BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika pengirimannya dilakukan melalui jaringan publik, apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak memiliki wewenang.[1]

Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan sistem kriptografi yaitu dengan menyediakan isi informasi (plaintext) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi (encipher), dan untuk memperoleh kembali informasi yang asli, dilakukan proses deskripsi (decipher), disertai dengan menggunakan kunci yang benar.[1]

Pada zaman teknologi informasi sekarang, data atau informasi merupakan suatu asset yang sangat berharga dan harus dilindungi. Hal ini juga diikuti oleh kemajuan teknologi komputer. Kemajuan teknologi komputer membantu semua aspek kehidupan manusia. Dari hal kecil sederhana sampai hal yang sangat rumit sekalipun bisa dikerjakan komputer. Keunggulan dari aplikasi komputer ini selain memberi kemudahan terhadap berbagai kegiatan pengolahan data dan informasi di berbagai bidang kehidupan, misalnya penggunaan komputer dalam bidang pemerintahan, organisasi social, militer, bank, pendidikan, transportasi, perdagangan, industri, dan lain sebagainya. Dengan adanya kemajuan dalam teknologi informasi, komunikasi dan komputer maka kemudian muncul masalah

baru, yaitu masalah keamanan akan data dan informasi dan dalam hal ini akan membuka peluang bagi orang-orang yang tidak bertanggung jawab untuk menggunakannya sebagai tindak kejahatan. Dan tentunya akan merugikan pihak tertentu.[2]

Oleh karena itu untuk menghindari agar hal tersebut tidak terjadi, penulis menggunakan algoritma kriptografi DES dengan kunci Simetri untuk proses enkripsi dan deskripsi data. Kriptografi telah menjadi suatu bagian yang tidak dapat di pisahkan dari sistem keamanan jaringan, Salah satu metode enkripsi data adalah Data Encryption Standard (DES). Data Encryption Standard (DES) merupakan algoritma cipher blok yang popular karena dijadikan standar algoritma enkripsi kunci-simetri. Sebenarnya DES adalah nama standar enkripsi simetri, nama algoritma enkripsinya sendiri adalah DEA (Data Encryption Algorithm), namun nama DES lebih popular dari pada DEA. Dari latar belakang di atas penulis mencoba untuk membuat rancangan keamanan data dengan menggunakan algoritma kriptografi DES, dengan mengambil judul "Analisis dan Perancangan Keamanan Data Menggunakan Data Encryption Standar (DES)".

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas dalam penelitian ini dirumuskan bagaimana merancang dan mengimplementasikan suatu keamanan data dalam sistem pengarsipan surat menggunakan metode enkripsi dan deskripsi dengan algoritma simetri yang dapat mendukung keamanan sistem pengarsipan surat berdasarkan file surat yang diproses didalam sistem?

1.3 Batasan Masalah

Supaya dalam penyusunan laporan Skripsi ini dapat mencapai sasaran dan tujuan yang diharapkan, maka permasalahan dibatasi sebagai berikut :

1. Aplikasi yang akan dibuat dibatasi pada kode halaman web dengan berekstensi php.
2. Aplikasi akan dibuat mengimplementasikan Algoritma DES dengan kunci Simetri dan Php Obfuscator menggunakan bahasa pemrograman java desktop(JavaSE).
3. Aplikasi akan membuat suatu berkas berekstensi php berisi kode enkripsi dan kode hasil dekripsi yang digunakan untuk mengamankan file tesebut.
4. Spesifikasi yang dibutuhkan meliputi Sistem Operasi, DBMS, Development Tools dan Bahasa Pemrograman yang dipakai akan diuraikan pada Tabel 1.1.

Tabel 1.1. Spesifikasi pembangunan aplikasi

Sistem Pengolahan Data	Spesifikasi
Sistem Operasi	Windows XP atau Linux
DBMS	MySQL
Development Tools	Java
Enkripsi Data	Algoritma Simetri
Bahasa Pemrogaman	PHP

1.4 Maksud dan Tujuan Penelitian

Berdasarkan pada latar belakang dan permasalahan yang sudah diuraikan sebelumnya, maka tujuan penelitian sebagai berikut,

1. Membangun sistem yang dapat mengelola keamanan data halaman web php agar kode didalamnya sulit dibaca oleh pelaku kejahatan yang bermaksud mencuri data dan atau berencana melakukan pengrusakan isi web itu sendiri.
2. Merancang dan membangun pengelola keamanan data dalam sistem pengarsipan surat menggunakan Algoritma Kriptografi DES dengan kunci Simetri.

