1. Pendahuluan

1.1 Latar Belakang Masalah

Dewasa ini perkembangan teknologi informasi terus mengalami kemajuan seiring dengan meningkatnya kebutuhan manusia terhadap informasi terkini maupun informasi yang *real-time*. Teknologi informasi telah menjadi kebutuhan primer hampir di semua lini kehidupan manusia. Tidak hanya berupa teks maupun suara, informasi multimedia seperti video pun telah digunakan dan akan semakin marak digunakan.

Perkembangan teknologi Internet pun semakin mendukung terselenggaranya pendistribusian data video. Melalui Internet memungkinkan video dapat diakses dari mana saja dan kapan saja, baik dengan cara *download* maupun *streaming*. Video streaming merupakan video yang dikirim langsung dari penyedia layanan kemudian dijalankan diaplikasi *media player* penerima secara *real-time* dan berkesinambungan tanpa menyimpan data video tersebut [1]. Contohnya IP video, IPTV, *video teleconference*, *video on demand*, serta monitoring lokasi (*surveillance*) dengan IP Camera maupun CCTV camera. Oleh karena jaringan Internet terbuka untuk publik maka masalah lain pun muncul. Hal ini memungkinkan pendistribusian data video dapat diakses oleh orang lain yang tidak berhak sehingga dapat menurunkan jaminan *privacy* dan *confidentiality* layanan video streaming.

Salah satu solusi untuk meningkatkan jaminan *privacy* dan *confidentiality* adalah dengan menggunakan teknik kriptografi dalam pendistribusian datanya. Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita[10]. Dalam penerapannya, terdapat bermacam-macam algoritma sandi kriptografi yang digunakan untuk keamanan video streaming, diantaranya yaitu algoritma *stream-cipher* RC4 (Rivest Chiper 4) dan *block-cipher* Rijndael (juga dikenal dengan nama AES [Advanced Encryption Standard]) [4]. Algoritma yang dipilih adalah algoritma yang memiliki tingkat keamanan yang tinggi serta menghasilkan performansi yang baik pada aplikasi video streaming [5]. Pada tugas akhir ini diimplementasikan algoritma *stream chiper* RC4 dan algoritma *block chiper* Rijndael untuk proses kriptografi pada video streaming. Setelah itu, hasil keduanya dianalisis dan dibandingkan algoritma mana yang lebih baik digunakan untuk video streaming.

1.2 Perumusan Masalah

Permasalahan yang akan diangkat dalam tugas akhir ini adalah :

1. Bagaimana mengimplementasikan algoritma *stream chiper* RC4 dan algoritma *block chiper* Rijndael dalam proses kriptografi video streaming.
2. Bagaimana hasil perbandingan proses kriptografi video streaming pada aplikasi dengan algoritma RC4 dan aplikasi dengan algoritma Rijndael untuk selanjutnya ditentukan algoritma mana yang lebih baik digunakan untuk video streaming.

Adapun batasan masalah dari perumusan masalah di atas adalah:

1. Data video streaming telah tersedia tinggal dijalankan mekanisme *request* (permintaan) oleh *client* dan *respon* pengiriman data oleh *application server*.
2. Pengujian hanya dilakukan pada *application server* dengan satu *client*.
3. Data video streaming yang akan digunakan adalah data video berformat MPEG-4. Hal ini dikarenakan video berformat MPEG-4 merupakan video terkompres yang memiliki kualitas gambar yang baik dan bisa dioptimasikan untuk data rate yang rendah[2]. Video berformat MPEG-4 juga digunakan untuk data aplikasi web (streaming media) dan aplikasi siaran TV[13].
4. Data video yang dienkripsi adalah gambar videonya saja, tidak termasuk suara. Hal ini dikarenakan informasi terpenting dari video streaming adalah gambar videonya. Jadi lebih berfokus pada pengamanan data videonya.
5. Gambar video hasil *decode* berformat YUV420P. Untuk memperingan proses enkripsi maka *byte* data gambar yang berisi nilai Y saja yang akan dienkripsi.
6. Hasil proses kriptografi yang akan dibandingkan adalah lama proses, *frame-rate* dan jumlah memori yang dibutuhkan pada saat enkripsi dan dekripsi, tingkat kualitas video yang diterima *client* dengan parameter MOS (*Mean Opinion Score*) dan PSNR (*Peak Signal-to-Noise Ratio*), serta ketahanan terhadap *brute force attack*.
7. Tidak melibatkan *error* yang terjadi selama proses transmisi data.
8. Tidak membahas proses pengiriman kunci antara pengirim dan penerima.

