# 1. Pendahuluan

## 1.1 Latar belakang

Kriptografi adalah ilmu yang digunakan untuk menjaga kerahasiaan. Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Dalam hal ini sangat terkait dengan betapa pentingnya data tersebut dikirim dan diterima oleh pihak atau orang yang berkepentingan, apakah data tersebut masih *authenticity*. Data akan tidak berguna lagi apabila di tengah jalan informasi itu diakses oleh orang yang tidak berhak atau berkepentingan [8]. Dalam penyimpanan dan pengiriman data komputer, isi dari data tersebut harus dijaga keaamanannya. Dalam kriptografi terdapat 2 proses utama yaitu enkripsi dan dekripsi. Untuk menjaga keamanan dan kerahasiaan data dalam suatu jaringan komputer maka diperlukan beberapa enkripsi guna membuat data agar tidak dapat dibaca (*ciphertext*) atau dimengerti oleh sembarang orang, kecuali untuk penerima yang berhak. Dan juga dekripsi untuk mengembalikan data yang terenkripsi tersebut (*ciphertext*) menjadi data yang sebenarnya (*plaintext*).

Salah satu algoritma kriptografi yang digunakan sekarang adalah RC4. Algoritma RC4 merupakan salah satu algoritma kriptografi yang termasuk ke dalam kategori *stream cipher* yang masih sering digunakan pada system keamanan. Algoritma ini terdiri dari 3 langkah utama (inisialisasi array, KSA, dan PRGA) untuk menggenerate suatu *keystream* yang akan digunakan dalam proses enkripsi dan dekripsi[7]. Algoritma ini dibuat oleh Ron Rivest (1987) dari laboratorium *RSA*. RC4 salah satu jenis stream cipher yang singkron yaitu cipher yang memiliki key simetris dan mengenkripsi atau dekripsi plaintext secara digit per digit atau bit per bit dengan cara mengkombinasikan secara operasi biner (XOR) dengan sebuah angka semiacak. RC4 dapat dijalankan dengan panjang key variable dan beroperasi dengan orientasi byte. RC4 terkenal sebagai metode enkripsi yang cepat,efisien dan sederhana, namun adanya kelemahan *Bit-Flipping Attack* atau BFA dimana penyerang dapat mengetahui sample atau keseluruhan *pleintext* dari *ciphertext* tanpa harus mengetahui key enkripsi menjadi salah satu metode enkripsi yang kurang aman.

Oleh karena itu, pada tugas akhir ini akan mengimplementasikan performasi RC4 serta keamanan data dari serangan *Bit Flipping Attack* pada proses enkripsi dan dekripsi. Solusi yang dibutuhkan untuk menangani masalah tersebut adalah dengan menggunakan *Initialization Vector (IV)* dalam key dan menambahkan crc32 pada plaintext sebelum dilakukan enkripsi. Selain memperkecil terjadinya *Bit-Flipping Attack* pada RC4 hal ini juga memungkinkan untuk mendapatkan hasil enkripsi yang berbeda walaupun memiliki key yang sama.

## 1.2 Perumusan masalah

Rumusan masalah dalam tugas akhir ini adalah bahwa metode enkripsi RC4 memiliki celah yang dapat diserang oleh *attacker*, yaitu masalah *Bit-Flipping Attack*. *Bit-Flipping Attack* merupakan serangan terhadap sebuah sandi kriptografi dimana *attacker* dapat mengubah ciphertext sedemikian rupa untuk menghasilkan perubahan yang dapat diprediksi *plaintext*.

## 1.3 Tujuan

Tujuan yang ingin dicapai dari tugas akhir ini yaitu membangun suatu aplikasi yang menerapkan algoritma stream cipher RC4 yang efisien, sederhana, dan aman dari serangan *Bit Flipping Attack*, sehingga data yang ditransmisikan lebih terjaga keabsahannya dan menyulitkan *attacker* dalam memecahkannya.

