BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan data adalah suatu hal yang diinginkan semua orang untuk menjaga privasi. Baik dari keamanan data di memori pribadi atau pun saat pengiriman data tersebut. Agar data yang disimpan atau pun yang dikirim aman dari orang – orang yang tidak bertanggung jawab dengan menyembunyikan data menggunakan algoritma kriptografi.

Transaksi pengiriman data adalah hal yang biasa saat ini, data tersebut berupa teks, gambar, video, file dan lainnya. Seiring dengan itu, algortima penyandian telah berkembang sejak zaman dahulu dan terus berkembang menjadi lebih rumit dan lebih sulit dipecahkan oleh orang yang tidak berhak.

Pengamanan data dengan cara enkripsi dan dekripsi dengan kunci algoritma atau yang sering disebut dengan algoritma, mendukung pengguna untuk memenuhi dua aspek keamanan informasi, yaitu perlindungan terhadap kerahasiaan data informasi dan perlindungan terhadap pemalsuan dan pengubahan informasi.

Enkripsi adalah merubah data asli ke dalam bentuk yang tidak dimengerti dan jika data itu ingin diketahui maka data tersebut harus didekripsi dengan kunci yang dipakai untuk enkripsi. Dalam kriptografi enkripsi dan dekripsi memiliki banyak algoritma yang digunakan dalam penerapannya, seperti RC4,AES,DES, dan lainnya.

Enkripsi dan dekripsi banyak diterapkan hanya pada saat pengiriman data, namun enkripsi dan dekripsi bisa juga diterapkan terhadap file tersimpan untuk mengamankannya. Seperti permasalahan Pada *smartphone* yang menerapkan pengamanan file dengan folder dikunci, file gambar yang terdapat pada folder tersebut masih bisa diakses melalui aplikasi-aplikasi media sosial, sehingga untuk lebih mengamankannya sebaiknya file sudah terenkripsi.

File gambar saat diubah kedalam bentuk teks mempunyai jumlah character yang besar sehingga jika file gambar dienkripsi dengan mengenkripsi perkarakter harus menggunakan metode algoritma yang cepat dalam melakukan prosesnya, menurut Ir, Yusuf Kurniawan,MT pada bukunya yang berjudul kriptograf keamanan internet dan jaringan komunikasi, algoritma RC4 beroperasi dengan metode XOR maka operasi enkripsi dengan XOR berlangsung sangat cepat sehingga sering digunakan bila diinginkan kecepatan yang memadai.[1]

Dalam melakukan enkripsi gambar dengan algoritma RC4 perlu dibantu oleh algoritma radix base 64 karena adanya perbedaan pembacaan karakter dan File, sehingga saat melakukan dekripsi ada beberapa karakter yang berubah mengakibatkan file asli tidak sama dengan file hasil dekripsi.

Berdasarkan latar belakang, maka diperlukan sebuah fasilitas yang dapat melakukan enkripsi dan dekripsi gambar untuk keamanannya pada penyimpanan maupun pengiriman. Oleh karena itu penulis bermaksud untuk merancang aplikasi berbasis web yang bisa melakukan enkripsi dan dekripsi gambar menggunakan algoritma Base64 dan RC4.

1.2 Rumusan Masalah

Perumusan masalah dalam skripsi ini adalah sebagai berikut:

a. Bagaimana cara membuat sebuah system enkripsi dan dekripsi gambar menggunakan algoritma base64 dan algoritma RC4?
b. Apa perbedaan jika proses tidak menggunakan algoritma base64?
c. Apakah ukuran hasil dekripsi sama dengan ukuran data sebelum enkripsi?

