

BAB III METODOLOGI

3.1 Umum

Pembahasan dalam skripsi ini untuk mengetahui penerapan WPA menggunakan enkripsi RC4 dan WPA2 yang menggunakan enkripsi AES, serta penerapan mode autentikasi PSK (*Pre Shared Key*) pada jaringan WLAN. Metodologi yang digunakan dalam skripsi ini adalah sebagai berikut :

1. Studi Literatur.
2. Pembuatan program simulasi.
3. Pemodelan WPA-PSK dan WPA2-PSK pada jaringan WLAN.
4. Pengujian enkripsi dan autentikasi pada WPA-PSK dan WPA2-PSK.
5. Perhitungan *delay time* dan *throughput*.
6. Analisis hasil perhitungan.

3.2 Metode Pengambilan Data

Data-data yang digunakan dalam skripsi ini berupa data sekunder dan data primer. Data sekunder yaitu data yang diperoleh dari buku referensi, jurnal, skripsi, badan standar telekomunikasi internasional dan internet. Data primer adalah data yang diambil dari hasil perhitungan.

3.2.1 Data Sekunder

Data-data sekunder yang digunakan pada skripsi ini adalah berupa studi literatur mengenai :

1. Proses pengiriman data pada jaringan *wireless* menggunakan standar IEEE 802.11b.
2. Proses enkripsi menggunakan algoritma RC4 (*Rivest Code 4*) dan algoritma AES (*Advanced Encryption Standard*).
3. Proses autentikasi menggunakan PSK (*Pre Shared Key*).
4. Perhitungan *delay* dan *throughput* pada *Wireless LAN*.

3.2.2 Data Primer

Sedangkan data-data primer yang digunakan pada skripsi ini adalah :

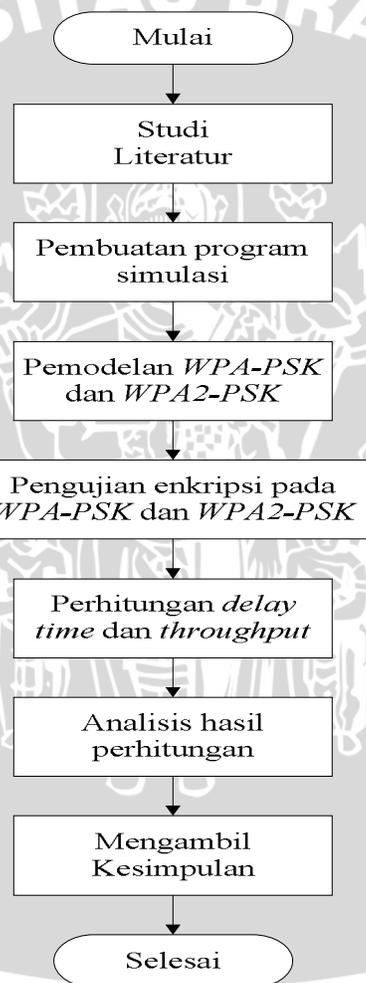
1. Perhitungan *delay* enkripsi menggunakan program simulasi.

Delay enkripsi adalah waktu yang dibutuhkan untuk mengenkripsi data. Pada simulasi enkripsi akan dilengkapi pewaktu (*timer*) sehingga dapat diketahui waktu yang dibutuhkan untuk enkripsi data.

2. Perhitungan *throughput* menggunakan rumus.

Throughput adalah jumlah total *byte* yang diterima di sisi penerima dengan baik. Setelah mengetahui besarnya *delay time*, maka besarnya *throughput* bisa dihitung.

3.3 Diagram Metodologi Penelitian



Gambar 3.1 Diagram Metodologi Penelitian

(Sumber : Perencanaan)

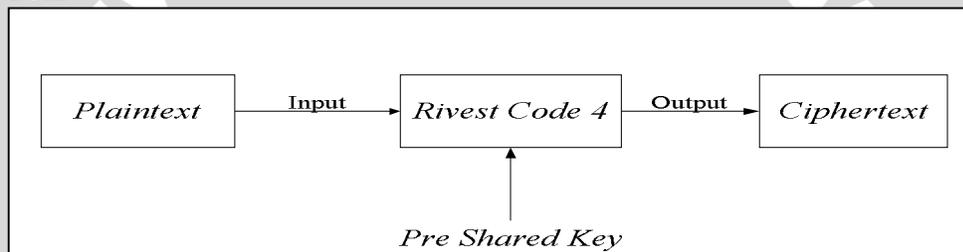
3.4 Metode Analisis Data

Metode analisis data yang dilakukan adalah pengumpulan beberapa data sekunder untuk kemudian dianalisis sesuai pembahasan, yang meliputi :

