Bab 1

Pendahuluan

1.1 Latar Belakang

Ketika penggunaan media *wireless* sebagai sarana komunikasi telah merambah ke berbagai segi kehidupan masyarakat saat ini, maka sejalan dengan itu juga ada beberapa masalah keamanan yang harus diperhatikan. Saat ini, pasar teknologi *wireless* LAN sedang tumbuh dan mengalami perkembangan yang pesat, namun dibalik semua perkembangan itu juga terdapat '*big black hole*' terhadap tingkat keamanan dari jaringan ini.

Standar *wireless* LAN yang ditawarkan saat ini memang sangat tidak memuaskan jika diperhatikan dari segi keamanannya, masih ada produk tanpa fungsi *security* apapun. Bahkan, IEEE 802.11 menspesifikasikan fungsi *security* sebagai feature yang optional. Sehingga tidak dapat mempercayakan seluruh aktifitas komunikasi dengan menggunakan produk dengan standar ini, maka hal yang harus diperhatikan adalah keamanannya.

Mengacu pada konsep diatas maka simulasi algoritma WEP (*Wired Equivalent Privacy*) dan AES (*Advance Encryption Standard*) diharapkan akan sangat membantu untuk mengetahui kelebihan dan kekurangan dari masing-masing algoritma yang digunakan pada *wireless* LAN. Pada simulasi ini aplikasi dilakukan sesuai dengan kondisi pada WLAN yaitu terdapat aplikasi *client* dan *server*. Pada aplikasi client akan ditampilkan setiap user yang terdapat dalam komunikasi dalam jaringan, penampilan HEX mode, benchmark *encryption*, *encryption debugging* (yang akan menampilkan proses dari algoritma), button *ReConnect* yang digunakan untuk memutuskan komunikasi pada jaringan dan button Send yang digunakan untuk mengirimkan pesan yang diketikkan

pada form. Sedangkan pada aplikasi *server* akan ditampilkan Connection *client* yang dapat menampilkan user ID dan alamat IP dari *client* yang melakukan komunikasi dalam jaringan dan *Activity Log* yang menampilkan hubungan komunikasi antara *client* yang melakukan komunikasi pada jaringan.

1.2 Tujuan dan Kegunaan

1.2.1 Tujuan

Tujuan dari penelitian ini adalah:

1. Melakukan uji implementasi *software* aplikasi *Client Server* pada WLAN
2. Menguji performansi dari algoritma WLAN (WEP dan AES) dengan parameter performansinya berupa:
   (a) Perbandingan komparisasi kecepatan
   (b) Perbandingan *Avallance Effect*
   (c) Perhitungan pola simpangan dari *ciphertext* yang diperoleh dari implementasi aplikasi *client server* dengan menggunakan kedua algoritma tersebut.
3. Pengujian kunci pada algoritma WEP dan AES

1.2.2 Kegunaan

Penelitian yang berdasarkan simulasi ini diharapkan dapat memberikan kontribusi positif di bidang *secure communication*. Terutama peningkatan keamanan komunikasi data pada pengguna jaringan WLAN dalam hal pemilihan algoritma yang digunakan pada kominikasi data yang dilakukan.

1.3 Perumusan Masalah

Keamanan lalu lintas data pada jaringan *wireless* LAN sangat rentan terhadap serangan yang dilakukan oleh pihak-pihak yang bermaksud mengganggu confidentialitas, integritas dan ketersediaan jaringan *wireless* LAN. Untuk itulah dilakukan pengujian dengan

menggunakan metode enkripsi WEP dan AES untuk mengetahui dan menganalis seberapa besar tingkat keamanan dari masing-masing algoritma tersebut sekaligus mencari kelebihan dan kekurangan dari algoritma enkripsi WEP dan AES.

1.4 Batasan Masalah

Batasan-batasan yang digunakan dalam pengerjaan tugas akhir ini adalah:

1. Pengujian yang dilakukan pada Tugas Akhir ini mencakup standarisasi WLAN 802.11 dengan pembahasan securitas berdasarkan performansi algoritma WEP dan AES.
2. Pengujian perangkat WLAN 802.11 tidak dibahas disini.
3. Semua peserta yang ada pada aplikasi *Client Server* diasumsikan sudah saling mengenal dan orang terpercaya serta sudah memberikan data *key* dan ID kepada *Server*.
4. Masalah keamanan yang berhubungan dengan penggunaan gelombang radio tidak dibahas disini.
5. Pengujian yang dilakukan dengan membuat simulasi algoritma enkripsi WEP dan AES
6. Program dibuat dengan memanfaatkan bahasa pemograman Delphi
7. Uji analisis untuk metoda enkripsi WEP dan AES 128 bit

1.5 Metode Penelitian

Metodologi yang ditempuh dalam Tugas Akhir ini berupa metoda kuantitatif dan kualitatif yang meliputi berbagai aktifitas sebagai berikut:

1. Studi Literatur. Pencarian dan pengumpulan literatur-literatur serta kajian-kajian yang berkaitan dengan masalah yang ada pada Tugas Akhir ini, baik berupa jurnal, artikel, buku referensi, internet, dan sumber-sumber lain yang berhubungan dengan masalah kriptografi WEP dan AES.

2. Analisa Masalah Dengan menganalisa semua permasalahan yang ada berdasarkan sumber yang ada dan pengamatan terhadap masalah tersebut.
3. Desain dan Implementasi Sistem Yaitu membuat rancangan dan prediksi dengan menggunakan komponen yang ada serta dapat merealisasikan sistem tersebut secara keseluruhan dalam simulasi *software*.
4. Evaluasi dan uji coba sistem

Setelah direalisasikan berdasarkan rancangan yang ada, kemudian tahap selanjutnya adalah melakukan uji coba untuk melihat kerja sistem tersebut serta melakukan evaluasi dan perbaikan sistem.

1.6 Sistematika Penulisan

Dalam penyusunan Tugas Akhir ini di susun sebagai berikut:

BAB I PENDAHULUAN Bab ini membahas latar belakang masalah, maksud dan tujuan, batasan masalah, metoda penelitan, dan sistematika penulisan yang digunakan dalam penulisan Tugas Akhir ini.

BAB II LANDASAN TEORI Berisi tinjauan teoritis *Crypthography* meliputi terminologi algoritma dan kunci simetris dari WEP dan AES, dan serangan attack yang mungkin terjadi.

BAB III PERANCANGAN DAN IMPLEMENTASI ALGORITMA WEP DAN AE
Bab ini berisi uraian mengenai perancangan sistem kriptografi WEP dan AES yang meliputi pembuatan aplikasi *Client Server*, pembuatan kanal pengujian performansi algoritma WEP dan AES, pembuatan animasi algoritma AES, dan pembuatan kanal pengujian kunci dari kedua algoritma tersebut.

BAB IV HASIL PERANCANGAN DAN ANALISA Bab ini membahas tentang pengujian sistem dan hasil yang diperolehnya, kemudian dianalisa apakah sesuai dengan keluaran yang diinginkan.

BAB V PENUTUP Berisi kesimpulan dari hasil pengujian dan saran bagi pengembangan selanjutnya.