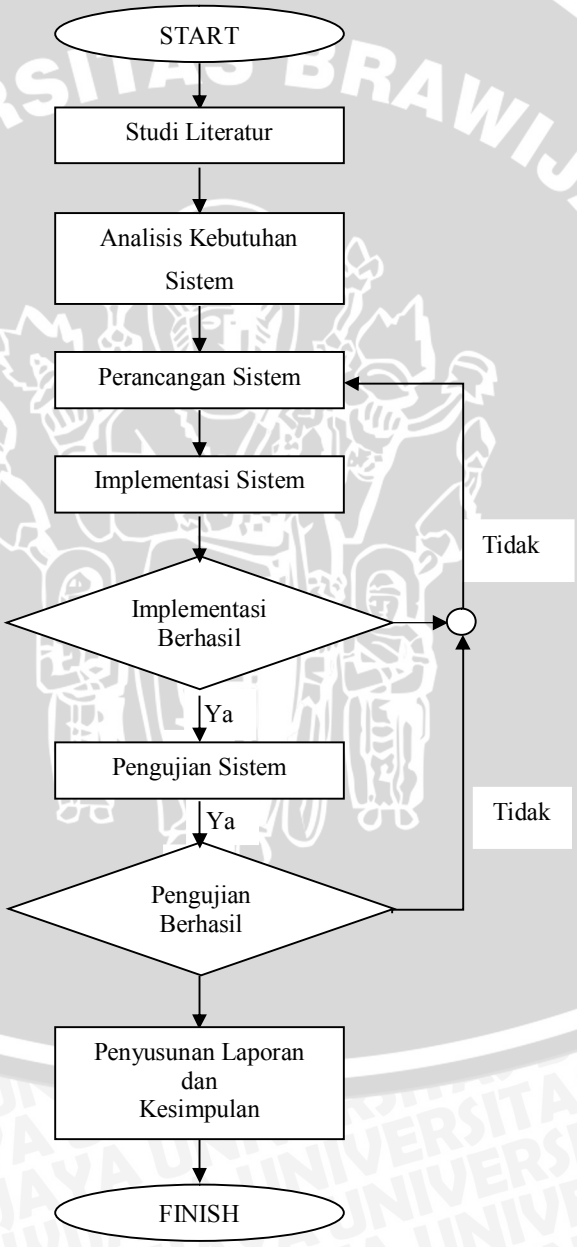
BAB III
METODOLOGI

Bab metodologi penelitian membahas langkah-langkah dalam merancang aplikasi transfer file menggunakan algoritma AES 128 bit dan RC4 128 bit dan dijelaskan langkah-langkah implementasi, analisis, dan pengujian sistem yang dirancang.



Gambar 3.1 Flowchart Metodologi Penelitian

3.1 Studi Literatur

Studi literature menjelaskan tentang dasar teori yang mendukung dalam implementasi dan analisis aplikasi transfer file menggunakan algoritma AES 128 bit dan RC4 128 bit. Teori-teori pendukung tersebut antara lain :

1. Jaringan Komputer
   - 1.1 Model Hubungan Pada Jaringan
     - 1.1.1 Jaringan *Peer to Peer*
     - 1.1.2 *Client-Server*
2. Protokol TCP/IP
   - 2.1 IP *Address*
3. Komunikasi Data
4. Algoritma Kriptografi
   - 4.1 Algoritma Enkripsi *Rivest Cipher* 4 (RC4)
     - 4.1.1 Transformasi RC4
     - 4.1.2 Langkah-langkah RC4
   - 4.2 Algoritma Enkripsi *Advanced Encryption Standart* (AES)
     - 4.2.1 Transformasi AES
     - 4.2.2 Langkah-langkah AES
5. QoS (*Quality of Services)*
   - 5.1 *Availability*
   - 5.2 *Jitter*
   - 5.3 *Troughput*
   - 5.4 *Packet Loss*
   - 5.5 *Delay*
     - 5.5.1 *Delay* Enkripsi
     - 5.5.2 *Delay* Dekripsi
     - 5.5.3 *Delay* Propagasi
     - 5.5.4 *Delay* Proses
     - 5.5.5 *Delay* Transmisi
     - 5.5.6 *Delay* Antrian
   - 5.6 *Mean Opinion Score* (MOS)
   - 5.7 *Estimate E-Mode*