1.4.1 Proses enkripsi dan autentikasi pada WPA-PSK dan WPA2-PSK.

Proses enkripsi menggunakan algoritma RC4 untuk WPA dan menggunakan algoritma AES untuk WPA2. Kedua jenis enkripsi ini digabungkan dengan mode autentikasi menggunakan PSK. Sehingga terdapat dua program simulasi yaitu simulasi WPA-PSK dan WPA2-PSK.

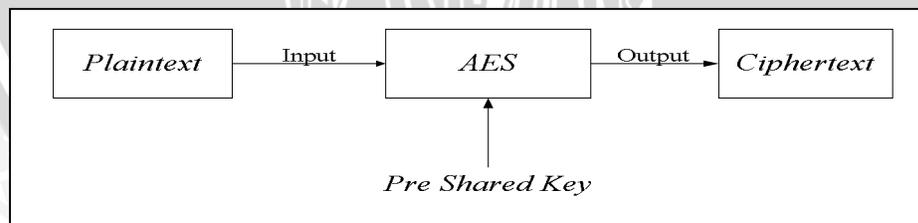
1.4.2 Blok diagram proses enkripsi dan autentikasi pada WPA-PSK dan WPA2-PSK



Gambar 3.2 Proses enkripsi pada WPA-PSK

(Sumber : Pemodelan)

Proses enkripsi WPA-PSK berupa *input* dalam bentuk teks tidak teracak (*plaintext*) yang dienkripsi menggunakan algoritma *Rivest Code 4* menghasilkan *output* berupa teks teracak (*ciphertext*). Proses enkripsi WPA-PSK ditunjukkan pada gambar 3.2.



Gambar 3.3 Proses enkripsi pada WPA2-PSK

(Sumber : Pemodelan)

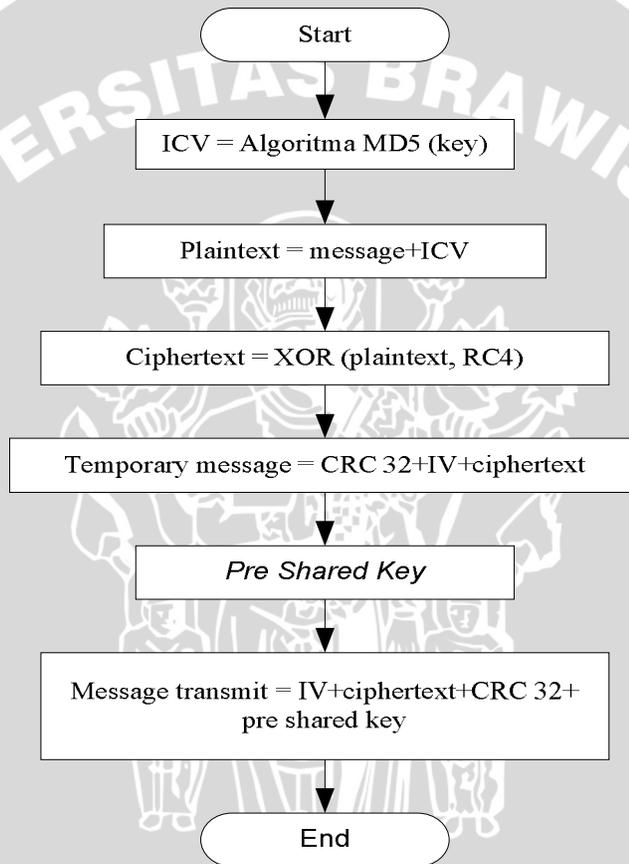
Proses enkripsi WPA2-PSK berupa *input* dalam bentuk teks tidak teracak (*plaintext*) yang dienkripsi menggunakan algoritma *Advanced Encryption*

Standard menghasilkan *output* berupa teks teracak (*ciphertext*). Proses enkripsi WPA2-PSK ditunjukkan pada gambar 3.3.

