BAB I

PENDAHULUAN

I.1. Latar Belakang

Di era modern seperti saat ini, data atau informasi yang bersifat penting dan rahasia telah menjadi suatu hal yang sangat berharga. Data atau informasi tersebut tentunya akan menimbulkan resiko dan masalah apabila diakses oleh pihak-pihak yang tidak berhak (*unauthorized person).* Oleh sebab itu pengamanan data dan informasi tersebut sudah menjadi hal yang penting untuk diperhatikan. Berbagai cara telah banyak dikembangkan untuk melindungi data dan informasi tersebut, misalnya kriptografi *(cryptography).*

Kriptografi adalah suatu teknik pengkodean atau penyandian suatu data dan informasi (pesan) menjadi suatu data ataupun kode-kode tertentu yang sulit dimengerti, yaitu dengan merubah data asli *(plain text)* ke dalam bentuk data tersandi *(cipher text)* atau disebut proses enkripsi *(encrypt).* Data yang telah dirubah tadi dapat dikembalikan ke dalam bentuk semula atau disebut proses dekripsi *(decrypt)* dengan menggunakan kunci *(key)* yang dimiliki oleh pihak-pihak yang sah dan berhak saja *(authorized person).*

Saat ini telah banyak bermunculan berbagai macam algoritma kriptografi yang tentunya masing-masing algoritma tersebut dapat menjamin keamanan data dan informasi apabila diterapkan dengan baik. Contohnya algoritma *gronsfeld cipher* dan *RC4*. Algoritma *gronsfeld* dan *RC4* merupakan algoritma simetris dimana algoritma ini memanfaatkan bentuk kunci yang sama dalam proses

enkripsi dan dekripsi. Penerapannya dapat dilakukan dimana saja, misalnya penerapan keamanan dalam berkomunikasi.

Komunikasi merupakan suatu kebutuhan yang sangat penting dan tidak bisa dilepaskan dari manusia. Manusia selalu ingin berhubungan dengan manusia lain bahkan dengan lingkungannya. Pada umumnya komunikasi dilakukan secara lisan atau verbal dan secara tertulis yang dapat dimengerti oleh kedua belah pihak, namun terdapat juga cara berkomunikasi dalam bentuk lainnya, yaitu dengan bahasa isyarat tubuh dan gerak-gerik tubuh, ini disebut komunikasi nonverbal.

Saat ini terdapat berbagai macam cara berkomunikasi tertulis yang sering digunakan oleh manusia. Misalnya, berkirim pesan via *internet* atau biasanya disebut dengan *chatting. Chatting* umumnya terdapat pada layanan berkomunikasi nirkabel yang sangat cepat dan efisien, sehingga *chatting* sangat populer untuk digunakan dari pada cara berkomunikasi lainnya misalnya surat menyurat. Layanan *chatting* yang populer ialah yang terdapat pada *Facebook. Facebook* merupakan media sosial yang populer saat ini dan terdapat sebuah fitur berkomunikasi yang diberi nama *Facebook messenger.* Terkadang keamanan dalam berkirim pesan melalui *Facebook messenger* ini menjadi hal yang tidak terlalu penting, bisa saja isi dari percakapan yang mungkin saja penting dapat diakses dan dibaca oleh pihak-pihak yang tidak bertanggung jawab.

Penulis disini mencoba merancang suatu perangkat lunak yang didalamnya terdapat fitur *messenger* seperti pada *Facebook* pada umumnya, namun didalam perangkat lunak ini terdapat sistem keamanan menggunakan teknik kriptografi yang dapat diaplikasikan kedalam *messenger* tersebut, dan diharapkan dapat

memberikan cukup keamanan dalam berkomunikasi yang memanfaatkan *messenger* pada media sosial *Facebook* tersebut.

