BAB I
PENDAHULUAN

1.1 Latar Belakang

Kriptografi memiliki berbagai macam algoritma penyandian pesan, baik itu model asimetris maupun simetris. Salah satunya adalah algoritma shift cipher, algoritma ini merupakan salah satu dari berbagai macam algoritma simetris klasik. Shift cipher merupakan salah satu algoritma yang bisa dikatakan memiliki tingkat kekuatan yang rendah sebagai pengamanan suatu pesan. Untuk saat ini algoritma klasik termasuk shift cipher sudah jarang bahkan hampir sudah tidak digunakan lagi karena terlalu sederhana dan banyak algoritma modern yang lebih kompleks dan lebih canggih. Meski begitu bukan berarti algoritma klasik sudah tidak mumpuni lagi untuk digunakan kembali pada zaman modern seperti sekarang ini.

Demi menjamin keamanan dalam bidang kriptografi, sebuah algoritma perlu dilakukan pembaruan dan pengembangan baik dengan cara menciptakan algoritma baru maupun memodifikasi suatu algoritma yang sudah ada. Maka dari itu dilakukanlah modifikasi pada algoritma shift cipher untuk memperkuat tingkat keamanannya agar mampu bersaing dengan algoritma kriptografi modern saat ini. Dimana hal ini diharapkan dapat dijadikan sebagai dasar atau acuan untuk pengembangan algoritma yang lain.

Algoritma shift cipher yang telah dimodifikasi ini dirancang dalam bentuk aplikasi sehingga mampu untuk dipelajari dan difungsikan sebagai pengamanan suatu pesan. Dengan adanya algoritma yang baru, diharapkan keamanan suatu

pesan menjadi lebih terjaga dan sulit untuk diterjemahkan oleh pihak yang tidak bertanggung jawab.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, maka suatu masalah yang dapat didefinisikan adalah bagaimana meningkatkan keamanan dari algoritma shift cipher dengan teknik modifikasi? dan bagaimana merancang aplikasi enkripsi dan dekripsi dengan algoritma modifikasi shift cipher menggunakan pola peredaran darah pada jantung?

1.3 Batasan Masalah

Dari permasalahan tersebut, penulis memberikan batasan sehingga permasalahan tersebut dapat terarah dan tidak menyimpang dari pembahasan utama. Berikut beberapa batasan yang penulis berikan:

1. Algoritma Kriptografi yang digunakan adalah Shift Cipher yang dimodifikasi.
2. Input data berupa teks (hanya huruf dan angka tanpa spasi) dengan panjang diusahakan tidak lebih dari 1000 karakter demi menjaga kinerja aplikasi agar mampu berjalan dengan baik.
3. Aplikasi dibuat menggunakan Bahasa C# dengan *software* Visual Studio 2012.
4. Aplikasi yang dibuat hanya berjalan pada perangkat komputer.
5. 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 penulis capai dalam penelitian ini adalah sebagai berikut:

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

1.5 Metode Penelitian

Dalam penelitian ini penulis menggunakan beberapa metode untuk mendapatkan informasi dan menyusun laporan agar mendapatkan hasil yang mudah dimengerti dan sesuai dengan tujuan penelitian. Metode yang penulis gunakan adalah sebagai berikut:

1.5.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan pada skripsi ini menggunakan metode studi literatur, yaitu teknik pengumpulan data dengan membaca buku – buku pustaka maupun dari internet yang merupakan penunjang dalam memperoleh data untuk menyusun laporan yang berhubungan dengan masalah yang dibahas.

1.5.2 Metode Analisis

Adapun metode analisis yang digunakan adalah metode analisis sistem dan analisis kebutuhan sistem yang terdiri dari kebutuhan fungsional dan non-fungsional.

1.5.3 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.

1.5.4 Metode Pengembangan

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

1.5.5 Metode Testing

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

1.6 Sistematika Penulisan

Sistematika yang digunakan dalam penyajian laporan penulisan isi masing-masing bab diuraikan sebagai berikut:

BAB I PENDAHULUAN

Bab ini menguraikan tentang latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini memuat tinjauan pustaka teori yang disajikan dalam landasan teori yang mendukung pembuatan aplikasi.

BAB III ANALISA DAN PERANCANGAN SISTEM

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

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini berisi tentang implementasi atau pembuatan aplikasi berdasar rancangan yang sebelumnya telah dibuat.

BAB V PENUTUP

Bab ini diuraikan kesimpulan dari hasil pembuatan aplikasi dan saran tentang pengembangan aplikasi untuk tahap selanjutnya di masa mendatang.