BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi Informasi saat ini memiliki peran penting di segala aspek kehidupan, baik dalam dunia bisnis , politik hingga pertahanan keamanan negara, Hal ini di sebabkan sangat penting dan bergunanya peran teknologi informasi dalam kehidupan. Dengan perkembangan teknologi informasi yang ada saat ini kita dapat mengolah data dengan sangat mudah, mendapatkan suatu informasi yang kita butuhkan dengan akurat, aman dan efektif waktu, serta dengan biaya yang kita keluarkan lebih efisien merupakan keunggulan yang mendasar dari sebuah teknologi informasi . dengan keunggulan itulah menjadikan teknologi informasi saat ini banyak berperan penting dalam segala bidang dan aspek kehidupan yang ada dan berkembang sesuai kebutuhan masyarakat sekarang.

Demikian halnya dengan kebutuhan masyarakat akan keamanan informasi, dengan adanya teknologi informasi, data-data informasi rahasia yang seharusnya tidak boleh diketahui oleh orang lain kecuali pemilik informasinya sangat mungkin terjadi, karena hal tersebut termasuk dalam teknologi informasi dalam hal keamanan informasi. Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan, data, atau informasi dengan cara menyamarkannya menjadi

bentuk tersandi yang tidak mempunyai makna[1] . Dalam kriptografi, terdapat 2 proses utama, enkripsi dan dekripsi. Enkripsi adalah proses penyandian pesan asli atau *plaintext* menjadi *ciphertext* (teks tersandi). Sedangkan dekripsi adalah proses penyandian kembali *ciphertext* menjadi *plaintext* [2]. Dengan membuat algoritma kriptografi berlapis di yakini akan membuat *chiphertext* tersebut memiliki level keamanan lebih tinggi. Metode kriptografi berlapis yakni dengan mengunakan kriptografi OpenSSL dan hash MD5 . Dimana hash MD5 digunakan untuk meng-enkripsi password kunci sedangkan OpenSSL untuk enkripsi isi keseluruhan pesan di yakini akan membuat level keaman informasi yang lebih tinggi. OpenSSL adalah sebuah *toolkit* kriptografi yang dijalankan pada protokol jaringan *Secure Socket Layer* (SSL) dan *Transport Layer Security* (TLS)[3]. OpenSSL dipilih karena masih minimnya dokumentasi yang beredar dimasyarakat luas dan sebagian masyarakat hanya mengetahui bahwasannya OpenSSL hanya digunakan pada *Hypertext Transfer Protokol Secure* (HTTPS) yaitu versi aman dari HTTP, protokol komunikasi dari World Wide Web.

Selanjutnya yang tak kalah menarik adalah Steganografi. Steganografi adalah ilmu menyembunyikan teks yang tersembunyi pada media lain yang telah ada sedemikian sehingga teks tersembunyi menyatu dengan media itu[4] . Steganogafi di sebut juga seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan

---

[1] Munir, R. *Kriptografi.*(Bandung:Informatika, 2006).
[2] Ibid.
[3] Pravir Chandra, Matt Messier, John Viega, *Network Security with OpenSSL.*(Sebastopol:O'Reilly, 2002).
[4] Rifki Sadikin, *Pengantar Kriptografi dan Keamanan Jaringan,*(Yogyakarta: Andi Offset,2012). 10

dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sehingga informasi rahasia bisa di simpan dalam sebuah media digital berupa gambar. Hal ini sangat ampuh dalam hal mengklabuhi orang awam. Karena didalam sebuah media digital gambar terdapat sebuah data atau informasi rahasia yang tidak bisa di baca oleh kasat mata.

Berdasarkan latar belakang diatas, maka penulis mencoba mengembangkan aplikasi berbasis web yang digunakan untuk keamanan data dan informasi. Karena pengguna Internet mencakup pengguna Smartphone dan Komputer. Dengan adanya aplikasi ini, diharapkan dapat membantu dalam hal pengamanan sebuah data informasi. Untuk itu penulis membuat penelitian skripsi dengan judul "Aplikasi Keamanan Data dan Informasi Berlapis dengan Metode Steganografi LSB, kriptografi OpenSSL dan MD5 Berbasis Web".

1.2 Rumusan Masalah

Bagaimana merancang aplikasi pengaman data dan informasi berlapis dengan metode steganografi LSB , kriptografi OpenSSL dan MD5 berbasis web?