1.3 Tujuan

Berdasarkan rumusan masalah di atas, maka tujuan akhir tugas akhir ini adalah:

1. Mengimplementasikan algoritma *stream chiper* RC4 dan algoritma *block chiper* Rijndael pada sebuah aplikasi yang dibangun dari sebuah bahasa pemrograman.
2. Menganalisis hasil proses kriptografi video streaming pada aplikasi algoritma *stream chiper* RC4 dan aplikasi algoritma *block chiper* Rijndael dengan melakukan perbandingan lama proses, *frame rate*, dan jumlah memori yang dibutuhkan pada saat enkripsi dan dekripsi, perbandingan tingkat kualitas video yang diterima *client* dengan parameter MOS (*Mean Opinion Score*) dan PSNR (*Peak Signal-to-Noise Ratio*), serta melakukan perbandingan tingkat keamanan data video streaming dengan melakukan simulasi uji *brute force attack*. Selanjutnya ditentukanlah algoritma mana diantara kedua algoritma tersebut yang lebih baik digunakan untuk video streaming.

Hipotesis

1. Algoritma *stream chiper* RC4 dan algoritma *block chiper* Rijndael dapat diimplementasikan dalam proses kriptografi video streaming.
2. Algoritma *stream chiper* RC4 memiliki proses enkripsi dan dekripsi yang lebih cepat dan lebih sedikit penggunaan memori dibandingkan dengan algoritma *block chiper* Rijndael. Namun algoritma *stream chiper* RC4 lebih

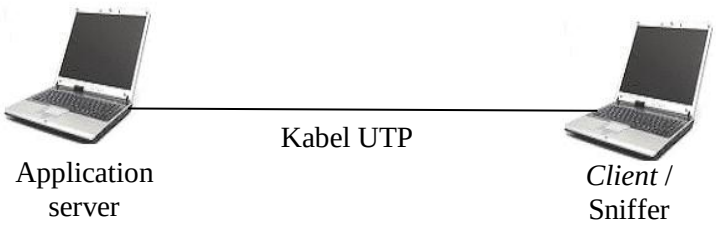
kurang kuat menghadapi *brute force attack* dibandingkan dengan algoritma *block chiper* Rijndael.

3. Algoritma *stream chiper* RC4 lebih baik digunakan untuk video streaming dibandingkan dengan algoritma *block chiper* Rijndael.

1.4 Metodologi Penyelesaian Masalah

Metodologi penyelesaian masalah yang akan digunakan adalah :

1. Studi Literatur
   Pada tahap ini dilakukan pendalaman pemahaman materi yang berhubungan dengan penelitian yang dilakukan, meliputi proses kriptografi video streaming, algoritma *stream chiper* RC4 dan penerapannya, algoritma *block chiper* Rijndael dan penerapannya, serta cara *brute force attack* terhadap kedua algoritma tersebut.
2. Perancangan desain dan analisis
   Pada tahap ini dilakukan analisis dan perancangan terhadap sistem yang akan dibangun serta menganalisis metode yang akan digunakan untuk menyelesaikan permasalahan, termasuk menentukan arsitektur sistem, bahasa pemrograman yang digunakan, fungsionalitas, dan antarmuka aplikasi.
   Gambar 1-1 menunjukkan arsitektur sistem yang akan dibangun.



