BAB I

PENDAHULUAN

I.1. Latar belakang

Pada era teknologi komunikasi dan informasi saat ini, sebagian masyarakat tidak lagi melakukan komunikasi dengan pertemuan secara langsung atau bertatap muka. Salah satu alat komunikasi yang digunakan adalah teknologi, sehingga penggunaan pesan teks dapat sampai dari sisi pengirim ke sisi penerima dengan memudahkan kita terutama lebih efektif dan efisien. Pesan teks yang kita miliki dikirim dengan bebas melalui jaringan dengan tingkat kemanan yang relatif rendah.

Dibutuhkan pengamanan yang dapat menjaga kerahasiaan pesan teks agar sampai kepada si penerima dengan aman dan tidak ada kebocoran atau serangan-serangan yang terjadi, seperti serangan eavesdropping.

Perlu adanya pengamanan data pada pesan teks dengan menyandikan (mengenkripsikan) pesan yang akan dikirim. Keamanan adalah salah satu faktor yang sangat penting, apalagi di era saat ini. Tujuannya untuk melindungi informasi dengan cara melakukan penyandian. Salah satunya dengan kombinasi Hiil Cipher dan Vigenere Chipher.

Penggunakan 2 Algortima ini tidak terlalu menyulitkan bagi penggunanya dikarenakan masih menggunakan teknik kriptografi klasik. Kriptografi klasik beroperasi dalam mode karakter, yakni menggunakan huruf abjad (A - Z).

Kelemahan Algoritma ini dikarenakan masih menggukan teknik kriptogarfi klasik yang dimana polanya begitu sederhana. Hill cipher adalah algoritma

keamanan data menggunakan perhitungan perkalian matriks, sedangkan vigenere cipher adalah algoritma yang melakukan enkripsi sekaligus sebuah teks yang terdiri dari beberapa huruf.

Salah satu solusi untuk mengatasi kelemahan-kelemahan kripto klasik ini dengan cara mengkombinasikan kedua metode algoritmanya. Jika kedua algoritma dikombinasikan dalam sebuah aplikasi keamanan data, maka akan lebih sulit memecahkan sandinya bila dibandingkan dengan hanya menggunakan satu algoritma saja. Penggabungan antara dua algoritma tersebut menjadi sebuah solusi untuk memperkuat algoritma menjadi lebih sulit untuk dapat dipecahkan dan untuk mengecoh kriptanalisis. File teks yang telah diamankan menggunakan Algoritma Vigenere Cipher akan diamankan lagi menggunakan Algoritma Hill Cipher.

Kombinasi dan modifikasi vigenere cipher dan hill cipher untuk menyulitkan kriptanalis untuk memecahkan pesan asli. Semakin banyak proses yang diperlukan dan semakin panjang waktu yang dibutuhkan untuk memecahkan pesan yang telah di enkripsi tersebut artinya semakin aman digunakan untuk merahasiakan pesan.Menggabungkan dua metode atau lebih dapat membuat pesan semakin sulit dimengerti bagi orang lain. Hal ini dapat memudahkan bagi pengirim pesan untuk menyampaikan pesan yang bersifat rahasia ke penerima.

Berdasarkan permasalahan yang telah dijabarkan, untuk mengamankan data seperti penyandian teks, maka penulis tertarik untuk mengambil judul tentang : "***Implementasi Algoritma Hill Cipher dan Vigenere Cipher Dalam Penyandian Teks Berbasis Web***"

I.2 Ruang Lingkung Permasalahan

I.2.1 Identifikasi Masalah

Berdasarkan latar belakang tersebut, penulis mengidentifikasi masalah sebagai berikut :

1. Dibutuhkan pengamanan yang dapat menjaga kerahasiaan pesan teks agar sampai kepada si penerima dengan aman dan tidak ada kebocoran atau serangan- serangan yang terjadi, seperti serangan eavesdropping.
2. Penyandian data masih meggunakan Algoritma klasik yang dimana polanya begitu sederhana.
3. Diperlukan kombinasi antar algoritma agar menyulitkan kriptanalisis memecahkan pesan aslinya.

I.2.2 Rumusan Masalah

Berdasarakan latar belakang yang sudah dijelaskan diatas, maka dapat diambil kesimpulan suatu rumusan masalah sebagai berikut :

1. Bagaimana merancang sistem keamanan berupa penyandian teks berbabis *website*.
2. Bagaimana penggabungan metode *Hill Cipher* dan *Vigenere Cipher*.
3. Bagaimana menetapkan metode *Hill Cipher* dan *Vigenere Cipher* dalam keamanan *website*.

I.2.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini agar tidak menyimpang dari tujuan semula adalah :

1. Aplikasi yang dibuat hanya berisi penyandian data berupa teks.

2. Aplikasi yang dirancang menggunakan algoritma *Hill Cipher* dan *Vigenere Cipher*.
3. Menggunakan Matrix 2x2.
4. Gabungan algoritma ini hanya berbasis karakter Abjad dari A – Z.
5. Menggunakan kunci yang simetris.
6. Implementasi aplikasi penyandian data berupa teks berbasis *web*.
7. Menggunakan Bahasa pemograman *HTML*, dan *PHP*.
8. Menggunakan Framework Boostrap.

