

Abstrak

Kehadiran teknologi *wireless* di tengah perkembangan teknologi telekomunikasi mendapat perhatian besar dari para operator dunia. Pada mulanya teknologi ini hanya menjadi elementer disamping jaringan tembaga, tetapi karakteristik *wireless* yang fleksibel menjadikannya sebagai salah satu teknologi utama yang diaplikasikan dalam jaringan telekomunikasi. Kondisi ini menciptakan peluang besar bagi para *vendor* dan *supplier* untuk membangun industri *wireless* dalam skala besar. *Wireless Local Area Network* merupakan aplikasi pengembangan *wireless* untuk komunikasi data, Sesuai dengan namanya *wireless* yang artinya tanpa kabel. WLAN adalah jaringan lokal (dalam satu daerah perasi gedung, ruang, kantor, dan sebagainya namun bukan antar kota) yang tidak menggunakan kabel. Standar IEEE 802.11b dan 802.11i menyebutkan metoda *kriptografi* yang digunakan pada jaringan WLAN adalah algoritma WEP(RC4) dan algoritma AES sebagai optional sekuritas. Dalam tugas akhir ini dibahas mengenai desain untuk membangun *software* simulasi sistem *client server* yang dapat diimplementasi pada jaringan WLAN yang berbentuk kanal aplikasi untuk melakukan komunikasi data dengan masukan berupa karakter ASCII atau hex. Kanal aplikasi *Client Server* ini mirip kanal *chatting*, dan membangun *software* simulasi untuk analisa tingkat sekuritas dan performansi algoritma WEP dan AES seperti *avallanche Effect*, perubahan *plaintext* dan *ciphertext*, komparisasi kecepatan *enkripsi* dan *dekripsi*, pencarian kunci lemah dari WEP dan AES, pencarian kunci setengah lemah dari WEP dan AES. Desain dilakukan dengan menggunakan metoda analisis terstruktur yang dituangkan dalam prosedur simulasi. Dari pengujian diperoleh kesimpulan bahwa algoritma AES memiliki kemampuan yang lebih baik daripada RC4 untuk digunakan pada keamanan data dari komunikasi Wireless LAN. Hal ini dapat dilihat dari perolehan data dengan parameter *avallanche effect* untuk algoritma WEP (RC4) sebesar: 49,92 dan untuk AES:50,00%, perubahan *Plaintext* terhadap *Ciphertext* dengan perolehan perbedaan bit sebesar: 41,41% untuk algoritma WEP (RC4) dan AES:49.97%. sedangkan untuk parameter kunci algoritma AES tidak memiliki *Semi Weak Key* dan *Weak Key*.