BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Kriptografi klasik merupakan cara penyamaran data atau informasi yang dilakukan oleh orang-orang dulu ketika belum ada komputer dengan tujuan untuk melindungi informasi dengan cara melakukan penyandian. Perlindungan informasi perlu dilakukan untuk mengamankan data yang bersifat rahasia agar tidak dapat diketahui oleh orang lain. Pada era komputer, pengiriman data atau informasi dilakukan menggunakan jaringan komputer dan data atau informasi tersebut disimpan di dalam komputer. Kriptografi juga dilakukan di era komputer tetapi di era komputer kirptografi yang digunakan disebut dengan kriptografi modern. Kritografi modern menggunakan algoritma matematika yang cukup rumit dengan penggunaan kunci. Kriptografi klasik dan kriptografi modern memiliki persamaan yaitu sama-sama melakukan penyandian dengan melakukan transposisi dan subtitusi huruf untuk menghasilkan susunan huruf atau angka yang teracak dan tak bisa terbaca atau dimengerti. Didalam dunia pendidikan kriptografi kurang diminati oleh mahasiswa karena perhitungannya yang rumit sehingga susah dipahami.

Dan seiring perkembangan teknologi informasi saat ini media merupakan salah satu teknik belajar yang sangat efektif untuk menigkatkan minat belajar seorang secara pribadi. media pembelajaran memerlukan suatu perangkat multimedia yang menampilkan materi pembelajaran dengan cara yang menarik. Dengan menggunakan suatu perangkat seperti, Televisi, Laptop, Handphone yang menggunakan jaringan internet, dan perangkat multimedia lainnya.

Jaringan internet merupakan salah satu teknologi yang dapat digunakan sebagai suatu sarana untuk mewujudkan sebuah media pembelajaran. Melalui jaringan internet semua pembelajaran dapat disajikan secara menarik sehingga menimbulkan minat belajar yang tinggi.

Oleh karena itu pada tugas akhir ini penulis mencoba membuat suatu aplikasi web yang membahas tentang media pembelajaran kriptografi dengan pembahasan materi vigenere cipher, stream cipher dan base64 berbasis web untuk mempermudah pengguna belajar dan mengerjakan soal tentang kriptografi.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas maka dapat di ambil rumusan masalah yaitu bagaimana membuat suatu aplikasi media pembelajaran kriptografi dengan menggunakan metode vigenere cipher, stream cipher dan base64 berbasis web.

1.3 Ruang Lingkup

Ruang lingkup masalah pada aplikasi ini adalah :

1. Aplikasi web media pembelajaran ini membahas tentang kriptografi.
2. Bahasa pemrograman yang digunakan adalah PHP berbasis web, sedangkan editor yang digunkan adalah Dreamweaver.
3. Aplikasi ini hanya membahas tentang metode vegenere cipher, stream cipher dan base64 tanpa mengkombinasi tiap metode.
4. Untuk konversi stream cipher mengunakan table ascii 127 bit.
5. Untuk konversi vigenere cipher mengunakan table vigenere.
6. Untuk konversi Base64 mengunakan table Base64.

7. Aplikasi ini menyediakan soal atau kuis yang bisa dikerjakan oleh pengguna.
8. Input data soal kuis, latihan dan materi dilakukan oleh admin.
9. Pengguna mengerjakan soal kuis, latihan, lihat materi dan melakukan enkrpsi.

1.4 Tujuan

Tujuan aplikasi ini adalah untuk menghasilkan sebuah aplikasi media pembelajaran kriptografi dengan materi vigenere cipher, stream cipher dan base64 berbasis web. Dan berupaya memberikan kemudahan bagi pengguna untuk dapat mempelajari kriptografi dengan metode yang akan di terapkan.

1.5 Manfaat Penelitian

Manfaat dari aplikasi ini adalah untuk memudahkan pengguna dalam mempelajari kriptografi dengan materi yang diterapkan. Karena aplikasi menyediakan enkripsi maupun dekripsi, berikut dengan langkah-langkah penyelesaian dan penjelasan bagaimana hasil bisa didapatkan.

1.6 Sistematika Penulisan

1. BAB I PENDAHULUAN

   Menjelaskan tentang ide penelitian secara terinci meliputi, latar belakang, rumusan masalah, ruang lingkup, tujuan dan manfaat penelitian.

2. BAB II TINJAUAN PUSTAKA DAN DASAR TEORI

   Menjelaskan tentang referensi dari penelitian ini yang berkaitan serta acuan dari pelaksanaan penelitian.

3. BAB III METODE PENELITIAN

Menjelaskan tentang apa saja properti yang dibutuhkan untuk melakukan penelitian ini, diantaranya : Data, Peralatan, Prosedur dan Analisis dan Rancangan sistem.

4. BAB IV IMPLEMENTASI DAN PEMBAHASAN

   Menjelaskan tentang pembahasan penelitian dari aplikasi sampai sistem yang telah diuji coba.

5. BAB V PENUTUP

   Menjelaskan tentang kesimpulan dan saran dari penelitian ini.