BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan analisis dan kajian yang telah dilakukan dapat diambil kesimpulan sebagai berikut :

1. Pada WPA-PSK enkripsi data menggunakan algoritma RC4 dan pada WPA2-PSK menggunakan algoritma AES.
2. Authentikasi atau pencocokan identitas menggunakan PSK (*Pre Shared Key*), yaitu penggunaan kunci yang sama antara *access point* dan *client.*
3. Penerapan WPA-PSK dan WPA2-PSK pada WLAN berpengaruh kepada format data WLAN. Besar data WLAN bertambah sebesar 4 *byte* untuk WPA-PSK dan bertambah 14 *byte* untuk WPA2-PSK.
4. Pada pengujian enkripsi data WPA-PSK yang menggunakan RC4 dan WPA2-PSK yang menggunakan AES mengakibatkan ukuran data hasil enkripsi bertambah. Besar data awal 1558 *byte* berubah menjadi 1562 *byte* pada WPA-PSK, dan berubah menjadi 1572 *byte* pada WPA2-PSK .
5. Penerapan WPA-PSK dan WPA2-PSK mempengaruhi *delay time. Delay time* sebelum penerapan WPA-PSK dan WPA2-PSK sebesar 9,068 ms. Setelah penerapan WPA-PSK *delay time* secara rata-rata menjadi 9,587 ms, dan setelah penerapan WPA2-PSK *delay time* secara rata-rata menjadi 10,158 ms.
6. Penerapan WPA-PSK dan WPA2-PSK juga mempengaruhi throughput WLAN. *Throughput* sebelum penerapan WPA-PSK dan WPA2-PSK sebesar 1390606 bps. *Throughput* secara rata-rata menjadi 1313064 bps pada WPA-PSK, dan menjadi 1252515 bps pada WPA2-PSK.

5.2 Saran

1. Metode keamanan WPA-PSK dan WPA2-PSK pada WLAN masih bisa ditingkatkan keamanannya menggunakan WPA-RADIUS dan WPA2-RADIUS.

2. Dalam analisisnya adalah hasil simulasi WPA-PSK dan WPA2-PSK yang tidak berjalan secara *real time*. Simulasi ini dapat disempurnakan sehingga bisa berjalan secara *real time*.