BAB I

PENDAHULUAN

1.1. Latar Belakang

Bagi negara-negara yang menganut asas demokratis seperti Indonesia, pemilihan umum (pemilu) merupakan kegiatan rutin yang dilaksanakan penduduknya secara periodik. Menurut istilah yang diperoleh dari (http://www.wikipedia.org), *Pemilu adalah proses pemilihan orang(-orang) untuk mengisi jabatan-jabatan politik tertentu. Jabatan-jabatan tersebut beraneka-ragam, mulai dari presiden, wakil rakyat di berbagai tingkat pemerintahan, sampai kepala desa. Pada konteks yang lebih luas, Pemilu dapat juga berarti proses mengisi jabatan-jabatan seperti ketua OSIS atau ketua kelas, walaupun untuk ini kata 'pemilihan' lebih sering digunakan.*

Salah satu pemilihan yang ada di tingkat perguruan tinggi adalah pemilihan ketua BEM, BEM merupakan singkatan dari Badan Eksekutif Mahasiswa, BEM adalah organisasi mahasiswa intra kampus yang merupakan lembaga eksekutif di tingkat Universitas. BEM sendiri dipimpin oleh Ketua dan Wakil Ketua BEM dan umumnya memiliki beberapa departemen yang menaungi masing-masing program kerja.

Dalam pemilihan BEM ini proses otentikasi peserta pemilu dilakukan dengan mencocokan data pemilih yang ada pada kartu mahasiswa dengan data yang ada pada kertas daftar mahasiswa.

Pemilihan dengan sistem seperti ini acapkali menimbulkan banyak masalah, diantaranya kesalahan yang disebabkan karena faktor manusia (*human error*) dan waktu yang lama dalam proses rekapitulasi suara.

Oleh karena itu mulai dikembangkan sistem pemilu melalui internet untuk mempermudah para pemilih. Salah satu masalah yang paling utama dalam pemilu melalui internet adalah masalah keamanan data dalam jaringan. Hal ini disebabkan karena internet merupakan jaringan yang bersifat global. Sehingga beberapa pihak yang luar pun dapat mencari cara untuk masuk ke dalam sistem dan mengacaukannya.

Sebagaimana dikemukakan oleh Silberschatz (2002) mengenai basis data dan keamanannya adalah :

Dengan kebutuhan basis data yang semakin kompleks maka timbul suatu kebutuhan keamanan data dari berbagai macam ancaman diantaranya pembacaan data, modifikasi data dan perusakan data oleh orang yang tidak berhak. Ada beberapa level keamanan pada basis data, diantaranya : keamanan sistem operasi, keamanan sistem manajemen basis data, keamanan jaringan, kemanan fisik, dan keamanan segi manusia.

Untuk mencegah hal tersebut, dikembangkan penerapan kriptografi menggunakan algoritma Arcfour/RC4 pada perangkat lunak yang dibangun dalam penelitian ini.

Penerapan kriptografi pada penelitian ini akan difokuskan bagaimana kriptografi dapat mengamankan transmisi data dalam jaringan dengan tetap memperhatikan integritas data. Algoritma kriptografi yang akan digunakan ialah algoritma kriptografi simetris, algoritma kunci simetris terbagi menjadi *block cipher* dan *stream cipher*. *Block cipher* beroperasi dengan transformasi yang sama dengan blok besar dari plainteks data sedangkan *stream cipher* beroperasi dengan tranformasi waktu pada tiap *byte* plainteks. Karena itu *stream cipher* memiliki kecepatan yang lebih cepat dan kebutuhan *hardware* yang lebih rendah dibandingkan dengan *block cipher*.

RC4 merupakan algoritma *stream cipher* yang paling tepat dibandingkan dengan algoritma *stream cipher* lainnya untuk masalah transmisi hasil *query* basis data seperti ini. Hal itu dikarenakan RC4 memiliki proses enkripsinya yang cukup sederhana dan hanya melibatkan beberapa operasi saja per *byte*-nya.