Dari latar belakang diatas maka penulis mengangkat judul **"Perancangan Perangkat Lunak Sistem Pengamanan *Messenger* pada Media Sosial *Facebook* dengan Kombinasi Algoritma Kunci Simetris *Gronsfeld Cipher* dan *RC4*".**

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Berdasarkan penjalasan latar belakang diatas maka identifikasi masalah yang akan dibahas yaitu:

1. Pengamanan pesan teks didalam *messengger* pada media sosial *Facebook.*
2. Mengaplikasikan teknik kriptografi kedalam *messenger* pada media sosial *Facebook* tersebut agar pesan teks tidak dapat diakses dan dibaca oleh pihak-pihak yang tidak bertanggung jawab.

I.2.2. Perumusan Masalah

Berdasarkan identifikasi masalah diatas, maka penulis merumuskan masalah tersebut kedalam rumusan masalah. Adapun rumusan masalah adalah sebagai berikut :

1. Bagaimana merancang suatu perangkat lunak sistem untuk pengamanan pesan teks didalam *messenger* pada media sosial *Facebook* ?

2. Bagaimana cara berkomunikasi menggunakan *messenger* pada media sosial *Facebook* dengan memanfaatkan teknik kriptografi agar pesan teks tersebut aman dari pihak-pihak yang tidak bertanggung jawab ?

I.2.3. Batasan Masalah

Adapun batasan masalah yang penulis sajikan yaitu hanya membahas tentang:

1. Pengamanan dalam berkomunikasi hanya dalam bentuk teks (*string*) dengan memanfaatkan *messenger* pada media sosial *Facebook.*
2. Mengimplementasikan teknik kriptografi kunci simetri *gronsfeld cipher* dan *RC4* kedalam *messenger* pada media sosial *Facebook.*
3. Pembuatan kunci rahasia Algoritma *RC4* menggunakan hasil pengkodean algoritma *gronsfeld cipher*.
4. Algoritma RC4 menggunakan versi 4 *byte* sesuai kebutuhan sistem yang terbatas, tidak mendukung beberapa bentuk *unicode* dan adanya pemotongan *ciphertext* (baris baru) apabila pesan terlalu panjang.
5. Menggunakan software *Visual Basic.Net 2010* untuk membangun *interface* dan program yang berhubungan dengan rumusan masalah diatas.
6. Pengguna sistem ini harus sudah mempunyai *account facebook* yang sudah aktif.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Tujuan dari penelitian terhadap masalah yang penulis angkat adalah sebagai berikut :

1. Memberikan keamanan (*security*) terhadap pesan yang dikirim melalui *messenger* pada media sosial *Facebook* tersebut agar tidak dapat dibaca oleh pihak-pihak yang tidak betanggung jawab.
2. Memberikan penjelasan cara kerja teknik kriptografi untuk mengamankan pesan teks dalam proses berkomunikasi khususnya penerapan algoritma *gronsfeld cipher* dan *RC4*.

I.3.2. Manfaat

Adapun manfaat dari penelitian terhadap masalah yang penulis angkat yaitu:

1. Agar pesan teks yang dikirimkan melalui *messenger* pada media sosial *Facebook* ini tidak dapat dibaca oleh pihak-pihak yang tidak bertanggung jawab.
2. Memberikan pengetahuan dan wawasan kepada penulis dan pembaca mengenai manfaat berkomunikasi secara aman, yaitu menggunakan teknik kriptografi dalam berkomunikasi.
3. Memberikan pengetahuan tentang algoritma kunci simetris, khususnya algoritma *gronsfeld cipher* dan *RC4.*

I.4. Metodologi Penelitian

Untuk dapat mengimplementasikan sistem di atas, maka secara garis besar digunakan beberapa metode sebagai berikut:

I.4.1 Metode Pengumpulan Data

a. Studi Literatur

   Dengan mempelajari buku-buku acuan dan literatur yang berhubungan dengan materi dan permasalahan yang diangkat dalam penulisan skripsi.

