji coba 200x200 piksel.
2. Format gambar yang dapat diproses adalah format jpg, bmp, dan png.
3. Pemodelan perancangan aplikasi menggunakan *Unified Modeling Language* (UML) 2.0.

I.3. Tujuan Dan Manfaat

Tujuan dan manfaat yang penulis peroleh dari penelitian skripsi ini adalah sebagai berikut :

I.3.1. Tujuan

Tujuan yang ingin dicapai melalui penulisan skripsi ini adalah sebagai berikut:

1. Menerapkan prinsip-prinsip aplikasi untuk menganalisa proses kebutuhan dalam mengenkripsi file gambar.
2. Merancang aplikasi enkripsi file gambar diterapkan melalui jaringan lokal.

3. Menganalisa file gambar yang ditransmisikan pada enkripsi.

I.3.2. Manfaat

Manfaat yang diharapkan dari penulisan skripsi ini adalah :

1. Aplikasi yang dirancang akan dapat digunakan dengan system enkripsi pada file gambar.
2. Memberikan keamanan pada file gambar dapat disimpan diperangkat komputer sehingga tidak perlu khawatir hilang.
3. Enkripsi berfungsi sebagai penerapan artifisial inteligensi pada file gambar.

I.4. Metodologi Penelitian

Berisikan metoda / cara / prosedur yang digunakan dalam melaksanakan penelitian serta menyelesaikan masalah yang telah didefinisikan pada poin 3 (Permasalahan). Mulai dari pengumpulan data sampai kepada terselesaikannya masalah. Ada beberapa prosedur yang digunakan dalam penelitian ini adalah sebagai berikut :

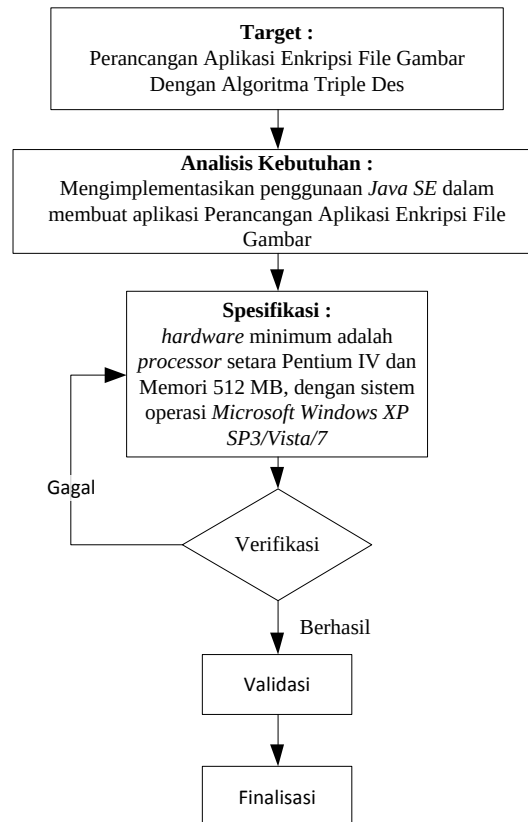
1. Prosedur Perancangan

Merupakan tata cara dan langkah-langkah yang diperlukan untuk mencapai tujuan perancangan yang dilakukan. Langkah-langkahnya adalah :

- a. Menganalisis permasalahan keamanan yang ada dalam aplikasi enkripsi file gambar.
- b. Merancang sistem yang baru dengan menggunakan model UML (*Unified Modeling Language*).

c. Membuat aplikasi dengan bahasa pemrograman Java.

Berikut adalah skema dalam melaksanakan penelitian :



Gambar I.1. Prosedur Perancangan

Pada gambar prosedur perancangan sistem di atas dapat diuraikan ke dalam beberapa tahap yaitu Tujuan Penelitian, tahap Analisa (*Analisis*), Spesifikasi, tahap Perancangan (*Design*) dan tahap Penerapan (*Implementasi*), Verifikasi serta tahap Validasi. Dan kegiatan yang dilakukan pada tiap-tiap tahap adalah sebagai berikut:

1. Target :

Menciptakan Perancangan Aplikasi Enkripsi File Gambar Dengan Algoritma TRIPLE DES.

2. Analisis Kebutuhan

Sesuai penyelesaian masalah yang akan dilakukan, kebutuhan pokok yang harus ada pada “*Perancangan Aplikasi Enkripsi File Gambar Dengan Algoritma TRIPLE DES*” adalah sebagai berikut :

- a. Mengimplementasikan penggunaan *Java* dalam membuat aplikasi Rancang Bangun aplikasi perancangan aplikasi enkripsi file gambar.
- b. Memberikan kemudahan dan solusi cepat dalam mengenkripsi file gambar.