I.3 Tujuan dan Manfaat Penelitian

I.3.1 Tujuan Penelitian

Tujuan yang diharapkan peneliti ini yaitu sebagai berikut :

1. Menghasilkan sebuah sistem keamanan berupa penyantian teks dengan penerapan *Hill Cipher* dan *Vigenere Cipher*.
2. Mampu membangun sebuah sistem keamanan dengan metode *Hill Cipher* dan *Vigenere Cipher* berbasis *website.*
3. Menerapkan *Algoritma Hill Cipher* dan *Vigenere Cipher* kedalam pengamanan data teks berbasis *website.*

I.3.2 Manfaat penelitian

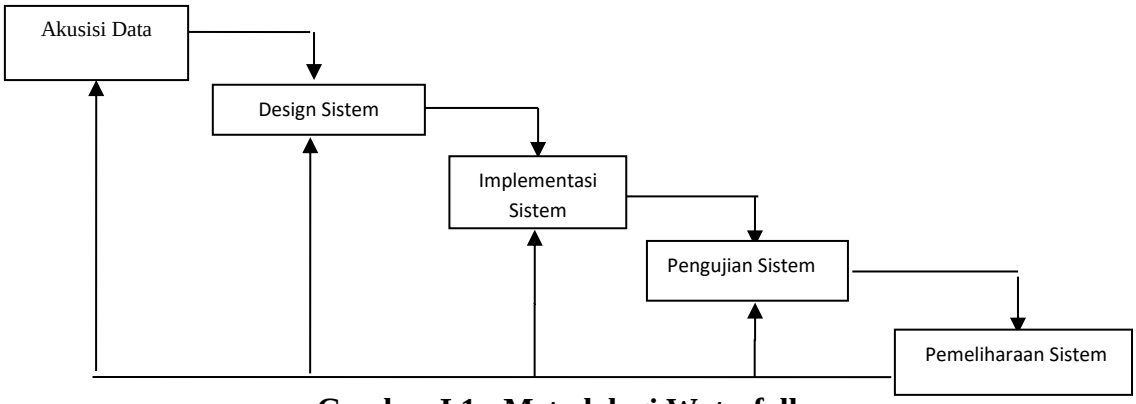
Adapun manfaat yang diharapkan peneliti dari penelitian ini yaitu sebagai berikut :

1. Terciptanya sebuah aplikasi berbasis website yang mampu mengamankan data berupa penyandian teks.

2. Dengan ada penerapan *Algoritma Hill Cipher* dan *Vigenere Cipher* pada penyandian teks, pengguna lebih mudah berkutar informasi.
3. Sebagai media pembelajaran untuk menguji enkripsi atau dekrisi.
4. Agar penilitian ini dapat menjadi referensi bagi yang membacannya.

I.4 Metodologi Penelitian

Dalam pengembangan suatu sistem ini peneliti menggunakan model *waterfall* kerena pengaplikasian menggunakan model ini mudah diimplementasikan dimana hal ini menggambarkan pendekatan yang sistematis dan juga berurutan pada pengembangan perangkat lunak. Tahapan metode *waterfall* dapat dilihat pada gambar III.1 di bawah ini.



Gambar I.1 : Metodologi Waterfall

Penjelasan gambar III.1 Implementasi Algoritma *Hill Cipher* dan *Vigenere Cipher* Dalam Penyandian Teks Berbasis Web pada model *waterfall:*

a. Akusisi Data

   Akuisisi data merupakan metode yang dilakukan penulis dengan mengambil, mengumpulkan dan menyiapkan data yang berisi tentang Implementasi Algoritma *Hill Cipher* dan *Vigenere Cipher* Dalam Penyandian Teks Berbasis Web. Pada penelitian ini penulis memilih referensi dari jurnal, web, buku, perpustakaan dan skripsi yang berkaitan dengan penelitian ini.

b. Design Sistem

Pada tahapan ini, design sistem membantu dalam menentukan perangkat keras *(hardware)* dan mendefenisikan arsitektur sistem secara keseluruhan dengan menggunakan *use case* pada sistem yang akan dibangun.

c. Implementasi Sistem

Pada tahap ini, sistem pertama kali dikembangkan di program kecil yang disebut *unit,* yang terintegrasi dalam tahap selanjutnya. Setiap *unit* dikembangkan dan diuji untuk fungsionalitas yang disebut sebagai *unit testing*.

d. Pengujian Sistem

Dalam tahapan ini, sistem yang dirancang diuji kemampuan dan keefektifan nya dalam suatu *BlackBox Testing*. Sehingga didapatkan kekurangan dan kelemahan sistem yang kemudian dilakukan pengkajian ulang dan perbaikan terhadap aplikasi.

e. Pemeliharaan Sistem

Tahap akhir dalam model *waterfall* ini perangkat lunak yang sudah jadi, dijalankan serta dilakukan pemeliharaan. Pemeliharaan termasuk dalam memperbaiki kesalahan yang tidak ditemukan pada langkah sebelumnya. Perbaikan implementasi *unit* sistem dan peningkatan jasa sistem sebagai kebutuhan baru.

I.5 Kontribusi Penelitian

Adapun kontribusi yang diberikan pada penelitian ini adalah sebagai berikut:

1. Aplikasi yang dihasilkan dari penelitian ini dapat memudahkan pengguna dalam uji coba enkripsi dan dekripsi pada 2 algoritma.

2. Meningkatkan penggunaan teknologi dalam membangun aplikasi web dalam melakukan penyandian teks.

3. Penelitian yang akan dihasilkan dapat djadikan rujukan bagi peneliti lainnya yang ingin mengembangkan sistem atau aplikasi yang lebih spesifik untuk diterapkan dalam bidang lainnya.

I.6 Sistematika Penelitian

Adapun sistematika penulisan yang diajukan dalam Skripsi ini adalah sebagai berikut:

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metodologi penelitian, kontribusi penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang sedang dihadapi.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan dan desain sistem secara detail.

BAB IV : HASIL DAN UJI COBA

Pada bab ini menerangkan hasil dan pembahasan aplikasi yang dirancang serta kelebihan dan kekurangan aplikasi yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan pada masa yang akan dating.