BAB I
PENDAHULUAN

1.1. Latar Belakang

Pada sebuah perusahaan, data merupakan sesuatu yang penting dalam kelangsungan proses bisnisnya. Kebijakan atau keputusan suatu perusahaan sering kali didasarkan dari data-data yang telah dikumpulkan dan diolah menjadi informasi. Contoh data-data yang dimaksud adalah data karyawan, data penjualan, data produksi, data konsumen atau pelanggan dan data yang memiliki nilai komersial seperti data yang hanya diberikan kepada konsumen atau pelanggan dari perusahaan tersebut. Melihat pentingnya kedudukan data bagi perusahaan, sudah seharusnya data dipelihara dan disimpan dengan baik dan aman.

Dalam pemeliharaannya banyak proses yang dapat dilakukan, misalnya dengan melakukan pengecekan data yang sudah tidak terpakai dan membuat data cadangan atau *backup* untuk antisipasi dari kehilangan data. Dengan meningkatnya peluang kehilangan data dan kapasitas *memory* penyimpanan yang tidak cukup pada mesin lokal, perusahaan dapat menyimpan data pada *remote server* atau *cloud*. Namun, dengan demikian penyimpanan pada *remote server* akan membuka celah keamanan. Dalam situasi ini, *remote server* yang digunakan harus terpercaya dan tidak memberikan informasi apapun kepada orang-orang yang tidak memiliki hak. Contoh orang yang tidak memiliki hak ialah sistem administrator yang memiliki akses langsung ke dalam *server*. Dimana pemilik data tidak mengetahui tingkat kejujuran administrator (Ucal, 2005).

Untuk memenuhi aspek-aspek keamanan informasi pada sistem penyimpanan *remote server*, diperlukan metode yang dapat melindungi keamanan data. Metode yang dapat dipakai misalnya adalah metode pengamanan pada perangkat infrastruktur yang digunakan dan metode kriptografi. Pada metode kriptografi, pemilik data dapat melakukan enkripsi terlebih dahulu terhadap data yang akan disimpannya. Namun, kendala selanjutnya adalah ketika pemilik data mencari data yang diinginkan pada

server. Pemilik data tidak akan menemukan data tersebut, karena *keywords* yang dikirim kepada *server* masih berbentuk plainteks sedangkan data yang dicari tersimpan dalam bentuk cipherteks. Ada beberapa solusi yang dapat dilakukan untuk permasalahan di atas, salahsatunya adalah dengan mendekripsi terlebih dahulu data yang tersimpan kemudian dicari dengan *keywords* yang diketahui. Namun cara tersebut tidak efissien karena dapat membuat *server* memiliki pekerjaan yang semakin besar. Selain itu, dapat dilakukan juga dengan cara mengunduh semua data yang tersimpan dan kemudian didekripsi satu per satu. Namun cara tersebut juga tidak efektif dan efisien karena akan membutuhakan *bandwith* yang besar dan banyak data yang tidak diinginkan terunduh. Satu cara lain yang dapat dipakai adalah skema *Public-Key Encryption with Keyword Search* (PEKS), PEKS bertujuan untuk tidak memberikan informasi yang dapat dipelajari oleh orang yang tidak berhak ataupun *server*. Dimana setiap data terenkripsi yang disimpan, memiliki beberapa *keywords* yang terenkripsi juga (Boneh dkk., 2004).

Dalam kasus penyimpanan data terpusat sebuah sistem (*cloud*), algoritma kriptografi *stream cipher* lebih cocok dipakai untuk mengenkripsi data yang akan disimpan. Karena algoritma *stream cipher* mengeksekusi bit per bit plainteks menjadi cipherteks (Munir, 2006, hlm. 102), sehingga tidak akan membuat ukuran *file* yang terenkripsi menjadi lebih besar dan memiliki waktu komputasi yang singkat. Dua algoritma kriptografi yang paling sering dipakai adalah RC4 & SEAL. Pada proses enkripsi, algoritma SEAL perlu membangkitkan tiga buah tabel (S *box*) dengan ukuran yang cukup besar terlebih dahulu dari kunci yang diterima. Sehingga SEAL memiliki kekurangan dari waktu yang dibutuhkan ketika awal proses enkripsi dan memerlukan memori yang cukup besar. Sebaliknya, RC4 cukup sederhana dalam pemakaiannya, namun memiliki tingkat keamanan yang mumpuni, kecepatan eksekusi yang tinggi dan efisien dalam penggunaannya (Mooduto & Albar, 2004).

