BAB I

PENDAHULUAN

1.1 Latar Belakang Permasalahan

Ketika Tahun Ajaran Baru Sekolah dimulai, beberapa sekolah menerapkan sistem seleksi ujian masuk sekolah. Sistem seleksi ujian masuk yang diterapkan dibanyak sekolah masih bersifat konvensional yaitu siswa mengikuti proses pendaftaran dan siswa yang dinyatakan lulus secara administrasi oleh pihak sekolah berhak mengikuti seleksi ujian masuk pada hari yang telah ditentukan. Kemudian pihak sekolah akan mengumumkan hasil seleksi ujian sesuai dengan waktu yang telah ditentukan sebelumnya. Proses ujian yang dilakukan dengan cara seperti itu, tentu saja masih mengalami beberapa masalah diantaranya, lamanya proses pengolahan hasil ujian, kesalahan ketika melakukan proses pengaolahan hasil ujian, dan adanya kemungkinan manipulasi data ujian oleh pihak yang tidak bertanggung jawab, serta masalah pemborosan tinta dan kertas. Untuk mencegah hal tersebut, maka dikembangkanlah sistem ujian online yang dapat diakses oleh para siswa lewat komputer dan internet, dengan adanya sistem ujian online ini maka proses seleksi ujian masuk menjadi lebih efektif dan efisien

Karena aplikasi yang akan dibangun berbasis web dan menggunakan bahasa pemograman php dimana data yang dikirimkan dalam bentuk plainteks, maka akan memunculkan beberapa masalah ketika proses transfer data dilakukan seperti, adanya usaha untuk menggagalkan proses transfer data, menyadap proses transfer data

atau melakukan modifikasi terhadap data yang dikirimkan. Untuk mencegah hal tersebut maka data yang dikirimkan harus diubah dalam bentuk enkripsi atau cipher teks. Php sendiri sudah memiliki library khusus untuk menangani proses enkripsi atau dekripsi, akan tetapi library yang sudah ada tersebut merupakan library yang bisa compatible dengan berbagai jenis algoritma enkripsi dekripsi, sehingga jika dilihat dari segi sintak dan kecepatan kurang maksimal untuk sistem yang akan dibangun. Oleh karena itu akan dibuat library tambahan yang digunakan sebagai pengganti fungsi enkripsi dekripsi dari library yang sudah ada sebelumnya. Library yang dibanguan dikhususkan untuk satu algoritma saja, sehingga library tersebut mudah untuk diimplemtasikan, lebih simple dalam pemakaiannya dan memiliki performa yang maksimal.

Algoritma yang akan diimplementasikan dalam aplikasi ini adalah algoritma kunci simetris. Kunci simetri (secret key) adalah salah satu algoritma kriptografi yang digunakan untuk melakukan enkripsi dan dekripsi, dengan menggunkan kunci rahasia yang sama. Salah satu algoritma dari algoritma kunci simetris adalah algoritma RC6. RC6 adalah algoritma blok kode (block cipher) yang sangat aman, padat, sederhana dan menawarkan performansi yang sangat bagus dan fleksibel, dikembangkan dari algoritma RC5 oleh Ronald Linn Rivest, Ray Sidney, Matt JB.Rodshaw dan Yiquin Yin dari RSA security Inc. pada tahun 1998. Algoritma RC6 merupakan algoritma block cipher yang paling tepat digunakan dibandingkan algoritma block cipher lainnya. (Dony Aryus, 2008).

1.2 Perumusan Permasalahan

Pada perumusan permasalahan ini, akan diungkapkan lebih rinci apa yang akan diteliti sehingga akan memberikan gambaran yang jelas. Untuk memecahkan permasalahan tersebut, maka penulis merumuskan permasalahan sebagai berikut:

1. Bagaimana proses pembangkitkan kunci internal pada algoritma RC6 serta implementasinya pada perangkat lunak yang dibangun?
2. Bagaimana proses enkripsi dan dekripsi data pada algoritma RC6 serta implementasinya pada perangkat lunak yang dibangun?
3. Bagaimana implementasi dari algoritma RC6 dalam menjamin keamanan data pada perangkat lunak yang akan dibangun?

1.3 Batasan Permasalahan

Dalam penyusunan Tugas Akhir ini, penulis memberikan pembatasan permasalahan pada perangkat lunak yang akan dibangun, hal ini di perlukan untuk memfokuskan lingkungan pembahasan, adapun pembatasan permasalah yang diberikan adalah sebagai berikut:

1. Algoritma RC6 digunakan untuk: proses enkripsi dan dekripsi data pada tabel daftar_jawaban ujian, tabel soal, tabel tes dan tabel kunci jawaban.

