BAB I
PENDAHULUAN

1.1 Latar Belakang

Sangat pentingnya sebuah nilai informasi menyebabkan seringkali informasi hanya boleh diakses oleh orang-orang tertentu saja. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi. Dari permasalahan tersebut ada beberapa metode yang bisa dipakai untuk meningkatkan keamanan data atau informasi, salah satunya adalah menggunakan kriptografi.

Kriptografi didefinisikan sebagai ilmu dan pelajaran untuk tulisan rahasia dengan pertimbangan bahwa komunikasi dan data dapat dikodekan untuk mencegah dari mata-mata atau orang lain yang ingin mengetahui isinya, dengan menggunakan kode-kode dan aturan-aturan tertentu dan metode lainnya sehingga hanya orang yang berhak yang dapat mengetahui isi pesan sebenarnya [1].

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses mengubah informasi atau data menjadi bentuk yang hampir tidak dikenali sebagai informasi dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi. Dalam prosesnya enkripsi dan dekripsi memerlukan satu atau beberapa kunci untuk sistem keamanannya. Jika kunci saat proses enkripsi dan dekripsi sama disebut kriptografi simetris dan jika berbeda disebut kriptografi asimetris.

Dalam penelitian ini akan dibahas mengenai salah satu algortitma kriptografi simetris yaitu vigenere cipher. Vigenere chiper merupakan salah satu

algoritma kriptografi klasik untuk menyandikan suatu plaintext dengan menggunakan teknik substitusi. Vigenere cipher pada dasarnya cukup rumit untuk dipecahkan. Meskipun begitu, Vigenere cipher tetap memiliki kelemahan. Salah satunya adalah dapat diketahui panjang kuncinya dengan menggunakan metode kasiski. Hal ini disebabkan karena umumnya terdapat frasa yang berulang-ulang pada ciphertext yang dihasilkan. Untuk mengatasi kelemahan tersebut diperlukan suatu pembaharuan atau modifikasi terhadap algoritma vigenere cipher tersebut. Pada penelitian ini modifikasi yang dilakukan berupa pembuatan kunci baru secara otomatis yang akan membuat panjang kunci sama dengan panjang plain text nya atau bisa disebut dengan key generator, sehingga cipher text nya akan lebih rumit untuk dianalisis.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka rumusan masalah pada penelitian ini adalah bagaimana merancang aplikasi kriptografi menggunakan algoritma modifikasi vigenere cipher dengan key generator?

1.3 Batasan Masalah

Agar skripsi ini sesuai dengan tujuan awal, maka ditentukan batasan masalah - masalah sebagai berikut:

1. Data input dan output berupa teks atau tulisan.
2. Teks yang dienkripsi berupa huruf A-Z dan angka 0 - 9.
3. Aplikasi berupa aplikasi desktop dengan bahasa pemrograman C#.
4. Aplikasi tidak memiliki fitur *save* maupun *backup* dan aplikasi tidak terhubung ke internet.

1.4 Maksud dan Tujuan Penelitian

Adapun maksud dan tujuan yang ingin dicapai dalam penelitian skripsi ini adalah:

1. Membangun suatu aplikasi desktop yang mampu melakukan enkripsi dan dekripsi pada suatu teks.
2. Mengimplementasikan algoritma enkripsi yang telah termodifikasi pada sebuah program.
3. Meningkatkan keamanan dalam merahasiakan suatu pesan.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dapat diperoleh dalam penelitian skripsi ini adalah:

1. Memberikan informasi tentang pengembangan algoritma vigenere cipher agar menjadi lebih aman.
2. Sebagai referensi untuk penelitian selanjutnya.

1.6 Metode Penelitian

Metode yang dipergunakan dalam pengerjaan skripsi ini adalah sebagai berikut:

1.6.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam perngerjaan skripsi ini menggunakan metode studi pustaka yaitu dengan cara mempelajari berbagai referensi atau literatur baik online maupun offline yang berkaitan dengan masalah yang diteliti.

1.6.2 Metode Analisis

Metode analisis yang digunakan adalah metode analisis SWOT dan analisis kebutuhan sistem yang terdiri dari kebutuhan fungsional dan nonfungsional

1.6.3 Metode Perancangan

Metode perancangan yang digunakan adalah dengan menggunakan flowchart dan Unified Modelling Language (UML). Rancangan yang dibuat akan digunakan sebagai dasar untuk pembuatan aplikasi.

1.6.4 Metode Pengembangan

Metode pengembangan aplikasi akan disesuaikan dengan perancangan system yang telah dilakukan sebelumnya. Tahapan ini meliputi coding dan implementasi algoritma ke dalam system.

1.6.5 Metode Testing

Untuk melakukan pengujian terhadap aplikasi yang telah dibuat. Penulis menggunakan metode white box testing dan black box testing.

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini terbagi menjadi 5 bagian utama yaitu sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi uraian mengenai latar belakang, tujuan penelitian, rumusan masalah, batasan masalah, manfaat, metodologi penelitian, dan sistermatika penulisan yang dipergunakan dalam skripsi ini.

BAB II LANDASAN TEORI

Bab ini berisi penjelasan dari teori - teori yang menunjang dan mendukung dalam pembahasan mengenai Perancangan Aplikasi Kriptografi Menggunakan Algoritma Modifikasi Vigenere Cipher Dengan Key Generator.

BAB III ANALISIS DAN PERANCANGAN

Bab ini membahas tentang analisis system, perancangan system, dan tampilan aplikasi.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bagian ini berisi mengenai hasil pengujian dan membahas data-data hasil pengujian yang diperoleh.

BAB V KESIMPULAN DAN SARAN

Bab ini akan menyimpulkan semua kegiatan, hasil-hasil yang diperoleh selama proses pembuatan dan pengujian sistem serta saran-saran yang sekiranya diperlukan untuk menyempurnakan penelitian berikutnya.

DAFTAR PUSTAKA

LAMPIRAN