Segala perkara dapat kutanggung

di dalam Dia yang memberi kekuatan

kepadaku (Filipi 4:13)

kekuatan dan kesanggupan yang diberikan oleh TUHAN melebihi setiap masalah yang ada,

bahkan menjadikanku semakin serupa dengan keinginan-NYA,

sehingga apapun yang kulakukan dibuat-NYA berhasil

melebihi dari keberhasilan seorang pemenang

Ku persembahkan buat keluargaku tercinta

Bapak, Mamak, dan adik-adik ku, dan smua keluarga yang mendukung

God bless My family ☺

ABSTRAK

Masalah keamanan dan kerahasiaan data merupakan aspek penting dalam komunikasi data, terutama pada jaringan wireless lan. Hampir rata-rata manusia sekarang mengetahui apa itu wireless lan. Seperti diketahui komunikasi data pada wireless lan ini menggunakan gelombang radio, oleh sebab itu banyak orang ingin mengeksplorasi pengetahuannya untuk melakukan serangan. Salah satu cara untuk menjaga keamanan dan kerahasiaan data tersebut adalah dengan menggunakan teknik penyandian yang disebut dengan kriptografi. Oleh karena itu, pada Tugas Akhir ini penulis membuat aplikasi layaknya wireless lan yang mana terdapat pengirim dan penerima.

Sistem aplikasi pada Tugas Akhir ini mencakup standarisasi wireless lan yang mencakup WEP, WPA, WPA2. Untuk WEP menggunakan algoritma RC4 standarisasi 64 bit, WPA menggunakan RC4 standarisasi 128 bit, dan untuk WPA2 menggunakan algoritma AES mode CBC standarisasi 256 bit. Pada aplikasi penulis membuat variansi panjang kunci menjadi 256 bit dan 1024 bit pada WEP dan WPA untuk menambah tingkat keamanan protokol WEP dan WPA, itu dikarenakan berdasarkan konsep jika semakin panjang kuncinya maka waktu proses enkripsi dan dekripsi serta waktu bongkar brute force akan semakin lama

Dari hasil pengukuran performansi terhadap waktu proses enkripsi dan dekripsi menyatakan semakin panjang bit nya maka waktu proses enkripsi dan dekripsi semakin lama, berdasarkan perhitungan waktu bongkar brute force menyatakan semakin panjang bit kunci mengakibatkan waktu untuk melakukan brute force semakin lama, begitu juga dengan perhitungan IV, semakin panjang IV nya maka akan semakin lama proses perulangan IV, sehingga jelas bahwa WPA lebih tangguh daripada WEP, namun walaupun WPA menggunakan 48 bit IV masih saja memungkinkan terjadi korelasi perulangan, sehingga WPA2 yang menggunakan AES jauh lebih tangguh daripada WEP dan WPA walaupun menggunakan 16 bit IV, itu dikarenakan proses schedulingnya jauh lebih rumit sehingga mempersulit cryptanalist dalam melakukan serangan.

Kata kunci : WEP, WPA, WPA2, AES, RC4, CBC, IV