**BAB I**

**PENDAHULUAN**

1. **Latar Belakang**

Basis data saat ini sudah banyak digunakan di berbagai organisasi, perusahaan, ataupun pihak-pihak lain telah memanfaatkan teknologi basis data untuk menyimpan dan mengelola data organisasi atau perusahaannya. Saat ini, keamanan terhadap data yang tersimpan dalam basis data sudah menjadi persyaratan mutlak. Dengan banyaknya serangan-serangan terhadap jaringan komputer yang terhubung dengan basis data maka sudah tidak lagi menjamin keamanan data. Hal tersebut dikarenakan kebocoran data dapat disebabkan oleh berbagai hal, seperti “orang dalam” atau pihak-pihak yang langsung berhubungan dengan basis data seperti administrator basis data (Y. Yohakim Marwanta, 2008). Dengan keadaan seperti tersebut diatas menyebabkan pengguna basis data harus menemukan cara untuk mengamankan data tanpa campur tangan administrator basis data. Kriptografi merupakan salah satu cara yang dapat digunakan untuk mengamankan basis data. Untuk itu, pengguna basis data membutuhkan bantuan keamanan untuk memenuhi kebutuhan keamanan data yang disimpan.

Kriptografi berasal dari dua kata Yunani, yaitu *Crypto* yang berarti rahasia dan *Grapho* yang berarti menulis. Secara umum kriptografi dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu pesan (Y. Yohakim Marwanta, 2008).

Peneitian ini merupakan pengembangan dari penilitian sebelumnya mengenai “Implementasi Enkripsi Basis Data Berbasis Web dengan Algoritma *Steram Cipher* RC4” yang dilakukan oleh Aditya Eka Arifyanto pada distributor sepatu Ramayana Semarang. Penelitian tersebut menggunakan algoritma *stream cipher* RC4 yang panjang kuncinya tidak disebutkan. Hasil dari penelitian ini yaitu basis data berhasil terenkripsi, tetapi hanya mampu mengenkripsi satu kolom saja yang telah ditentukan sebelumnya yaitu kolom password.

Penerapan kriptografi pada Tugas Akhir ini akan ditambahkan pengukuran kecepatan proses enkripsi/dekripsi algoritma RC4. Panjang kunci maksimal yang akan digunakan yaitu 1 sampai 256 *byte*. Pada peneitian kali ini yang akan di enkripsi/dekripsi adalah keseluruhan isi basis data. Penelitian ini akan dilakukan pada Fakultas Ilmu Komputer, Universitas Ichsan Gorontalo.

RC4 merupakan salah satu jenis stream chipher sehingga RC4 memproses unit atau input data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah *byte* atau bahkan kadang-kadang bit (*byte* dalam hal RC4) sehingga dengan cara ini enkripsi atau deskripsi dapat dilaksanakan pada panjang variabel. Algoritma ini tidak harus menunggu sejumlah input data, pesan atau informasi tertentu sebelum diproses, atau menambahkan *byte* tambahan untuk mengenkripsi. RC4 digunakan secara luas pada beberapa aplikasi dan umumnya dinyatakan sangat aman, karena RC4 termasuk dalam algoritma simetris maka kerahasiaan kunci harus dijaga dan dikirim di saluran komunikasi yang aman. Sampai saat ini diketahui tidak ada yang dapat memecahkan atau membongkarnya, hanya saja versi ekspor 40 bitnya dapat dibongkar dengan cara *brute force* (mencoba semua kunci yang mungkin). Dengan teknik ini (*brute force*) Tahun 1995 Damien Doligez menjebolnya menggunakan 120 komputer Unix yang terhubung pada jaringan dalam waktu 8 hari (John Pagik, 2014). Oleh karena itu kekuatan algoritma RC4 terletak pada panjang kunci. Keamanan yang tinggi dan kecepatan dalam memproses data merupakan alasan penulis memilih algoritma *stream cipher* RC4 dalam penelitian kali ini.

Berdasarkan informasi diatas, penulis merancang sebuah sistem yang menggunakan metode enkripsi simetris yang merupakan pengembangan dari sistem sebelumnya dalam aplikasi yang diimplementasikan pada Tugas Akhir dengan judul “**Pengembangan Teknik Kriptografi *Stream Cipher* RC4 Untuk Pengamanan Basis Data”.**

1. **Identifikasi Masalah**

Berdasarkan latar belakang masalah yang telah dikemukakan diatas, masalah dapat di identifikasi sebagai berikut:

1. Adanya ancaman yang serius terhadap basis data yang saat ini banyak digunakan organisasi atau perusahaan untuk menyimpan dan mengelola informasi organisasi atau perusahaannya.
2. Sering terjadinya kebocoran data yang dapat disebabkan oleh banyak hal, seperti “orang dalam” dan pihak-pihak yang berhubungan langsung dengan basis data, seperti administrator basis data (Y. Yohakim Marwanta, 2008).
3. Pada penelitian sebelumnya hanya mengenkripsi satu kolom saja yaitu kolom password, sedangkan isi basis data lainnya tidak dienkripsi.
4. **Rumusan Masalah**

Berdasarkan latar belakang dan identifikasi masalah diatas, dapat diambil rumusan masalah sebagai berikut:

1. Bagaimana cara mengimplementasikan algoritma kriptografi simertis *stream cipher* RC4 pada sebuah sistem enkripsi basis data.?
2. Bagaimana pengaruh panjang kunci dan panjang data terhadap kecepatan dan keamanan proses enkripsi/dekripsi algoritma RC4.?
3. Bagaimana mengenkripsi keseluruhan isi basis data.?
4. **Tujuan Penelitian**

Tujuan penelitian ini adalah sebagai berikut:

1. Untuk membuat pengembangan sistem keamanan aplikasi program dengan menggunakan enkripsi yang lebih baik.
2. Mengimplementasikan teknik kriptografi *stream cipher* RC4 kedalam sebuah aplikasi sistem.
3. **Manfaat Penelitian**

Adapun manfaat penelitian ini adalah sebagai berikut:

1. Pengembangan iptek

Penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan ilmu pengetahuan dan teknologi khususya untuk penerapan algoritma kriptografi simetris *stream cipher* rc4.

1. Praktisi

Hasil penelitian dapat digunakan organisasi, perusahaan, atau pengguna basis data lainnya dalam menambah integritas basis data dari ancaman serangan yang sering terjadi di jaringan komputer.

1. Peneliti

Dengan penelitian ini diharapkan dapat menjadi referensi dalam pengembangan keamanan jaringan khususnya kriptografi bagi peneliti selanjutnya yang tertarik untuk meneliti tentang Implementasi teknik kriptografi *stream cipher* rc4 untuk pengamanan basis data.