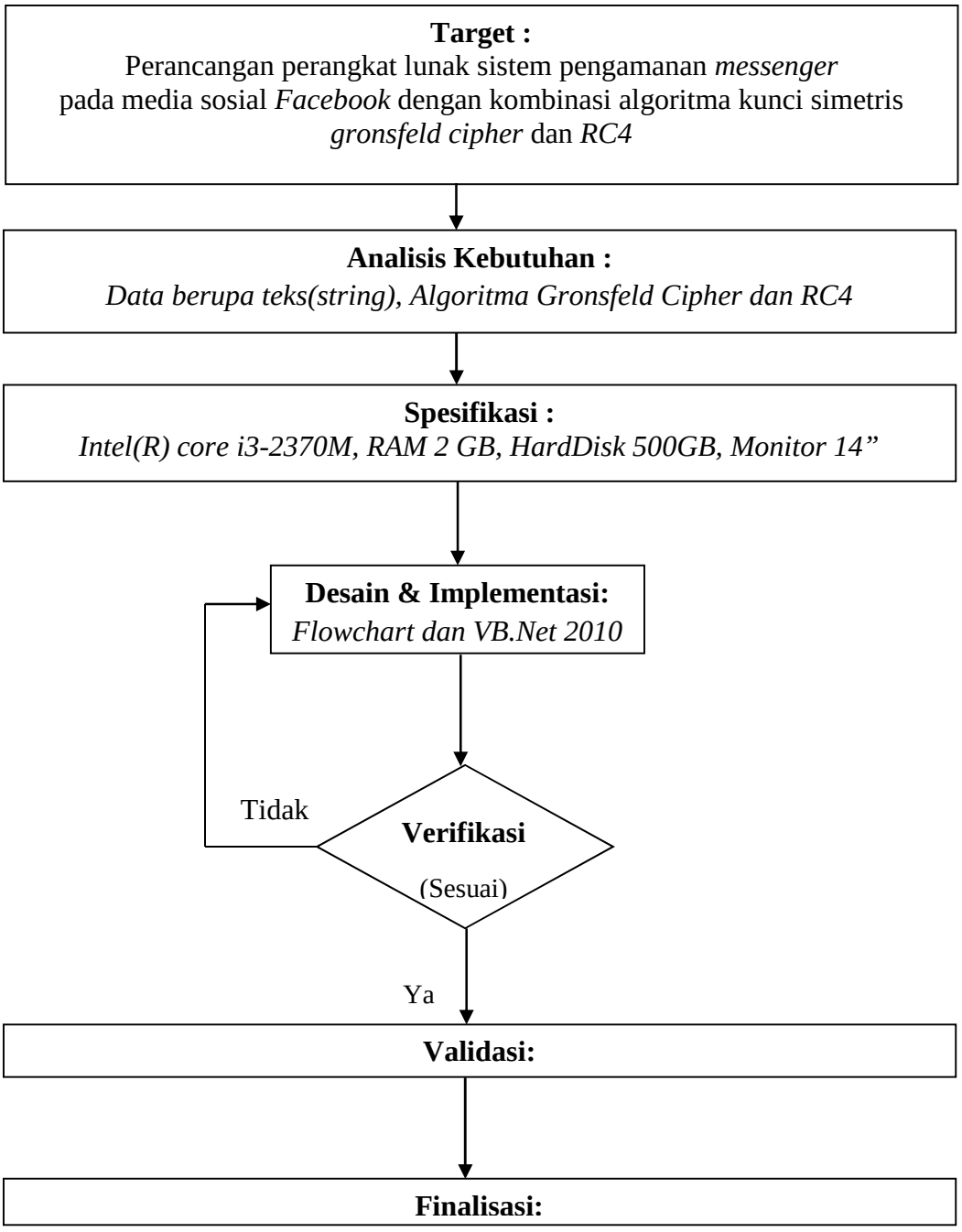
b. Studi Lapangan

   Mengumpulkan informasi dan mempelajari tentang cara kerja teknik kriptografi khususnya algoritma *gronsfeld cipher* dan *RC4* serta implementasinya dalam hal berkomunikasi.

I.4.2 Metode Perancangan Sistem

a. Prosedur Perancangan

Langkah-langkah yang harus diperhatikan dan diperlukan agar mencapai tujuan perancangan dapat dilihat dalam Gambar.1 berikut:



Gambar: I.1 Prosedur Perancangan Sistem

b. Analisis Kebutuhan

Suatu perangkat lunak dirancang agar dapat mudah dimengerti oleh pengguna (*user*). Didalam merancang suatu perangkat lunak harus jelas dan tepat sasaran. Tahap analisis adalah tahapan pengumpulan kebutuhan dari semua elemen sistem perangkat lunak yang akan dibuat.