1.4.3 Pemodelan WPA-PSK dan WPA2-PSK pada WLAN.

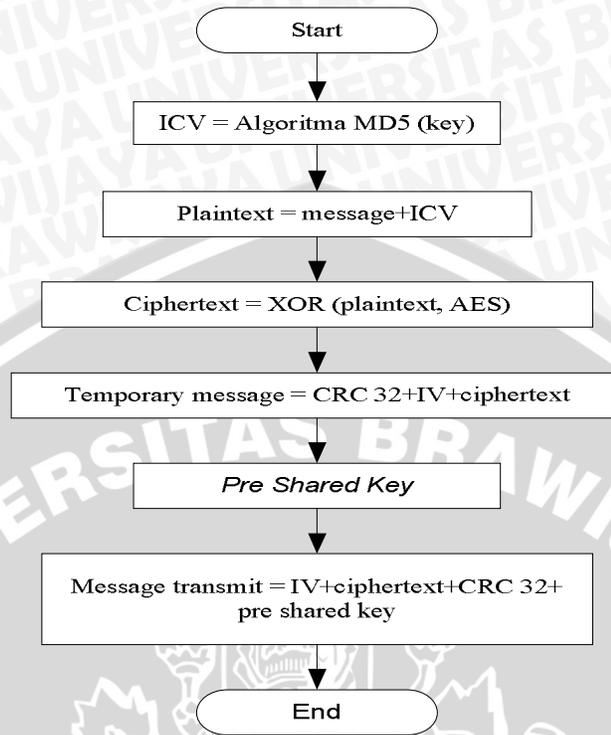
Setelah program simulasi WPA-PSK dan WPA2-PSK selesai. Selanjutnya kedua program tersebut dimodelkan pada jaringan WLAN.

1.4.3.1 Diagram alir pemodelan WPA-PSK pada jaringan WLAN.



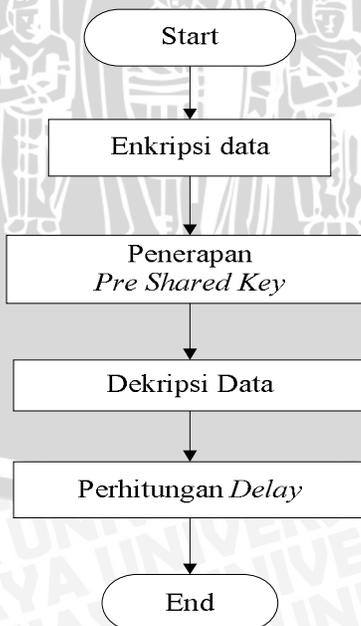
Gambar 3.4 Diagram alir program simulasi WPA-PSK
(Sumber : Pemodelan)

1.4.3.2 Diagram alir pemodelan WPA2-PSK pada jaringan WLAN.



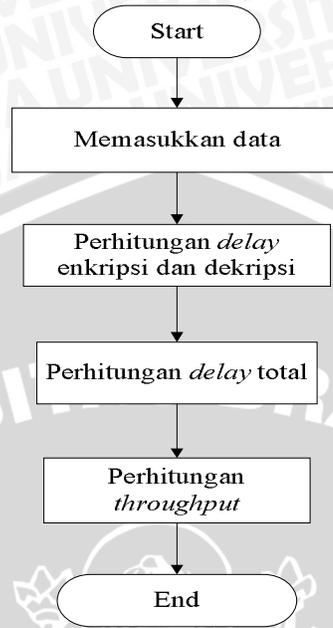
Gambar 3.5 Diagram alir program simulasi WPA2-PSK
(Sumber : Pemodelan)

1.4.4 Diagram alir pengujian WPA-PSK dan WPA2-PSK pada WLAN



Gambar 3.6 Diagram alir pengujian WPA-PSK pada Wireless LAN.
(Sumber : Pemodelan)

1.4.5 Diagram analisis pengaruh penerapan WPA-PSK dan WPA2-PSK terhadap *delay time* dan *throughput*.



Gambar 3.7 Diagram analisis pengaruh penggunaan WPA-PSK dan WPA2-PSK terhadap *delay time* dan *throughput* (Sumber : Pemodelan)