1.3 Batasan Masalah

Batasan masalah ini dibuat agar pembahasan dalam perancangan aplikasi pengaman data dan informasi steganografi berbasis web ini tidak menyimpang dari fokus penelitiannya, berikut kami paparkan beberapa batasan masalah yang perlu dibuat , yakni:

1. Aplikasi berbasis web.
2. Pesan yang akan dienkripsi berupa text.
3. Enkripsi dan deskripsi pesan mengunakan perpustakaan/liberary Kriptografi OpenSSL dengan algoritma AES 128 bit.
4. Enkripsi MD5 menghasilkan panjang kunci 32 karakter yang digunakan untuk password kunci pada saat encripsi dan deskripsi pesan.
5. File yang akan dienkripsi berupa media digital gambar dalam extensi jpg , jpeg dan png .
6. Ukuran file yang dapat dienkripsi maksimal 5 MB.
7. File hasil enkripsi berupa media digital gambar dalam extensi png.
8. File yang akan dideskripsi berupa media digital gambar dalam extensi png.
9. Software yang digunakan peneliti dalam membuat aplikasi ini yaitu PhpStorm 8.0.2 dan PHP sebagai bahasa pemrogramannya.

10. Software yang digunakan untuk menjalankan aplikasi ini yaitu xampp sebagai web server dan browsernya menggunakan Mozila Firefox.

1.4 Tujuan Penelitian

Merancang aplikasi pengaman data dan informasi berlapis dengan metode steganografi LSB , kriptografi OpenSSL dan MD5 berbasis web.

1.5 Manfaat Penelitian

Manfaat yang ingin dicapai dari penelitian ini adalah sebagai berikut:

1. Bagi Penulis

   Menerapkan dan mengembangkan ilmu serta teori-teori yang telah didapatkan selama studi sebagai persiapan pengaplikasian pada dunia kerja.

2. Bagi Perkembangan Ilmu Pengetahuan

   Penulis berharap aplikasi yang dirancang ini, dapat ikut ambil dan menjadi pelopor diciptakannya aplikasi-aplikasi baru tentang pengamanan data dan informasi yang sangat penting.

3. Bagi Masyarakat

   Penulis berharap aplikasi pengaman data dan informasi berlapis berbasis web ini dapat digunakan masyarakat umum sebagai media keamanan informasi.

1.6 Metode Penelitian

Adapun metode yang dilakukan untuk perancangan aplikasi pengaman data dan informasi berlapis dengan metode steganografi LSB , kriptografi OpenSSL dan MD5 berbasis web adalah sebagai berikut:

1.6.1 Metode Pengumpulan Data

Metode kepustakaan adalah metode pengumpulan data yang dilakukan dengan cara membaca, mempelajari, mencari bahkan menulis dari sebuah buku, artikel, jurnal ilmiah, majalah baik dari media cetak maupun media elektronik yang berkaitan dengan topik yang dibahas dalam pembuatan aplikasi.

1.6.2 Metode Analisis Data

Melakukan analisis data yang telah dikumpulkan untuk penyusunan laporan kemudian merancang dan membuat aplikasi. Analisis data dalam penelitian meliputi :

a. Analisis kebutuhan fungsional

   Merupakan pendefinisian fungsi sistem yang harus disediakan, bagaimana reaksi sistem terhadap input dan apa yang harus dilakukan sistem pada situasi khusus.

b. Analisis kebutuhan non fungsional

   Menganalisis kebutuhan pendukung bagi sistem.

1.6.3 Metode Perancangan Aplikasi

Metode perancangan aplikasi meliputi perancangan antarmuka dan perancangan algoritma yang akan digunakan dalam aplikasi yang akan dibuat.

1.6.4 Metode Implementasi Aplikasi

Metode ini adalah mengimplementasikan aplikasi yang sudah dirancang, yaitu implementasi menggunakan perangkat lunak menulis baris kode atau biasa disebut *programming* untuk menghasilkan aplikasi yang akan diinginkan.

1.6.5 Metode Testing

Aplikasi yang sudah dibuat masuk dalam metode testing, metode ini digunakan untuk mendapatkan diantaranya data-data dan hasil yang diinginkan. Pada metode ini menghasilkan dokumentasi-dokumentasi dari aplikasi yang dibuat untuk digunakan sebagai panduan penggunaan aplikasi

1.7 Sistematika Penulisan

Untuk memperoleh gambaran yang konprehensif dan mudah dimengerti mengenai isi penulisan skripsi ini secara umum, maka dapat dilihat dari sistematika penulisan skripsi di bawah ini:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang , rumusan masalah , batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab landasan teori merupakan tinjauan pustaka, berisi dasar-dasar teori yang digunakan dalam penyusunan skripsi. Pada bab ini juga berisi tentang software / tools yang digunakan dalam pembuatan aplikasi.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini menjelaskan tentang analisis terhadap kasus yang diteliti dan perancangan aplikasi yang akan dibuat.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini memaparkan hasil-hasil dari tahapan penelitian, mulai dari analisis, desain, implementasi desain, hasil testing dan implementasi.

BAB V PENUTUP

Bab ini berisi tentang kesimpulan dan saran dan kekurangan, yang diharapkan dapat bermanfaat untuk pengembangan pembuatan program aplikasi keamana data dan informasi selanjutnya.