3. Spesifikasi

Secara umum yang dirancang memiliki spesifikasi sebagai berikut :

- a. Di bangun dengan menggunakan *Java* sebagai *tools* pemrogramannya.
- b. Aplikasi yang dibuat dapat digunakan pada komputer, dengan *hardware* minimum adalah *processor* setara Pentium IV dan Memori 512 MB, dengan sistem operasi *Microsoft Windows XP SP3/Vista/7*.

4. Desain dan Implementasi

Setelah jelas spesifikasi, selanjutnya dilakukan pembuatan desain aplikasi dengan memanfaatkan masing-masing komponen. Untuk mengetahui apakah pemanfaatan masing-masing komponen sudah dapat bekerja dengan baik perlu dilakukan uji coba sementara dengan melakukan implementasi tahap awal.

5. Verifikasi

Selanjutnya dilakukan verifikasi terhadap aplikasi yang telah masuk ke tahap implementasi tahap awal sehingga data-data, komponen-komponen yang terintegrasi benar-benar telah sesuai dengan prinsip kerja aplikasi dan apa yang menjadi tujuan penulis. Dengan demikian bila ada kesalahan atau kekurangan

dapat diperbaiki terlebih dahulu sebelum dirangkai menjadi kesatuan aplikasi yang utuh dan siap pakai.

6. Validasi

Pada tahap ini dilakukan pengujian aplikasi secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan sistem. Pengujian fungsional dilakukan untuk mengetahui bahwa aplikasi dapat bekerja dengan baik sesuai dengan prinsip kerjanya. Pengujian ketahanan berkaitan dengan kemampuan aplikasi untuk dapat berjalan pada sistem minimum yakni pada PC dengan PC dengan *Processor* IV 1,6 Ghz, Memori 512MB, Kartu Grafik 512 MB. Dari validasi ini dapat diketahui kesesuaian hasil perancangan dengan analisis kebutuhan yang diharapkan.

7. Finalisasi

Merupakan tahap akhir, berupa implementasi aplikasi “*Perancangan Aplikasi Enkripsi File Gambar Dengan Algoritma TRIPLE DES*”.

I.5. Keaslian Penelitian

Sebagai bukti penelitian yang akan dibuat, maka penelitian akan dibandingkan terhadap penelitian sejenis yang pernah dilakukan perbandinganya dapat dilihat pada tabel 1 dibawah ini :

Tabel I.1. Keaslian Penelitian

No	Materi Perbandingan	Instrumen
	Penelitian pertama : Enkripsi Dan Dekripsi Data Dengan Algoritma 3 Des (Triple Data Encryption Standard)	
	Hasil : Proses enkripsi dan dekripsi suatu data dengan algoritma 3DES	

dilakukan dengan cara mengimplementasikan algoritma DES sebanyak tiga kali, sesuai dengan pemilihan kuncinya dan urutan proses yang dipilih		
1.	Algoritma yang digunakan	3DES
2.	Penelitian	Enkripsi dan Deskripsi Data
3.	Basis Aplikasi	Desktop
4.	Perangkat Lunak	Belum Diketahui
Penelitian kedua : Aplikasi Enkripsi Dan Dekripsi Pesan Dengan Algoritma Vigenere Cipher Pada Ponsel Menggunakan J2me. Hasil : Hasil pengujian digambarkan dengan tabel hasil pengujian, yang kemudian dijabarkan dengan grafik hasil uji coba terhadap file yaitu Grafik kecepatan aplikasi terhadap besar file, Grafik rerata waktu eksekusi terhadap besar file dan Tabel perbandingan kecepatan maksimum dengan kecepatan rerata terhadap besar file.		
1.	Algoritma yang digunakan	Vigenere Cipher
2.	Penelitian	Enkripsi Dekripsi Pesan
3.	Basis Aplikasi	Tidak Diketahui
4.	Perangkat Lunak	Tidak digunakan
Penelitian yang akan dibuat : <i>Perancangan Aplikasi Enkripsi File Gambar Dengan Algoritma TRIPLE DES</i>		
1.	Algoritma/Metode yang digunakan	3DES
2.	Penelitian	Enkripsi File Gambar.
3.	Basis Aplikasi	Dekstop.
4.	Perangkat Lunak	Algoritma RC4, Java SE

I.6. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam Skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang sedang dihadapi.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan dan desain sistem secara detail.

BAB IV : HASIL DAN UJI COBA

Pada bab ini menerangkan hasil dan pembahasan program yang dirancang serta kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan di masa yang akan datang untuk sistem.