3.2 Analisis Kebutuhan

Analisis kebutuhan bertujuan untuk mendapatkan semua kebutuhan dari sistem aplikasi *transfer file* menggunakan algoritma AES 128 bit dan RC4 128 bit. Pada analisis kebutuhan tindakan yang dilakukan adalah mengidentifikasi perangkat lunak, perangkat keras serta topologi yang digunakan dalam perancangan, implementasi dan analisis sistem yang akan dibuat. Dengan demikian diharapkan dapat mempermudah dalam mendesain sistem dan hasil analisis terhadap sistem yang dibuat dapat lebih akurat.

3.2.1 Perangkat Keras yang Digunakan

Sistem aplikasi ini dibuat dengan menggunakan 2 buah laptop dengan spesifikasi pada table 3.1.

Tabel 3.1 Spesifikasi Perangkat Keras

Spesifikasi	ASUS	SONY
Prosesor	CORE i3	AMD E-450
Installed Memory (RAM)	2 GB	2 GB
System Type	64-bit Operating System	32- bit Operating System

3.2.2 Perangkat Lunak yang Digunakan

Untuk membangun sebuah program aplikasi ini dibutuhkan perangkat lunak yang dijelaskan pada table 3.2.

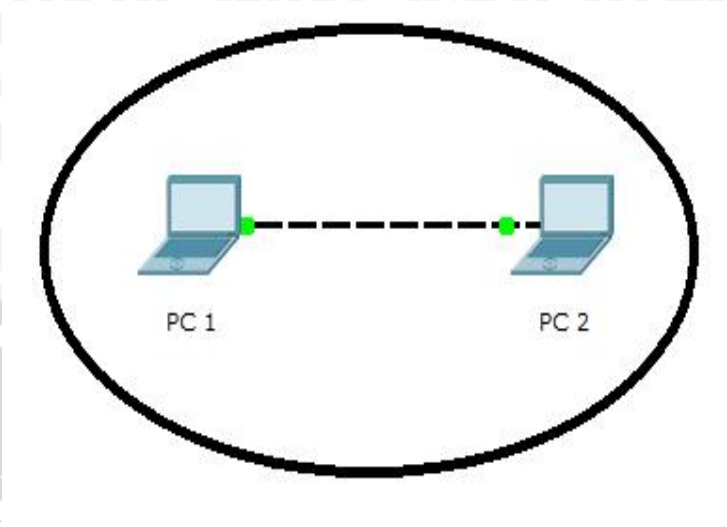
Tabel 3.2 Spesifikasi Perangkat Lunak

No	Jenis Kebutuhan	Software
1	Sistem operasi	Microsoft Windows
2	Bahasa pemrograman	Visual C# 2010
3	Aplikasi Tambahan	.Net Framework 4.0
4	Network Analyzer	Wireshark 1.84

3.3 Perancangan

Perancangan dilakukan setelah didapatkan seluruh kebutuhan sistem yang didapat pada analisis kebutuhan. Dalam pembuatan sistem ini fokus perancangan adalah menggunakan jaringan *Ad-hoc* dengan protokol TCP/IP.

Topologi Ad-Hoc pada perancangan program ini dapat dilihat pada gambar 3.2 berikut ini.



Gambar 3.2 Topologi *Ad-Hoc*

Perancangan aplikasi ini menggunakan jaringan *ad-hoc*, dikarenakan mode ini selalu bergerak (*mobility*) sehingga dapat mengakses informasi secara *real time* ketika berhubungan dengan mobile node lain, sehingga pertukaran data dan pengambilan keputusan dapat segera dilaksanakan.

