# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan teknologi saat ini berkembang sangat pesat khususnya penyedia informasi seperti internet. Dengan adanya internet, memudahkan masyarakat untuk memperoleh dan berbagi informasi kapanpun dan dimanapun masyarakat berada. Di sisi lain, penyebaran internet membuat data multimedia seperti musik , gambar, dan khususnya video menyebar dengan begitu banyak dan menimbulkan ancaman bagi pihak-pihak tertentu. Ancaman yang timbul adalah masalah hak cipta, status kepemilikan, dan HAKI (Hak Kekayaan Intelektual). Masalah tersebut muncul diakibatkan oleh pembajakan atau penggandaan video tanpa izin dari pihak terkait dalam hal ini adalah *Video On Demand*.

Karena video tersebut bisa diakses oleh siapa saja maka dibutuhkan suatu teknologi yang disebut DRM (*Digital Right Management*) dan kriptografi untuk mencegah pembajakan hak cipta, menyalin secara ilegal [1], dan mengatur hak akses yang diberikan kepada mahasiswa ataupun dosen serta membantu dalam proses penyembunyian pesan. Teknologi DRM berfungsi untuk mengontrol penggunaan media digital dengan mencegah akses, menyalin, dan tindakan yang melanggar hak cipta lainnya. Sedangkan kriptografi merupakan salah satu teknologi dalam keamanan suatu sistem yang bertujuan untuk membantu dalam proses penyembunyian pesan atau data dengan cara mengenkripsi dan mendekripsi data tersebut dengan syarat memiliki kunci yang sama untuk mendekripsinya.

Tugas Akhir ini meneliti tentang performansi dari algoritma kriptografi HC-128 pada *Video on Demand*. Algoritma kriptografi HC-128 adalah salah satu dari empat algoritma yang dipilih di kompetisi eStream untuk aplikasi perangkat lunak. Algoritma HC-128 menghasilkan sebuah *keystream* dengan 128 bit kunci dan 128 bit kunci inisiasi vektor. HC-128 stream cipher [2] terdiri dari dua tabel rahasia, masing-masing dengan 512 bit untuk masing-masing elemen terdiri dari 32-bit. Setiap langkah memperbarui satu elemen dari tabel dengan fungsi umpan balik non-linear. Semua elemen dari dua tabel diupdate setiap 1.024 langkah. Pada setiap langkah, satu output 32-bit yang dihasilkan dari non-linear fungsi *output filtering* [3]. Proses penelitian dilakukan dengan membuat program menggunakan Netbeans IDE 8.0.2. Hasil keluaran dari implementasi ini adalah data uji performansi menggunakan lima parameter, yaitu

*avalanche effect*, waktu proses enkripsi dan dekripsi, pengujian waktu normal video asli pada aplikasi, dan kualitas dari video yang kemudian akan dianalisis.

## 1.2 Perumusan Masalah

Penelitian Tugas Akhir ini berkonsentrasi pada implementasi algoritma kriptografi HC-128 pada *Video on Demand* yang terdiri dari permasalahan-permasalahan berikut:

1. Bagaimana mengimplementasikan algoritma kriptografi HC-128 pada konten digital seperti V*ideo on Demand* berbasis DRM (*Digital Right Management*)?
2. Bagaimana pengimplementasian DRM pada *Video on Demand*?
3. Bagaimana performansi algoritma HC-128 pada *Video on Demand* berbasis DRM?

## 1.3 Tujuan

Tujuan penulis membuat Tugas Akhir ini adalah sebagai berikut:

1. Mengetahui cara untuk mengimplementasikan algoritma kriptografi HC-128 pada konten digital seperti *Video on Demand* berbasis DRM.
2. Mengimplementasikan DRM pada konten digital seperti *Video on Demand*.
3. Mengetahui performansi algoritma kriptografi HC-128 pada *Video on Demand* berbasis Digital Right Management.

## 1.4 Batasan Masalah

Hal-hal yang dibatasi dalam penelitian Tugas Akhir ini adalah :

1. Algoritma yang digunakan adalah algoritma kriptografi HC-128
2. *Client* tidak terlibat dalam memasukkan kunci
3. *Client* terdiri dari *client member* dan *client non member*
4. Tipe data yang digunakan adalah video
5. Video yang digunakan berformat .mp4
6. Performansi yang diukur adalah alanisa *avalanche effect*, waktu proses enkripsi dan dekripsi, dan kualitas video
7. Pembobolan akun *client member, server,* dan *database* tidak dibahas
8. Video yang digunakan video tanpa suara

## 1.5 Metodologi Penyelesaian Masalah

Metodologi penelitian yang digunakan adalah:

1. Studi literatur, yaitu mempelajari literatur-literatur yang ada sesuai dengan permasalahan yang akan dibahas meliputi, konsep *Video on Demand*, konsep *Digital Right Management* (DRM), konsep kriptografi, teori algoritma kriptografi HC-128.
2. Konsultasi dengan dosen pembimbing terkait permasalahan dan kemungkinan solusi yang ditawarkan.
3. Perancangan sistem dan perancangan fungsionalitas serta pembuatan desain antarmuka bagi *user* dengan menggunakan bahasa pemograman java, Netbeans IDE 8.0.2.
4. Melakukan uji coba aplikasi yang telah dibuat, serta menganalisa masalah-masalah yang muncul, serta melakukan perbaikan terhadap masalah-masalah tersebut. Uji performansi menggunakan parameter waktu enkripsi dan dekripsi, *avalanche effect* dan kualitas video.
5. Pembuatan laporan dari hasil penelitian

## 1.6 Sistematika Penulisan TA

Adapun sistematika penulisan pada Tugas Akhir ini adalah :

BAB I PENDAHULUAN

Berisi tentang latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, metodologi penelitian, dan sistematika penelitian

BAB II DASAR TEORI

Berisi tentang penjelasan mengenai video, *Video on Demand*, kriptografi, algoritma HC-128, *Digital Right Manajement*, dan dasar teori yang menunjang pada Tugas Akhir ini..

BAB III ANALISIS DAN PERANCANGAN SISTEM

Berisi tentang perancangan sistem yangdan proses analisis yang akan dibangun pada Tugas Akhir ini.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Berisi tentang implementasi dan pengujian dari aplikasi yang telah dibuat seperti performansi algoritma terhadap sistem dan analisis hasil penelitian

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan dari hasil penelitain yang telah dilakukan dan rekomendasi untuk penelitian berikutnya.