Adapun analisis kebutuhan dalam rancangan sistem yang akan dibangun adalah sebagai berikut:

1. Data atau informasi apa yang akan diproses merupakan data langkah pembuatan aplikasi ini hanya berupa teks (*string).*
2. Program yang dirancang merupakan aplikasi menggunakan menggunakan algoritma *gronsfeld cipher* dan algoritma *RC4*

c. Spesifikasi Kebutuhan Sistem

Dalam merancang perangkat lunak ini, penulis menggunakan spesifikasi perangkat keras *(hardware)* dan perangkat lunak *(software)* sebagai berikut :

1. Perangkat keras *(hardware)*

   Perangkat keras *(hardware)* yang digunakan yaitu :

   a. *Processor*: Intel(R) Core(TM) i3-2370M CPU @ 2.40GHz (4 CPUs), ~2.4GHz.
   b. RAM 2GB.
   c. *Monitor* LCD 14 “
   d. *Hardisk* 500GB

e. *Keyboard & mouse*

f. *Modulator-demulator* (Modem)

2. Perangkat lunak *(software)*

Perangkat lunak *(software)* yang digunakan yaitu :

a. *Operating System*: Windows 7 Ultimate 64-bit

b. Microsoft *Visual Basic.Net* 2010

d. Desain dan implementasi

Setelah spesifikasi, selanjutnya dilakukan tahapan desain atau pembuatan aplikasi, yaitu merancang bagaimana suatu aplikasi seharusnya berjalan. Sedangkan, implementasi merupakan tahap pengkodean, dimana aplikasi dijalankan sesuai dengan rancangan yang telah didesain sebelumnya menggunakan bahasa pemrograman dengan menggunakan *software Visual Basic.Net 2010* sebagai perancangan *interface* dan program.

e. Verifikasi

Verifikasi program merupakan tahap yang digunakan untuk menjamin kebenaran suatu program. Metode ini mencegah terjadinya kesalahan dengan memberikan jaminan kebenaran berdasarkan komputasi matematis dalam bentuk program.

f. Validasi

Selanjutnya dilakukan pengujian aplikasi secara menyeluruh. Setelah melewati tahap validasi dan sistem telah berjalan dengan baik sesuai dengan kebutuhan dam target dari aplikasi yang dirancang.

I.5. Sistematika Penulisan

Berikut ini adalah sistematika penulisan skripsi dari masalah yang penulis angkat yaitu:

BAB I : PENDAHULUAN

Pada bab ini, berisikan dasar pemikiran penulis yang kemudian diangkat menjadi judul skripsi, terdiri dari latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metodologi penelitian serta sistematika penulisan.

BAB II : LANDASAN TEORI

Pada bab ini, berisikan teori-teori penunjang dan berkaitan langsung penulisan skripsi. Didalamnya terdapat studi literatur yang didalamnya terdapat masalah yang diangkat.

BAB III : ANALISIS DAN DESAIN SISTEM

Pada bab ini, berisikan strategi penyelesaian masalah dalam bentuk analisis masalah, penerapan metode/algoritma, desain sistem, desain *user interface*.

BAB IV : HASIL DAN UJI COBA

Pada bab ini, berisikan tampilan hasil sistem/perangkat lunak yang telah selesai dibangun dengan implementasi rancangan sistem baru. Menampilkan hasil uji coba, apakah sesuai dengan apa yang penulis inginkan pada bab-bab sebelumnya.

BAB V : KESIMPULAN DAN SARAN

Berisikan kesimpulan dari penelitian dan hasil akhir dari pemecahan masalah yang didefinisikan pada Bab I dan berisikan hal-hal (kelemahan sistem yang dibangun) yang dianggap penting untuk diperhatikan atau dijalankan pada masa yang akan datang untuk kesempurnaan hasil penelitian/pemecahan masalah, sehingga masalah serupa tidak terjadi lagi serta antisipasi terhadap timbulnya masalah lain.