1.3 Batasan Masalah

Pada aplikasi ini penulis membatasi masalah dengan membuat sebuah aplikasi web yang akan digunakan dalam pengamanan gambar dan hanya meliputi:

a. Data yang dienkripsi hanya berupa gambar berekstensi .jpg, .png, .gif, .bmp, .tiff
b. Flatform system adalah PHP > versi 5.3.5
c. Algoritma encode dan decode yang digunakan adalah base64
d. Algoritma kriptografi yang digunakan adalah RC4
e. File gambar yang dienkripsi dan didekripsi sekali proses adalah 5 gambar
f. Maksimal ukuran file yang dienkripsi adalah 2MB.

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud Penelitian

Berdasarkan uraian latar belakang masalah dan rumusan masalah diatas, maka maksud dari penelitian ini ialah untuk mengamankan file berupa gambar secara pribadi dan aman saat dikirim.

1.4.2 Tujuan Penelitian

Tujuan penelitian yang hendak dicapai ialah membuat Aplikasi berbasis web yang dapat melakukan enkripsi dan dekripsi gambar dengan algoritma base64 dan RC4 yang diharapkan mampu mengamankan gambar yang bersifat privasi.

1.5 Metode Penelitian

Model yang digunakan untuk menyelesaikan penelitian ini adalah Prototyping. Tahapan-tahapan dalam Prototyping Adalah:

1.5.1 Pengumpulan kebutuhan

Mengumpulkan Data kebutuhan fungsional dan non fungsional. Mengumpulkan dasar – dasar teori dan cara implementasinya

1.5.2 Membangun prototyping

Membangun prototyping dengan membuat perancangan sementara yang berfokus pada encode dan decode base64 serta enkripsi dan dekripsi algoritma RC4.

1.5.3 Evaluasi protoptyping

Evaluasi ini dilakukan dengan wawancara apakah prototyping yang sudah dibangun sudah sesuai dengan keinginan users. Jika sudah sesuai maka langkah 4 akan diambil. Jika tidak prototyping direvisi dengan mengulang langkah 1, 2, dan 3.

1.5.4 Mengkodekan sistem

Dalam tahap ini prototyping yang sudah disepakati diterjemahkan ke dalam bahasa PHP.

1.5.5 Menguji Sistem

Setelah sistem sudah menjadi suatu perangkat lunak yang siap pakai, harus dites dahulu sebelum digunakan.

1.5.6 Evaluasi Sistem

Pengguna mengevaluasi apakah sistem yang sudah jadi sudah sesuai dengan yang diharapkan. Jika ya, langkah 7 dilakukan; jika tidak, ulangi langkah 4 dan 5.

1.5.7 Menggunakan system

Perangkat lunak yang telah diuji dan pantas maka siap untuk digunakan.

1.6 Sistematika Penulisan

Untuk lebih memahami pembahasan yang terdapat pada proposal skripsi ini, maka penulisan materi yang akan disampaikan disusun dalam sistematika sebagai berikut:

1.6.1 BAB I PENDAHULUAN

Pada bab ini akan dibahas latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan.

1.6.2 BAB II LANDASAN TEORI

Bab ini akan menjelaskan tentang landasan teori yang digunakana dalam proses perancangan dan pembuatan sebuah aplikasi berbasis web dan teori – teori yang berhubungan dengan kriptografi dan encode serta decode.

1.6.3 BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi uraian analisis dan perancangan apikasi, serta desain sise yang akan dibuat

1.6.4 BAB IV IMPLEMENTSI DAN PEMBAHASAN

Bab ini akan memaparkan hasil-hasil gambaran umum aplikasi dan pembahasan terhadap program aplikasi yang telah dibuat serta implementasi aplikasi yang telah dibuat.

1.6.5 BAB V PENUTUP

Bab ini berisi kesimpulan dan saran yang berkaitan dengan aplikasi ini, sehingga data digunakan untuk pengembangan penelitian serupa selanjutnya.

1.6.6 DAFTAR PUSTAKA

Dalam bab ini berisi tentang pustaka yang digunakan penulis sebgai acuan dan bahan dalam pembuatan laporan skripsi.