

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat telah membawa perubahan besar dalam berbagai aspek kehidupan, terutama dalam hal komunikasi dan pertukaran data. Salah satu *platform* yang paling banyak digunakan dalam pengelolaan dan penyebaran informasi adalah aplikasi berbasis web. Namun, seiring dengan kemudahan akses dan pertukaran data secara daring, risiko terhadap keamanan informasi juga semakin meningkat. Ancaman seperti pencurian data, penyadapan komunikasi, hingga manipulasi informasi menjadi tantangan serius yang harus dihadapi [1].

Untuk menjawab tantangan tersebut, penggunaan algoritma kriptografi menjadi salah satu solusi utama dalam menjamin kerahasiaan, integritas, dan keaslian data. Algoritma kriptografi simetris, seperti RC4, RC5, dan RC6, telah banyak digunakan dalam berbagai sistem karena kecepatan dan efisiensinya dalam memproses data [2]. Namun, setiap algoritma memiliki karakteristik, tingkat keamanan, serta kompleksitas implementasi yang berbeda-beda.

RC4 dikenal sebagai algoritma yang ringan dan cepat, tetapi memiliki kelemahan serius dalam hal keamanan sehingga mulai ditinggalkan [3]. RC5 menawarkan struktur yang fleksibel dengan tingkat keamanan yang lebih baik, sementara RC6, sebagai pengembangan dari RC5, dirancang untuk memberikan keamanan yang lebih tinggi dan efisiensi pada platform modern [4].

Perbedaan ini menimbulkan pertanyaan penting: algoritma mana yang paling optimal untuk diimplementasikan dalam sistem berbasis web, terutama dalam hal keamanan, efisiensi waktu, dan kemudahan integrasi ke dalam aplikasi.

Melalui perbandingan tersebut, dapat diidentifikasi beberapa permasalahan utama yang menjadi fokus dalam penelitian ini. Permasalahan pertama adalah perlunya pemahaman yang mendalam mengenai tingkat keamanan dari masing-masing algoritma ketika diimplementasikan dalam sistem berbasis web yang rawan terhadap ancaman digital. Permasalahan kedua terletak pada tingkat kompleksitas serta kemudahan implementasi dari algoritma RC4, RC5, dan RC6 dalam pengembangan aplikasi web. Dan yang ketiga, dibutuhkan analisis mengenai algoritma mana yang paling optimal untuk digunakan dalam sistem web, jika dilihat dari segi keamanan, efisiensi waktu eksekusi, serta kemudahan integrasi ke dalam sistem aplikasi.

Untuk menjawab permasalahan tersebut, penelitian ini menggunakan metode *Rapid Application Development* (RAD), yaitu pendekatan dalam pengembangan perangkat lunak yang menekankan pada kecepatan dan efisiensi melalui proses iteratif dan pembuatan prototipe. Metode ini memungkinkan pengembangan sistem secara cepat dengan melibatkan pengguna secara langsung dalam setiap tahapannya, sehingga sistem yang dihasilkan lebih sesuai dengan kebutuhan nyata di lapangan [5].

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk melakukan analisis komparatif terhadap algoritma RC4, RC5, dan RC6 sistem berbasis web dengan metode RAD. Penelitian ini tidak hanya dilakukan secara teoritis, tetapi

juga melalui implementasi nyata dalam sebuah aplikasi web yang akan menguji masing-masing algoritma berdasarkan waktu eksekusi dan tingkat kesulitannya dalam pengembangan.