## 1.4 Hipotesa

Sistem yang dibangun mengimplementasikan enkripsi (penyandian data) sebagai bentuk pengamanan data oleh pihak yang tidak berwenang. Dalam tugas akhir ini, implementasi enkripsi dan dekripsi dilakukan dengan menggunakan algoritma RC4 dengan pertimbangan sebagai berikut:

1. RC4 merupakan metode enkripsi tercepat dibandingkan stream cipher lainnya sebagai salah satu metode enkripsi. Selain itu kesuksesan RC4 antara lain adalah efisien untuk diimplementasikan baik dalam hardware maupun software, dan mudah untuk dikembangkan.
2. RC4 adalah salah satu jenis *stream cipher* yang sinkron yaitu cipher yang memiliki key simetris dan mengenkripsi atau mendekripsi *plaintext* secara digit per digit atau bit per bit dengan cara mengkombinasikan secara operasi biner (biasanya operasi XOR) dengan sebuah angka semi acak.
3. RC4 dapat dijalankan dengan panjang key variable dan beroperasi dengan orientasi byte.

Namun metode enkripsi RC4 memiliki celah yang dapat diserang oleh *attacker*, yaitu masalah *Bit-Flipping Attack. Bit-Flipping Attack* merupakan serangan terhadap sebuah sandi kriptografi dimana *attacker* dapat mengubah *ciphertext* sedemikian rupa untuk menghasilkan perubahan yang dapat diprediksi *plaintext*.

Hal tersebut dapat diatasi dengan CRC32 yang dapat mendeteksi *error* (kerusakan) pada sebuah data yang mungkin terjadi pada saat pengiriman data. Metode ini menghitung nilai *checksum* dari panjang bit sebuah data yang kemudian membandingkannya dengan aturan CRC dengan menggunakan bit untuk mendeteksi apakah data tersebut mengalami kerusakan atau tidak. Jika akan menggunakan key yang sama untuk setiap kali mengenkripsi file, maka diperlukan *Inisialisasi Vector (IV)* pada *secret key*. Selain memperkecil terjadinya Bit-Flipping Attack pada RC4 hal ini juga memungkinkan untuk mendapatkan hasil enkripsi yang berbeda walaupun memiliki key yang sama.

## 1.5 Batasan Masalah

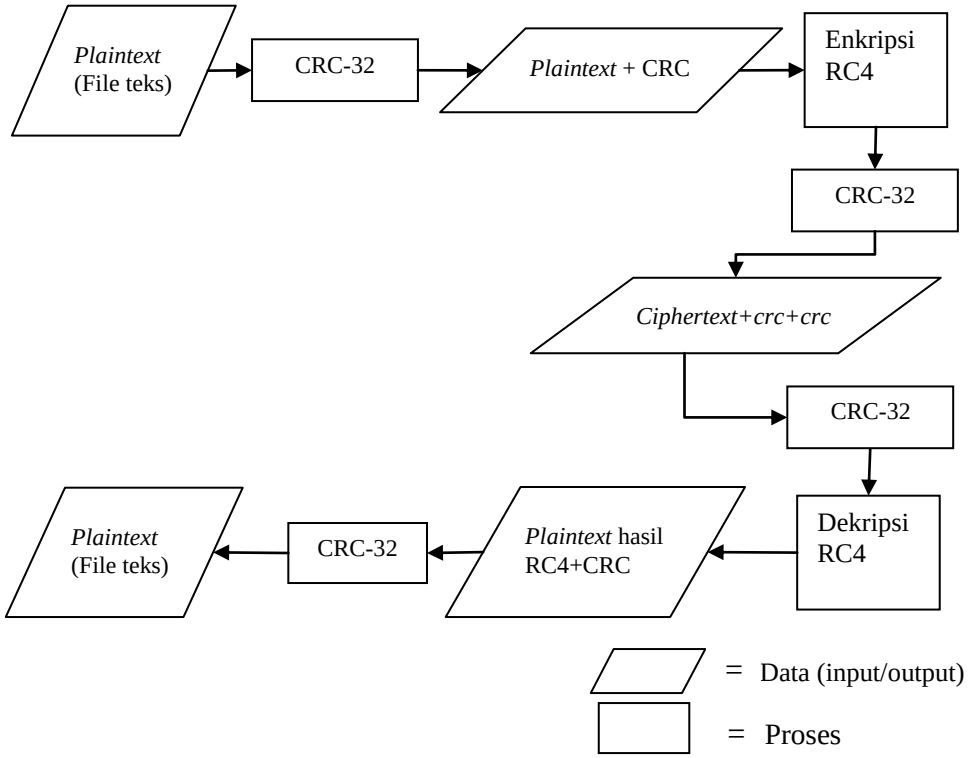
Pada tugas akhir ini akan dibatasi oleh beberapa batasan masalah, yaitu:

