BAB I PENDAHULUAN

1.1 Latar Belakang

Kemajuan dan perkembangan teknologi informasi yang telah berkembang dengan sangat baik, telah membantu kehidupan umat manusia. Bidang komunikasi adalah salah satu contoh bidang yang menjadi pehatian saat ini. Internet hadir, dan komunikasi jarak jauh dapat dilakukan dengan mudah, cepat dan kini menjadi murah. Namun di lain pihak, ternyata Internet tidak aman karena merupakan media komunikasi umum yang digunakan oleh siapapun, sehingga sangat rawan keamanannya terhadap penyerangan ke dalam sistem keamanan informasi oleh pihak-pihak yang tidak berhak untuk mengetahui setiap rahasia komunikasi.

Penyerangan terhadap data di dunia maya tidak dapat dicegah, tetapi kita dapat untuk memperlambat penyerangan terhadap pencurian, perusakan dan lain sebagainya. Salah satu caranya dengan menyandikan isi informasi menjadi suatu kode-kode yang tidak dimengerti sehingga apabila disadap maka akan kesulitan untuk mengetahui isi informasi yang sebenarnya.

Metode penyandian pertama kali dibuat masih menggunakan metode algoritma rahasia yaitu sebuah algoritma yang tingkat keamanannya diperoleh dengan menyembunyikan secara rahasia bagaimana algoritma itu

bekerja. Namun metode ini tidak efisien saat digunakan untuk berkomunikasi dengan banyak orang karena seseorang harus menggunakan algoritmanya sendiri, dan jika algoritma ini diketahui orang lain, maka algoritma ini harus diganti dengan yang baru, dan kelemahan lainnya adalah tidak memungkinkannya standarisasi sebagai kendala mutu, karena setiap kelompok pengguna harus mempunyai algoritmanya sendiri-sendiri. Sebagai contoh algoritma rahasia digunakan oleh Julius Caesar, dikenal dengna nama Caesar cipher dimana tiap huruf didistribusikan dengan huruf berikutnya. Contoh :"*Fly at once*" menjadi "*Gmz bu podf*". Oleh karena itu penggunaan algoritma rahasia mulai ditinggalkan dan dikenalkan suatu metode baru yang disebut dengan algoritma kunci atau *Public Key Encryption.*

1.2 Rumusan Masalah

1. Bagaimana menerapkan konsep – konsep pembentukan kunci pada setiap masing – masing *Public Key Encryption* ?
2. Bagaimana cara membandingkan efisiensi kecepatan, *LOC*, dan s*ize* dari ketiga teknik penyandian(Rabin, ElGamal, dan McEliece)?

1.3 Tujuan

Tujuan dari pembahasan ini yaitu :

1. Merancang dan membuat aplikasi dengan menerapkan teknik-teknik *Public-Key Encryption* (McEliece,ElGamal, dan Rabin)

2. Menganalisis efisiensi dari algoritma tersebut, yang dilihat dari segi kecepatan enkripsi, banyaknya karakter yang dikodekan, dan besarnya ukuran dari file yang dihasilkan.

1.4 Ruang Lingkup Proyek

Aplikasi ini membuat sebuah enkripsi sebuah pesan atau gambar dengan menggunakan Public-Key Encryption dengan teknik ElGamal, McEliece, dan Rabin. Pembahasan hanya mencakup dua buah tujuan kriptografi yaitu kerahasiaan dan integritas data.

1.5 Definisi, Akronim, dan Singkatan

Tabel I.1 Definisi, Akronim, dan Singkatan

OOP	*Object Oriented Programing*
SRS	*Software Requirement Spesification*
UML	*Unified Modeling Language*
C#	*C Sharp*
Encryption	Penyandian sesuatu dengan menggunakan aturan tertentu.
Decryption	Pengembalian terhadap suatu bentuk yang telah disandikan dengan menggunakan aturan tertentu

1.6 Overview Laporan

Dalam karya tulis ini pembahasan materi disusun menjadi lima bab. Materi tersebut disajikan dengan sistematika sebagai berikut ini.

BAB 1 PENDAHULUAN

Pada bab ini akan dibahas mengenai latar belakang, perumusan masalah, tujuan, batasan masalah, dan sistematika pembahasan.

BAB 2 LANDASAN TEORI

Pada bab ini menggambarkan fitur-fitur yang akan dibuat pada perangkat lunak, sehingga semua persyaratan, fungsionalitas, dan kemampuan perangkat lunak dapat dipaparkan dengan sangat jelas sesuai dengan apa yang telah dijelaskan pada BAB 1.