Berdasarkan pengelompokan kunci, algoritma RC4 termasuk kedalam kelompok algoritma kunci-simetri. Dimana kunci yang digunakan baik dalam proses enkripsi maupun dekripsi adalah kunci yang sama. Sedangkan kriptografi

yang menggunakan kunci berbeda dalam enkripsi dan dekripsi adalah kriptografi kunci-asimetri. Memanfaatkan gabungan antara kriptografi kunci-simetri dan kriptografi kunci-asimetri (*hybryd cryptosystem*) akan membuat sistem menjadi lebih efektif. Dimana enkripsi dan dekripsi data menggunakan kriptografi kunci-simetri, sedangkan kunci simetri dienkripsi dan didekripsi dengan kriptografi kunci-asimetri (Munir, 2006, hlm. 178). Manfaat lainnya adalah kriptografi kunci-asimetri tersebut dapat digunakan sebagai protokol otentikasi pengguna yang terdaftar. Sistem menyimpan tabel yang berisi kunci publik semua pengguna, dan setiap pengguna memiliki kunci rahasia yang bersesuaian dengan kunci publiknya (Munir, 2006, hlm. 260).

Dari sekian banyak algoritma kriptografi kunci-asimetri, algoritma yang paling sering adalah algoritma RSA. Meskipun prosesnya cukup sederhana, namun keamanan algoritma ini terjamin. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima (Munir, 2006, hlm.179). Maka dalam penelitian ini, skema PEKS akan dipakai untuk mengamankan data pada sistem. Dimana data akan dienkripsi dengan algoritma RC4 dan algoritma RSA sebagai pengaman kunci algoritma RC4.

1.2. Rumusan Masalah

Poin-poin rumusan masalah yang akan dibahas dalam "pencarian data terenkripsi menggunakan skema PEKS" adalah sebagai berikut :

a. Bagaimana proses enkripsi dan dekripsi data dengan menggunakan algoritma kriptografi RC4 pada skema PEKS?
b. Bagaimana proses pencarian data terenkripsi dengan menggunakan skema PEKS?

1.3. Batasan Masalah

Adapun batasan masalah dalam penelitian ini, diantaranya :

a. Sistem enkripsi dan dekripsi data menggunakan algoritma RC4 dengan *bitlength* 255 bit.
b. Sistem enkripsi dan dekripsi *key* enkripsi algoritma RC4 menggunakan algoritma RSA dengan *bitlength* 1024 bit.

c. Penelitian ini disesuaikan dengan ruang lingkup elearning P.T. USADI Sistemindo Intermatika.

1.4. Tujuan Penelitian

Tujuan penelitian ini adalah untuk membangun suatu sistem dalam pengimplementasian pencarian data terenkripsi menggunakan skema PEKS. Adapun tujuan khusus diantaranya :

a. Mengimplementasikan algoritma RC4 dalam mengenkripsi dan mendekripsi data pada skema PEKS.
b. Membuktikan PEKS sebagai skema yang dapat dipakai untuk pencarian data terenkripsi.

1.5. Sistematika Penulisan

Sistematika penulisan dalam penelitian ini sebagai berikut :

BAB I PENDAHULUAN

Berisi pembahasan masalah secara umum, terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Berisi dasar-dasar teori yang digunakan dalam penelitian ini. Adapun yang dibahas pada bab ini adalah teori yang berkaitan dengan pembangunan sistem pencarian data terenkripsi pada media penyimpanan.

BAB III METODOLOGI PENELITIAN

Bab ini merupakan penjabaran dari pencarian data terenkripsi pada media penyimpanan. Mencakup analisis dan desain model sistem.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini akan dibahas secara mendalam mengenai hal-hal yang dilakukan selama penelitian berlangsung, mulai dari proses pembangunan perangkat lunak, hingga proses pengujian pencarian data terenkripsi yang akan digunakan untuk menjawab apa yang sudah dirumuskan dalam rumusan masalah.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi tentang kesimpulan dari BAB IV dan saran yang diajukan agar dapat menjadi bahan pertimbangan untuk rekomendasi penelitian selanjutnya.