Dalam bab perancangan akan dijelaskan lebih lanjut tugas serta spesifikasi masing-masing, dengan demikian akan mempermudahkan konfigurasi masing-masing PC pada tahap implementasi. Bandwidth rata-rata pada Ad Hoc adalah 54 MBit/s.

3.4 Implementasi

Implementasi dilakukan mengacu pada topologi dalam perancangan. Pada tahap ini ada beberapa langkah yang harus dilakukan antara lain :

3.4.1 Instalasi dan Konfigurasi Perangkat Keras

Instalasi dan konfigurasi perangkat keras yang dilakukan adalah dengan menghubungan antara PC yang satu dengan lainnya menggunakan jaringan *Ad-Hoc,* yaitu dengan mengkoneksikan PC dengan SSID yang telah dibuat. Pengujian dilakukan terhadap 2 jenis PC yang berbeda, yaitu PC pengirim menggunakan

ASSUS dengan prosessor core i3 dan PC penerima adalah VAIO dengan prosessor AMD E-450**.**

3.4.2 Instalasi dan Konfigurasi Perangkat Lunak

Aplikasi ini menggunakan bahasa C# 2010 dan Wireshark 1.84 sebagai analisis paket datanya. Pada bagian ini ada beberapa konfigurasi yang dilakukan, anatara lain menginstal .Net Framework 4.0 dan wireshark pada PC penerima.

Mengimplementasikan algoritma RC4 128 bit, AES 128 bit, penerima dan pengirim pada program aplikasi.

3.5 Pengujian dan Analisis

Pada tahap pengujian dan analisis dilakukan pengujian terhadap sistem apakah program dapat digunakan untuk mentransfer file serta menganalisis parameter *throughput* dan *delay*.

Throughput dan *delay* saling berhubungan, karena ketika suatu sistem atau jaringan tidak mencukupi *throughput*, maka paket data akan mengalami waktu tunda (*delay)*. Jadi, semakin tinggi nilai *throughput*, semakin kecil nilai *delay*nya.

Delay yang dianalisis adalah *delay* enkripsi dan *delay* dekripsi, *delay* transmisi serta *delay* total.

3.5.1 Pengujian

Pengujian yang dilakukan yaitu pengujian untuk menjalankan program pada penerima, antara lain :

1. Pengujian dilakukan dengan menggunakan konfigurasi *ad-hoc.*
2. Memasukkan *port (default* 8071*)*dan IP penerima akan otomatis terisi.

Pengujian yang dilakukan yaitu pengujian pengiriman data, antara lain:

1. Pengujian dilakukan dengan menghubungkan PC dengan SSID yang telah dibuat.
2. Masukkan IP dan *port* yang sesuai dengan penerima, sedangkan jenis enkripsi dan *password* ditentukan oleh pengirim.

3. Pengujian dilakukan terhadap semua jenis file dengan ukuran maksimal 100 MB.
4. Data yang dikirimkan berupa *chipertext,* dan ketika diterima oleh penerima sudah dalam bentuk *plaintext.*

3.5.2 Analisis Hasil Pengujian

Analisis hasil pengujian dilakukan ketika proses transfer *file* berlangsung. Parameter yang akan dianalisis yaitu *throughput* dan *delay* dari algoritma AES 128 bit dan algoritma RC4 128 bit menggunakan *wireshark* 1.84. Paket data yang akan dianalisis terlebih dahulu di *filter* berdasarkan *port,* agar dapat mengetahui nilai *throughput* dan *delay* yang aktual pada saat proses pengiriman *file.*

3.6 Penarikan Kesimpulan

Pengambilan kesimpulan dilakukan setelah perancangan, implementasi, pengujian dan analisis telah selesai. Kesimpulan disusun berdasar pada hasil pengujian dan analisis terhadap sistem yang dibangun. Isi pada kesimpulan diharapkan dapat menjadi acuan untuk pengembangan dan penyempurnaan sistem. Pada akhir penulisan ini adalah saran yang bertujuan untuk memperbaiki kesalahan dan penyempurnaan terhadap sistem yang telah dibuat.