Gambar 1-1 : Perancangan Arsitektur

   Keterangan:
   - *Application server* merupakan server yang menyediakan layanan aplikasi video yang akan distreaming.
   - Kabel UTP sebagai penghubung antar dua buah komputer/laptop. Jadi kabel UTP jenis crossing yang digunakan.
   - *Client* merupakan pengguna sah yang akan menggunakan layanan video streaming. Dilain pihak, laptop ini akan digunakan oleh *sniffer* untuk melakukan simulasi *brute force attack*.
3. Implementasi
   Pada tahap ini dilakukan penerapan hasil rancangan desain dan analisisi yang terdiri dari:
   a. Pengkodean algoritma *stream chiper* RC4 dan algoritma *block chiper* Rijndael menggunakan bahasa pemrograman Java.
   b. Pembuatan antarmuka/interface aplikasi.
   c. Pengadaan kabel UTP dan pengkonfigurasian koneksi antar dua laptop.
4. Pengujian dan Analisis Hasil
   Pada tahap ini dilakukan pengujian terhadap aplikasi yang telah dibangun. *Application Server* menyediakan lima buah video dengan *content* dan *size* yang berbeda yang akan diakses oleh *client*. Pengujian dilakukan dengan

melakukan analisis perbandingan. Secara objektif pengujian dipusatkan pada perbandingan rata-rata lama proses, *frame rate*, dan jumlah memori yang dibutuhkan pada saat enkripsi di sisi *application server* dan dekripsi di sisi *client*. Data video setelah dekripsi juga akan dibandingkan dengan data video asli dari *application server*, lalu dihitung PSNR (*Peak Signal-to-Noise Ratio*) dan secara subjektif dihitung MOS (*Mean Opinion Score*) dari dua puluh *user client*. Ketahanan terhadap *brute force attack* dilakukan dengan menghitung seberapa lama proses untuk mencoba semua kemungkinan kunci.

Algoritma yang lebih baik digunakan untuk video streaming ditentukan dengan menganalisis algoritma mana yang memiliki waktu proses lebih cepat, jumlah memori lebih sedikit, tingkat kualitas video yang diterima lebih tinggi, serta yang tahan lama terhadap *brute force attack* dibandingkan dengan algoritma lainnya. Kemudian dibuat kesimpulan yang ada sesuai dengan tujuan tugas akhir ini.

5. Pembuatan laporan Tugas Akhir
   Pada tahap ini dilakukan pendokumentasian tahap-tahap yang telah dilakukan pada bagian metodologi ini mulai dari studi literatur sampai analisis hasil yang berisi kesimpulan sebagai bahan hasil penelitian yang telah dilakukan.

1.5 Sistematika Penulisan

Tugas akhir ini disusun dengan sistematika penulisan sebagai berikut :

BAB I Pendahuluan
Bab ini berisi latar belakang, perumusan masalah, tujuan dan batasan masalah dari tugas akhir, metodologi yang digunakan dalam menyelesaikan tugas akhir ini serta sistematika penulisan buku tugas akhir.

BAB II Dasar Teori
Bab ini berisi tentang uraian mengenai keamanan informasi dengan Kriptografi, Algoritma *Stream Chiper* RC4, Algoritma *Block Chiper* Rijndael dan Kriptoanalisis dengan *Brute Force Attack*.

BAB III Analisis dan Perancangan Sistem
Bab ini berisi analisis kebutuhan sistem serta rancangan sistem secara terstruktur yang tertuang dalam bentuk *Unified Modeling Language (UML)*.

BAB IV Implementasi dan Analisis Hasil Pengujian
Bab ini berisi hasil implementasi dan pengujian algoritma *stream chiper* RC4, algoritma *block chiper* Rijndael serta analisis perbandingan dari hasil pengujian tersebut.

BAB V Kesimpulan dan Saran
Bab ini berisi tentang kesimpulan yang didapat dari pelaksanaan tugas akhir ini dan saran-saran yang diperlukan untuk perbaikan maupun pengembangannya lebih lanjut.