1. Informasi yang akan dienkripsi adalah karakter (angka, huruf, atau simbol) yang dalam sistem akan dijadikan bilangan decimal dengan format file teks berekstensi *.txt sebesar 0 sampai 102400 byte.
2. Penggunaan CRC sebesar 32 bit sebagai algoritma ICV (*Integrity Check Value*).
3. Program dibuat dengan bahasa pemrograman Java.
4. Pengujian hanya dilakukan pada *localhost application server* dengan satu client.
5. Tidak membahas proses pengiriman key antara pengirim dan penerima.

## 1.6 Metodologi Penyelesaian Masalah

Metodologi penelitian yang diterapkan pada pengerjaan Tugas Akhir ini adalah:

1. Studi Literatur
   Studi literature dari beberapa buku, jurnal, artikel yang membahas tentang Kriptografi RC4 (Enkripsi & Dekripsi), *Bit Flipping Attack* (BFA), CRC32,dan *Initialization Vector* .
2. Perancangan Sistem dan Implementasi Sistem
   Tahap ini meliputi pembangunan perangkat lunak berdasarkan skema system yang telah dirancang. Adapun skema proses enkripsi dan dekripsi yang dibangun dapat ditunjukkan oleh gambar 1.1 berikut:




Gambar 1-1: Skema Proses Enkripsi & Deskripsi

3. Penguji dan Analisis
   Pada tahap ini dilakukan pengujian dan analsisi terhadap Metode Kriptografi RC4 dari serangan *Bit Flipping Attacks*. Pengujian dilakukan dengan memperhatikan pengaruh penambahan CRC-32 dalam *plaintext* sebelum di enkripsi dan akan dipadukan dengan membangkitkan nilai random untuk pengisian *key byte array* sehingga pengisian kunci ke dalam array tidak berulang. Pengujian kunci yang digunakan dilakukan dengan tidak menggunakan kunci yang sudah pernah digunakan. Setelah itu dilakukan pengujian ketahanan data enkripsi terhadap serangan BFA.
4. Penyusunan Laporan
   Pada tahap ini dilakukan penyusunan laporan hasil analisis yang telah dilakukan dan membuat kesimpulan dari hasil analisis tersebut.

## 1.7 Sistematika Penulisan

Tugas Akhir ini terdiri dari beberapa bagian yaitu:

Pada **BAB 1** dibahas tentang latar belakang, perumusan masalah, batasan masalah, tujuan pembahasan dan sistematika penulisan.

Pada **BAB 2** dibahas tentang penjelasan singkat mengenai konsep-konsep yang mendukung dibuatnya sistem ini. Konsep yang digunakan untuk sistem ini adalah *Bit Flipping Attack* (BFA), RC4, CRC-32, *Initialization Vector* (IV), dan *Avalanche Effect* (AE).

Pada **BAB 3** dibahas tentang rincian mengenai desain serta skema proses sistem yang dibuat pada Tugas Akhir ini.

Pada **BAB 4** dibahas tentang rincian implementasi tampilan layar sistem Tugas Akhir yang dibuat serta lingkkungan pendukung perangkat keras dan perangkat lunak.

Pada **BAB 5** dibahas tentang rincian mengenai skenario dan pengujian terhadap sistem yang disertai dengan analisa hasil pengujian.

Pada **BAB 6** dibahas tentang kesimpulan yang diambil berdasarkan sistem yang telah dibuat disertai dengan saran untuk perbaikan di masa mendatang.