Namun, penelitian-penelitian sebelumnya umumnya hanya membandingkan dua algoritma, atau hanya membahas satu aspek saja (contohnya efisiensi atau keamanan). Belum banyak penelitian yang secara eksplisit membandingkan ketiga algoritma RC4, RC5, dan RC6 secara bersamaan dalam implementasi praktis di aplikasi web, yang mempertimbangkan keamanan, efisiensi waktu dan memori, serta kemudahan integrasi. Gap inilah yang coba diisi oleh penelitian ini.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan, dapat diidentifikasi beberapa permasalahan utama yang menjadi dasar penelitian ini, yaitu:

1. Masih adanya celah keamanan pada algoritma kriptografi tertentu, seperti RC4, yang rentan terhadap serangan kriptografi, sehingga diperlukan analisis mendalam mengenai tingkat keamanan algoritma RC4 dibandingkan dengan RC5 dan RC6.
2. Belum adanya acuan komparatif yang menyeluruh dalam bentuk sistem web yang dapat menunjukkan perbandingan langsung antar algoritma dari segi keamanan, efisiensi, dan kemudahan implementasi secara praktis.
3. Diperlukan media uji berbasis web untuk mengevaluasi langsung algoritma kriptografi RC4, RC5, dan RC6 sehingga hasil analisis dapat lebih aplikatif dan mudah dipahami oleh pengguna maupun pengembang.

1.3 Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana tingkat keamanan algoritma kriptografi RC4, RC5, dan RC6 dapat diandalkan pada sistem berbasis web ?
2. Seberapa besar kemudahan dalam mengimplementasikan algoritma RC4, RC5, dan RC6 pada sistem berbasis web ?
3. Bagaimana menganalisa perbandingan ketiga algoritma kriptografi tersebut, untuk mencari algoritma yang optimal berdasarkan aspek keamanan, efisiensi, dan kemudahan implementasi ?

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Menganalisis dan membandingkan tingkat keamanan algoritma RC4, RC5, dan RC6 pada sistem berbasis web.
2. Mengukur efisiensi algoritma dalam satuan waktu proses dan konsumsi memori selama proses enkripsi dan dekripsi.
3. Membangun aplikasi web sederhana untuk menguji dan mengevaluasi performa ketiga algoritma.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. **Bagi akademisi:** Sebagai referensi dalam studi kriptografi simetris dan implementasinya dalam aplikasi web.
2. **Bagi pengembang sistem:** Memberikan gambaran praktis mengenai performa dan kompleksitas dari masing-masing algoritma.
3. **Bagi penelitian selanjutnya:** Menjadi dasar dalam penelitian lanjutan terkait pengembangan sistem keamanan data berbasis web.

1.6 Batasan Masalah

Agar penelitian ini lebih fokus dan terarah, maka ditetapkan beberapa batasan masalah sebagai berikut:

1. Penelitian ini hanya membahas tiga algoritma kriptografi simetris, yaitu RC4, RC5, dan RC6.
2. Implementasi sistem dilakukan dalam bentuk aplikasi web sederhana untuk menguji dan membandingkan algoritma.
3. Pengujian efisiensi hanya difokuskan pada waktu proses enkripsi dan dekripsi data.
4. Aspek keamanan yang dianalisis terbatas pada analisis kerentanan umum secara deskriptif, bukan melalui eksploitasi nyata.
5. Aplikasi web yang dikembangkan tidak menyertakan sistem autentikasi pengguna atau manajemen basis data kompleks, fokus hanya pada proses enkripsi-dekripsi.

1.7 Sistematika Penulisan

Adapun sistematika penulisan skripsi ini disusun sebagai berikut:

BAB I PENDAHULUAN

Berisi latar belakang, identifikasi masalah, rumusan masalah, tujuan, manfaat, batasan masalah, metode, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Berisi teori-teori dasar yang mendukung penelitian, termasuk pembahasan algoritma kriptografi RC4, RC5, dan RC6, serta teknologi pengembangan web yang digunakan.

BAB III METODOLOGI PENELITIAN

Menjelaskan proses metode RAD yang akan diimplementasikan, desain sistem, spesifikasi teknis, serta langkah-langkah implementasi.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisi tentang perancangan sistem, penerapan antarmuka sistem dan hasil dari implementasi sistem.

BAB V PENUTUP

Pada bab ini berisi tentang kesimpulan dari hasil penelitian, baik dari permasalahan, tujuan, dan hasil implementasi sistem.