BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam sebuah sistem informasi masalah keamanan dan menjaga kerahasiaan data merupakan salah satu aspek yang penting. Namun masalah keamanan ini sering kali kurang mendapat perhatian dari pihak pemilik dan pengelola sistem informasi. Jika berbicara mengenai masalah keamanan yang berkaitan dengan penggunaan komputer, maka sulit memisahkannya dengan proses *login*. *Login* bertujuan untuk memberikan layanan keamanan pada sistem[1].

Saat melakukan *login* pengguna akan memasukkan *password* dimana *password* tersebut bersifat privasi dan rahasia. Namun demikian penggunaan *user-id* dan *password* bukannya tanpa kelemahan. *User* sering kali memilih *user-id* dan *password* yang pendek dan lemah sehingga mudah dicuri. Selain itu format standar dari *form login* akan mengirimkan *user-id* dan *password* dari *client* ke *server* dalam format *plaintext* atau teks asli. Dalam format ini, sangat mudah bagi para *hacker* untuk mendapatkan data *user-id* dan *password* yang valid dan dapat digunakan pada *form login* yang dimaksud[2].

Untuk menjaga agar *user-id* dan *password* tidak mudah dibaca oleh *hacker* diperlukan proses pengamanan data *user-id* dan *password* tersebut. Alternatif proses pengamanan yang ditawarkan adalah dengan melakukan enkripsi di sisi

client sebelum data dikirimkan ke *server* melalui internet. Dengan demikian yang dikirimkan melalui jaringan internet adalah *ciphertext*. Format *chipertext* juga dapat melindungi *user-id* dan *password* dari pencurian dengan teknik *brute force*[3]. Selanjutnya pada sisi *server* dilakukan dekripsi kembali data sehingga didapatkan data asli.

Salah satu algoritma enkripsi yang terkenal adalah RC6 (*Ron's Code* 6) yang merupakan yang sederhana dan cepat sehingga mudah diaplikasikan untuk pengamanan data. Implementasi baru RC6 dapat dipakai untuk melakukan pengacakan terhadap kunci. Sehingga data *teks* yang diamankan tidak dapat di akses oleh orang yang tidak bertanggung jawab setelah diacak dengan kunci yang tidak beraturan lagi. *Teks* tersebut setelah diacak dapat dikirim kepada orang yang berhak lewat jaringan terbuka seperti Internet.[4]

Dalam penelitian ini diharapkan agar keamanan *userid* dan *password* pada *weblogin* lebih optimal sehingga terhindar dari serangan – serangan yang dilakukan oleh pihak yang tidak bertanggung jawab, maka solusi yang ditawarkan untuk mengatasi permasalahan ini adalah dengan melakukan enkripsi *user-id* dan *password* menggunakan algoritma simetri RC-6, dan diharapkan dapat melindungi *loginweb* dari serangan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka dapat dirumuskan suatu masalah yaitu :

1. Apa metode yang tepat untuk mengamankan *user id* dan *password*?

2. Bagaimana merancang sebuah enkripsi data menggunakan algoritma RC6 pada form *weblogin*?
3. Bagaimana merancang pemodelan algoritma simetri RC6 yang dapat mengamankan *weblogin* dari serangan?
4. Bagaimana mengimplementasikan PHP untuk mengamankan *userid* dan *password*?

1.3 Batasan Masalah

Dalam hal ini penelitian dilakukan dengan batasan-batasan sebagai berikut:

1. Penelitian difokuskan pada penggunaan algoritma enkripsi simetri RC-6 pada *form login* halaman *web*.
2. Variabel pengujian menggunakan query SQL*Injection*.
3. Penelitian dilakukan dengan menggunakan *local host*.
4. *User-id* dan *password* yang dibatasi maksimal 12 karakter.
5. Aplikasi ini dirancang dengan menggunakan bahasa pemrograman php *native*.

1.4 Maksud Penelitian

Maksud dari penelitian dengan judul "Implementasi Keamanan Web Login Menggunakan Algoritma RC-6" untuk memenuhi persyaratan dalam mencapai gelar sarjana pada program studi S1 Informatika di Universitas Amikom Yogyakarta.

Adapun yang menjadi tujuan dalam penelitian ini adalah sebagai berikut :

1. Menghasilkan sebuah form login yang aman.
2. Menguji ketangguhan dari algoritma simetri RC6.
3. Mencegah serangan SQL *injection* pada *login web*.
4. Menjadikan rekomendasi kepada para programer untuk menggunakan algoritma RC6 dalam mengamankan form login web.

1.5 Manfaat Penelitian

Manfaat dilakukan penelitian skripsi ini yaitu :

1.5.1 Bagi Peneliti

Hasil penelitian ini oleh peneliti diharapkan bermanfaat untuk:

a. Menambah wawasan, serta pemahaman dan fungsi dari algoritma enskripsi RC-6 sehingga nantinya berguna di dunia kerja.
b. Mengetahui tahapan – tahapan yang harus dilakukan jika ingin melakukan penelitian.