2. Peserta yang mengikuti ujian online ini adalah siswa yang telah dinyatakan lulus administrasi oleh pihak sekolah. Peserta atau siswa yang telah dinyatakan lulus kemudian diberikan username user_id dan password yang akan digunakan untuk proses login.
3. Enkripsi data dilakukan terhadap data atau query yang ditransmisikan ke database server, dalam hal ini data yang ditransmisikan adalah data jawaban soal ujian siswa yang dikirimkan ketika proses pengisian soal ujian
4. Dekripsi dilakukan terhadap data atau query yang merupakan hasil enkripsi yang ada pada tabel daftar_jawaban, tabel soal dan tabel tes, dari tabel tes selanjutnya hasil dekripsi tersebut akan diguanakan untuk proses pengolahan hasil ujian.

1.4 Tujuan Penelitian

Sejalan dengan permusan permasalahan, maka tujuan yang ingin dicapai pada penelitian ini adalah:

Membuat fungsi tambahan pada Php dengan mengimplementasikan algoritma RC6 untuk proses enkripsi / dekripsi yang akan digunakan pada sistem seleksi ujian masuk online.

1.5 Manfaat Penelitian

Dengan studi implementasi algoritma RC6 dalam sistem ujian online ini, diharapakan dapat memberikan manfaat khususnya bagi penulis, dan umumnya bagi

pembaca karya tulis ini. Adapun beberapa manfaat dalam penulisan karya tulis ini diantaranya:

1. Bagi pihak pengguna:

   Lebih memudahkan pengguna dalam mengikuti proses ujian masuk, serta keamanan data dalam transmisi data jaringan lebih terjamin karena sistem dilengkapi dengan tehnik enkripsi dan dekripsi data.

2. Bagi penulis:

   Hasil penelitian ini diharapkan dapat menambah pengetahuan, pemahaman dan keterampilan penulis serta dapat menjawab keingintahuan penulis terhadap permasalahan yang diteliti, sehingga penulis dapat memahami lebih dalam mengenai permasalahan enkripsi dan dekripsi.

3. Bagi pihak lain:

   Dapat menambah pengetahuan pembaca dan dapat dijadikan sebagai salah satu referensi bagi yang ingin melakukan penelitian lebih lanjut.

1.6 Metode Penelitian

Setiap penelitian terlebih dahulu harus menentukan metode penelitian yang akan dipergunakan. Metode penelitian merupakan cara untuk menentukan berhasil atau tidaknya tujuan yang akan dicapai. Dalam pengerjaan sistem ujian masuk sekolah menengah atas online ini dilakukan beberapa metode penelitian yaitu:

1. Metode Pengumpulan Data

    a. Metode Studi Kepustakaan

    Dengan mengumpulkan dan mempelajari literatur yang berkaitan dengan teori kriptografi, algoritma RC6 dan bahasa pemograman Php serta pembahasan mengenai ujian online.

    b. Metode Wawancara

    Metode ini dilakukan untuk mendapatkan variabel-variabel penting serta batasan (*constraint*) dalam sistem, dalam hal ini metode wawancara dilakukan pada salah satu staf pengajar dan salah satu siswa disekolah yang bersangkutan.

2. Metode Pengembangan Perangkat Lunak

    a. Pendekatan Klasik

    Pendekatan klasik yang digunakan untuk pengembangan perangkat lunak ini adalah model proses *waterfall*. Model proses ini melakukan pendekatan secara sistematis dan urut mulai dari level kebutuhan sistem lalu menuju ke tahap analisis (*analysis*), desain (*design*), implementasi (*coding*), pengujian (*testing/verification*), dan pemeliharaan (*maintenance*).

b. Pendekatan Terstruktur

Pendekatan ini menyediakan tambahan alat – alat dan teknik – teknik untuk mengembangkan sistem disamping tetap mengikuti tahapan dalam pendekatan klasik. Alat yang digunakan dalam pendekatan terstruktur yaitu diagram aliran data (*DFD/Data Flow Diagram*), diagram keterhubungan entitas (*ERD/Entity Realationship Diagram*), kamus data (*Data Dictionary*) dan proses spesifikasi (*PSpec*).

1.7 Sistematika Penulisan

Dalam penulisan skripsi ini, sistematika penulisan dibagi ke dalam beberapa bab, sebagai berikut:

BAB I PENDAHULUAN

Bab ini merupakan pembahasan permasalahan secara umum meliputi latar belakang permasalahan, pembatasan permasalahan, perumusan permasalahan, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini memuat landasan teori yang berfungsi sebagai sumber atau alat dalam memahami permasalahan yang berkaitan dengan enkripsi dan dekripsi menggunakan algoritma RC6.

BAB III METODOLOGI PENELITIAN

Bab ini merupakan penjabaran metode penelitian dari pengembangan system yang digunakan.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini akan membahas secara mendalam tentang hal - hal yang menjadi jawaban dalam perumusan masalah.

BAB V KESIMPULAN DAN SARAN

Kesimpulan merupakan jawaban atas perumusan permasalahan dalam penelitian dan juga intisari dari BAB IV. Saran atas kesimpulan serta rekomendasi pengembangan sistem, penulis utarakan pada subbab saran.