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, masalah yang diteliti dalam penelitian ini dirumuskan sebagai berikut :

1. Bagaimana pola algoritma kriptografi RC4 ?
2. Keamanan data seperti apa yang ingin dicapai dengan adanya implementasi algoritma RC4 pada perangkat lunak yang dibangun?

1.3. Batasan Masalah

Dalam Tugas Akhir ini dibahas mengenai metode sistem keamanan pengamanan data hasil pilihan pemilih dan tingkat keamanan dari sistem keamanan tersebut dengan batasan-batasan sebagai berikut :

1. Pada penelitian ini ditekankan pada bagaimana algoritma RC4 digunakan untuk melakukan teknik kriptografi *stream cipher* pada data yang ada pada tabel pilihan pemilih pada basis data perangkat lunak pemilu yang dibangun.
2. Sistem ini melakukan enkripsi terhadap data atau *query* yang ditransmisikan ke database server, dalam hal ini data yang ditransmisikan berupa partai/kandidat calon pilihan pemilih pada saat proses pencoblosan.
3. Sistem ini melakukan dekripsi terhadap data atau *query* hasil enkripsi yang ada pada tabel pilihan pemilih pada saat penghitungan perolehan suara.
4. Sistem ini menggunakan data hasil *merger* antara data random dengan data pilihan pemilih, nilai random yang digunakan dijadikan variabel pengganti *initialization vector* sebelum proses enkripsi dilakukan,
5. Data random dibangkitkan melalui proses *seed random* dengan menggunakan variabel alfanumerik.
6. Sistem ini menggunakan hasil *hash* dari SHA1 untuk kunci (*key*). Kunci ini digunakan setelah proses *merger* data random dengan data pilihan pemilih.

1.4. Tujuan dan Manfaat Penelitian

1.4.1. Tujuan Penelitian

Tujuan yang ingin dicapai penulis dalam penelitian ini adalah membangun sebuah perangkat lunak pemilu berbasis web dengan mengimplementasikan algoritma RC4 untuk keamanan transmisi data dalam jaringan, sehingga data yang ditransmisikan lebih aman dan menyulitkan para hacker dalam melakukan serangan.

1.4.2. Manfaat Penelitian

Manfaat penelitian ini adalah :

1. Dapat memecahkan permasalahan keamanan basis data dalam pemilihan elektronik dengan menggunakan solusi yang ditawarkan penulis, yaitu implementasi algoritma RC4 .
2. Lebih memudahkan pekerjaan dalam menyelenggarakan pemilu atau pemilihan sejenisnya secara lebih optimal berbantu teknologi informasi.
3. Untuk memotivasi dalam melakukan penelitian berikutnya, baik untuk permasalahan serupa (pemilihan elektronik) maupun permasalahan lainnnya dengan berlandaskan ilmu pengetahuan.

1.5. Metode Penelitian

Dalam pengerjaan penelitian ini, digunakan metode penelitian dengan tahapan-tahapan sebagai berikut :

1.5.1. Metode Pengumpulan Data

1. Metode Studi Kepustakaan

   Dengan mengumpulkan dan mempelajari literatur yang berkaitan dengan teori kriptografi dengan RC4 dan pembahasan mengenai masalah pemilihan elektronik.

2. Metode Observasi

   Dengan melakukan pengamatan pada proses pemilihan umum BEM yang diterapkan di Universitas Pendidikan Indonesia.

3. Metode Wawancara

   Untuk mendapatkan variabel-variabel penting serta batasan (*constraint*) dalam sistem, dalam hal ini studi kasus pemilihan Presiden dan Wakil Presiden BEM UPI.

1.5.2. Model Proses Pembangunan Perangkat Lunak

Adalah tahapan-tahapan yang dilakukan dalam rangka pembangunan perangkat lunak, adapun model proses yang digunakan dalam tugas akhir ini adalah *Sequential Linier Model Process.*