1.5.2 Bagi Universitas

a. Sebagai asrip dan referensi bagi mahasiswa selanjutnya dalam menyusun tugas kuliah , materi perkuliahan , tugas akhir dan skripsi mengenai algoritma enskripsi RC-6.

1.5.3 Bagi Pembaca

a. Sebagai referensi bagi pembaca terutama mahasiswa dan peneliti dalam menyusun penelitian mengenai algoritma enskripsi RC-6.

b. Desain login web yang aman terhadap serangan SQL*injection*

1.6 Metode Penelitian

Dalam menyusun penelitian skripsi ini ada beberapa metode yang digunakan, antara lain:

1.6.1 Metode Pengumpulan Data

Untuk mendapatkan data yang benar dan relevan sesuai topik yang dibuat, maka diperlukan metode yang tepat untuk mencapai maksud dan tujuan penelitian. Adapun sumber-sumber data yang diperoleh untuk keperluan penelitian ini menggunakan metode studi literature untuk menambah referensi yang relevan akan teori-teori yang diperlukan, penulis melakukan studi literatur dengan membaca dan mempelajari secara literatur yang mendukung penelitian ini. Referensi ini dapat dicari dari buku, jurnal, artikel, laporan penelitian, dan situs-situs di internet yang berhubungan dengan materi skripsi ini.

1.6.2 Metodologi Pengembangan Aplikasi

Pada tahap ini akan dikembangkan pembuatan halaman *login website*, menggunakan metode *waterfall*. Metode ini mempunyai beberapa tahapan yaitu seperti berikut :

1. Analisis Kebutuhan (*Requirement Analisis*)

   Tahap ini pengembang sistem diperlukan komunikasi yang bertujuan untuk memahami perangkat lunak yang diharapkan oleh pengguna dan batasan perangkat lunak tersebut. Informasi ini biasanya dapat diperoleh melalui wawancara, diskusi atau survei langsung. Informasi dianalisis untuk mendapatkan data yang dibutuhkan oleh pengguna.

2. Desain Sistem (*System Design*)

   Spesifikasi kebutuhan dari tahap sebelumnya akan dipelajari dalam fase ini dan desain sistem disiapkan. Desain sistem membantu dalam menentukan perangkat keras (*hardware*) , sistem persyaratan, dan juga membantu dalam mendefinisikan arsitektur sistem secara keseluruhan.

3. Implementasi (*Implementation*)

   Implementasi sistem: adalah tahap meletakkan sistem supaya siap dioperasikan. Kegiatan dalam implentasi sistem adalah:

   a. Mempersiapkan rencana implementasi
   b. Melakukan kegiatan implementasi.
   c. Menindak lanjuti implementasi.

4. Penerapan / pengujian program (*Integration & Testing*)

   Tahapan ini bisa di katakan final dalam pembuatan sebuah sistem. Setelah melakukan analisa, *design* dan pengkodean maka sistem yang sudah jadiv akan digunakan oleh *user*.

5. Pemeliharaan (*Operation&Maintenance*)

   Perangkat lunak yang susah disampaikan kepada pelanggan pasti akan mengalami perubahan. Perubahan tersebut bisa karena mengalami kesalahan karena perangkat lunak harus menyesuaikan dengan lingkungan (peripheral atau sistem operasi baru) baru, atau karena pelanggan membutuhkan perkembangan fungsional.

1.7 Sistematika Penulisan

Penulis skripsi yang berjudul "Implementasi Algoritma RC-6 Untuk Keamanan *Web Login*" mempunyai sistematika penulisan sebagai berikut.

BAB I **PENDAHULUAN**

Bab ini merupakan pendahuluan yang menjelaskan tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II **LANDASAN TEORI**

Bab ini menjelaskan landasan-landasan teori yang digunakan sehubungan dengan Implementasi algoritma RC-6 untuk keamanan *web login*.

BAB III **ANALISIS DAN PERANCANGAN**

Pada bab ini berisi tentang analisis sistem yang akan dibangun, perancangan dan gambaran umum sistem, pembahas tempat penelitian, identifikasi masalah, analisis kebutuhan sistem, serta langkah-langkah dalam implementasi sistem.

BAB IV **HASIL DAN PEMBAHASAN**

Pada bab ini berisi tentang perancangan sistem yang telah dibuat dan pembahasan percobaan serangan pada sistem, serta pengujian terhadap hasil penelitian apakah sesuai dengan tujuan penelitian dan pembahasan

terhadap hasil yang di capai.

BAB V **PENUTUP**

Pada bab ini berisi kesimpulan dan saran dari perumusan masalah yang telah disampaikan.

DAFTAR PUSTAKA Pada bagian ini akan dipaparkan tentang sumber-sumber dan literatur yang digunakan dalam pembuatan laporan tugas akhir.