

Daftar Isi

1	Pendahuluan	1
1.1	Latar Belakang	1
1.2	Tujuan dan Kegunaan	2
1.2.1	Tujuan	2
1.2.2	Kegunaan	2
1.3	Perumusan Masalah	2
1.4	Batasan Masalah	3
1.5	Metode Penelitian	3
1.6	Sistematika Penulisan	4
2	Dasar Teori	5
2.1	Konfigurasi Jaringan WLAN	5
2.1.1	Ad Hoc WLAN	5
2.1.2	Infrastruktur WLAN	6
2.2	Keamanan dan Kriptografi	6
2.3	Kriptografi	7
2.4	Algoritma Kriptografi	8
2.4.1	WEP	9
2.4.2	Advance Encryption Standard (AES)	10
3	Perancangan dan Implementasi Algoritma WEP dan AES	14
3.1	Pemodelan Simulasi untuk Analisa	14
3.1.1	<i>Avallanche Effect</i>	14
3.1.2	Perubahan <i>Plaintext</i> dan <i>Ciphertext</i>	16
3.1.3	Komparisasi Kecepatan Enkripsi dan Deskripsi	17
3.1.4	Pencarian <i>Weak Key</i> dari WEP dan AES	18

3.1.5	Pencarian <i>Semi Weak Key</i> dari WEP dan AES	21
3.2	Implementasi Sistem	23
3.2.1	Spesifikasi Perangkat Sistem	23
3.3	Proses Komunikasi dalam Sistem	24
3.4	Pemodelan Simulasi <i>Client Server</i> pada WLAN	24
3.4.1	Disisi <i>Client</i>	24
3.4.2	Di sisi <i>Server</i>	25
3.5	Mekanisme Software Aplikasi	26
4	Hasil Perancangan dan Analisa	28
4.1	Pengujian Fungsional Sistem pada Aplikasi <i>Client Server</i>	29
4.2	Analisa Proses Enkripsi dan Dekripsi RC4	29
4.2.1	Proses Enkripsi algoritma WEP (RC4)	32
4.2.2	Proses Dekripsi pada Algoritma RC4	33
4.3	Proses Enkripsi dan Dekripsi pada AES	34
4.3.1	Proses Enkripsi pada AES	34
4.3.2	Proses <i>Hashing Key</i> pada AES	38
4.3.3	Proses Dekripsi pada Algoritma AES	39
4.4	Analisa hasil Simulasi Performansi Algoritma WEP dan AES	41
4.4.1	<i>Avallanche Effect</i>	41
4.4.2	Perubahan <i>plaintext</i> terhadap <i>ciphertext</i> pada RC4	45
4.4.3	Perubahan <i>plaintext</i> terhadap <i>ciphertext</i> pada AES	48
4.5	<i>Weak Key</i> dan <i>Semi Weak Key</i>	51
4.5.1	Analisa <i>Weak Key</i> dan <i>Semi Weak Key</i> pada RC4	51
4.5.2	Analisa <i>Weak Key</i> dan <i>Semi Weak Key</i> pada AES	52
4.5.3	Analisa Simulasi Komparisasi Kecepatan Proses Enkripsi dan Dekripsi	52
5	Penutup	54
5.1	Kesimpulan	54
5.2	Saran	55