1.5 Metode Penelitian

1.5.1 Metode Pengumpulan Data

1.5.1.1 Metode Observasi

Metode observasi dilakukan langsung dengan melihat langsung bagaimana proses atau cara kerja dari permasalahan yang terjadi, kemudian proses penugasan yang terjadi di beberapa sistem dan aplikasi.

1.5.1.2 Metode Wawancara

Wawancara dilakukan untuk mengetahui masalah yang timbul dan dialami langsung oleh sebuah instansi terkait, serta menggali suatu masalah yang sering dialami dan itu merugikan.

1.5.1.3 Metode Studi Pustaka

Dalam penelitian mengenai pengelola keamanan data ini tidak lepas dari data yang terdapat dari buku-buku yang menjadi referensi seperti pedoman pembuatan penulisan tugas akhir, forum diskusi online dan buku-buku lain yang

berhubungan dengan penyusunan usulan penelitian dan rancangan sistem yang akan dibuat serta menyelesaikan masalah yang akan dihadapi.

1.5.2 Metode Analisis Data

Analisis data merupakan tahapan proses penelitian, dimana data yang sudah dikumpulkan dikelola untuk diolah dalam rangka menjawab rumusan masalah. Pada penelitian ini penulis menggunakan metode analisis data kuantitatif yang pada umumnya berupa dataset yang masih mentah. Kemudian dataset tersebut diolah lagi menggunakan teknik clearing (membersihkan) data mentah yang tidak relevan untuk diolah.

1.5.3 Metode Perancangan

Perancangan sistem memiliki tujuan menghasilkan perancangan yang dapat memenuhi kebutuhan analisis sistem. Perancangan sistem menghasilkan rincian perancangan yang mudah diimplementasikan pada proses pembuatan program, yaitu berupa perancangan masukan, perancangan keluaran, perancangan platform.

Desain sistem dapat mudah dipahami dengan adanya gambaran yang dibuat dengan beberapa alat. Alat yang digunakan untuk menggambarkan aliran data menggunakan diagram alir data. Alat yang digunakan untuk menggambarkan perancangan proses berbasis objek adalah Unified Modeling Language (UML). Sedangkan alat yang digunakan untuk membuat perancangan basis data yaitu Entity Relationshop Diagram (ERD).

1.5.3 Metode Pengembangan

Dalam penelitian mengenai pengelola keamanan data dalam sistem pengarsipan surat ini, penulis menggunakan metode pengembangan sistem model waterfall. Metode waterfall di mulai dengan tahapan menganalisa kebutuhan sistem, menentukan desain user interface sistem, melakukan pembuatan kode program, melakukan pengujian sistem dan terakhir maintenance sistem agar beradaptasi dengan lingkungan baru dan tetap berjalan sesuai dengan yang dirancang.

1.5.4 Metode Pengujian

Tahap pengujian merupakan tahap terakhir dari pembuatan sistem. Tujuannya adalah menguji kesesuaian aplikasi dengan rancangan dan analisis yang sebelumnya dilakukan, mengurangi adanya kesalahan pada sistem dan memastikan aplikasi ini dapat diimplementasikan.

1.6 Sistematika Penulisan

Sistematika dalam penelitian ini terdiri dari lima bab

BAB I PENDAHULUAN

Bab satu berisi penjelasan dari latar belakang masalah dari penelitian yang penulis lakukan, batasan-batasan masalah dalam pengembangan sistem, penjelasan mengenai tujuan yang ingin dicapai melalui penelitian yang telah dilakukan, metodologi penelitian serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi tinjauan pustaka, dasar-dasar teori yang digunakan, pembahasan mengenai penelitian terdahulu yang digunakan sebagai bahan referensi dalam penelitian ini.

BAB III METODE PENELITIAN

Bab ini berisi alat dan bahan penelitian, alur penelitian, lingkungan yang dipakai untuk mengembangkan program, strategi pemecahan masalah dan struktur data yang digunakan.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi hasil dan pembahasan, tahapan ini merupakan tahapan yang penulis lakukan untuk memaparkan hasil yang disertai dengan pembahasan.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran yang dapat peneliti rangkum selama proses penelitian sebagai acuan untuk pengembangan sistem ke tahap selanjutnya.

DAFTAR PUSTAKA

Daftar Pustaka merupakan bagian yang berisi referensi sumber dari studi literatur yang digunakan dalam penyusunan laporan skripsi ini.