BAB 3 SPESIFIKASI PRODUK

Pada bab ini akan dibahas mengenai teori- teori yang melandasi fungsi – fungsi matematis dan mengenai Kriptografi itu sendiri. Akan dijelaskan pula isi dari desain-desain produk secara lengkap dan menggambarkan pemikiran penulis bagaimana perangkat lunak akan dibangun dengan memperhatikan beberapa faktor.

Faktor-faktor yang termasuk didalamnya, yaitu:

a. Rancangan *UML*
b. Rancangan antarmuka

Bagian-bagian tersebut akan dijabarkan lagi lebih mendetail dan terstruktur pada bab ini.

BAB 4 PENGEMBANGAN SISTEM

Pada bab ini menjelaskan bagaimana sebuah desain yang telah disusun secara terstruktur dan jelas menjadi sebuah produk yang dapat diimplementasikan. Bagian ini juga berisikan *screenshot* dari aplikasi dan keterangannya.

BAB 5 TESTING dan EVALUASI SISTEM

Pada bab ini berisikan tentang implementasi dan pengujian terhadap program. Dan juga berisikan hasil dari evaluasi dari pengujian program tersebut.

BAB 6 KESIMPULAN dan SARAN

Pada bab ini berisikan uraian singkat produk yang dihasilkan berdasarkan pembuatan. Saran berisi hal-hal apa saja yang dapat dikembangkan untuk memberikan kemampuan lebih kepada produk yang dibangun baik secara teknis maupun dokumentasi.

1.7 Gambaran Keseluruhan

Gambaran keseluruhan dari produk adalah deskripsi produk secara umum. Gambaran keseluruhan terdiri dari perspektif produk, fungsi produk, karakteristik target pengguna produk, batasan-batasan produk, asumsi dan ketergantungan.

1.7.1 Perspektif Produk

Aplikasi ini merupakan aplikasi *desktop* dan bersifat *stand-alone*.Aplikasi ini dibuat untuk membantu menyandikan sebuah pesan atau gambar dengan menggunakan algoritma tertentu.

1.7.2 Fungsi Produk

Fungsi –fungsi utama yang terdapat dalam aplikasi ini adalah:

1. Pengkodean menggunakan algoritma enkripsi kunci-publik yang dapat dipilih antara lain adalah ElGamal, McEliece, atau Rabin.
2. Pembuatan algoritma pembangkit kunci.
3. Enkripsi, Dekripsi pesan dan gambar dengan teknik Rabin
4. Enkripsi, Dekripsi pesan dan gambar dengan teknik ElGamal
5. Enkripsi, Dekripsi pesan dan gambar dengan teknik McEliece
6. Efisiensi perbandingan algoritma (waktu, LOC, dan ukuran).
7. Hasil analisa.

1.7.3 Karakterisitik Pengguna

Pengguna dari aplikasi ini adalah pengguna yang membutuhkan pengamanan sebuah pesan dengan menggunakan *Public-Key* dengan menggunakan algoritma tertentu. Pengguna sistem hanya butuh mengerti cara menggunakan aplikasi yang dibuat ini dan memiliki sedikit pengetahuan dalam penggunaan suatu aplikasi.

1.7.4 Batasan – Batasan

Batasan-batasan aplikasi dapat ditinjau dari beberapa sisi, diantaranya yaitu:

1. Tipe permasalahan dibatasi hanya pada penggunaan algoritma ElGamal, McEliece, dan Rabin.
2. Penyandian dibentuk berdasarkan proses matematis yang mendasari pembentukan tiap algoritma
3. Suatu gambar hanya dibatasi dalam ukuran maksimum 8000px
4. Suatu pesan hanya dibatasi maksimal 1000 karakter
5. Keluaran yang dihasilkan adalah barisan kode hasil penyandian

1.7.5 Asumsi Ketergantungan

Asumsi-asumsi agar aplikasi ini dapat berjalan dengan baik adalah sebagai berikut:

1. Perangkat komputer yang mendukung *.NET Framework 2.0* atau versi yang lebih tinggi.

1.8 Time Schedule

Tabel I.2 Time Schedule

	Januari		Febuari				Maret				April				Mei		
	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3
Analisis																	
Desain																	
Coding																	
Testing																	
Laporan																	