BAB I

PENDAHULUAN

I.1. Latar Belakang

Penyandian sebuah informasi merupakan suatu hal yang harus diperhatikan. Masalah tersebut penting karena jika sebuah informasi dapat di akses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan.

Kriptografi hadir untuk meningkatkan aspek penyandian pesan. Hal ini dilakukan dengan menyandikan pesan ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Di dalam kriptografi, algoritma yang menentukan bagaimana pesan asal yang dapat dimengerti (*plaintext*) diubah menjadi pesan acak (*ciphertext*) dan selanjutnya diubah kembali menjadi pesan asal tidak dapat dirahasiakan karena pihak-pihak yang berhak mengetahui pesan asal dapat berubah sewaktu-waktu. Jika algoritma dirahasiakan, algoritma harus berubah setiap terjadi pergantian pihak yang terlibat.

Masalah penyandian dan kerahasiaan pesan merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi. Apalagi jika pesan tersebut berada dalam suatu jaringan komputer yang terhubung/terkoneksi dengan jaringan lain. Hal tersebut tentu saja akan menimbulkan resiko bilamana informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak. Yang mana jika hal Tersebut sampai terjadi, kemungkinan besar akan merugikan

bahkan membahayakan orang yang mengirim pesan atau menerima pesan, maupun organisasinya. Informasi yang terkandung di dalamnya pun bisa saja berubah sehingga menyebabkan salah penafsiran oleh penerima pesan. Selain itu pesan yang dibajak tersebut akan memiliki kemungkinan rusak bahkan hilang yang akan menimbulkan kerugian material yang besar.

Merkle Hellman digunakan subset masalah untuk membuat *Cryptosystem* untuk mengenkripsi pesan, *Superincreasing* S ransel vektor diciptakan dan Properti superincreasing tersembunyi dengan membuat kedua vektor M oleh perkalian Modular dan permutasi, Vektor M adalah kunci umum *cryptosystem* dan S digunakan untuk mendekripsi pesan. Kelebihan algoritma ini adalah proses pendistribusian kunci pada media yang tidak aman seperti internet, tidak memerlukan kerahasian. Karena kunci yang didistribusikan adalah kunci publik. Sehingga jika kunci ini sampai hilang atau diketahui oleh orang lain yang tidak berhak, maka pesan sandi yang dikirim akan tetap aman. Sedangkan kunci private tetap disimpan (tidak didistribusikan)

Chatting adalah aktivitas berkomunikasi yang dilakukan oleh dua orang atau lebih dengan memanfaatkan aplikasi chatting dan jaringan internet. Aplikasi chatting saat ini sudah sangat maju. Tidak hanya mengirim pesan teks saja, aktivitas chatting sekarang ini juga bisa mengirimkan emoticon, pesan suara, bahkan video. “Chatting” merupakan salah fitur dari kecanggihan teknologi informasi saat ini. Mulai dari anak kecil hingga orang dewasa saat ini sudah familiar dengan istilah chatting. Singkatnya, pengertian chatting adalah suatu program yang melibatkan koneksi internet untuk saling bertukar pesan antar satu

orang dengan orang lain. Chatting adalah bentuk komunikasi yang paling efektif dan efisien sata ini.

Permasalahan yang terjadi pada saat melakukan penelitian yaitu masih lemahnya sistem keamanan data terutama dalam pengamanan pesan chat dan berkembangnya tindakan penyalahgunaan informasi sehingga diperlukan pengembangan teknik keamanan yang dapat memberikan proteksi lebih baik agar kerahasiaan pesan terjaga.

Alasan penulis mengambil judul penelitian "**Aplikasi Penyandian Pesan Chatting Menggunakan Metode Merkle Hellman**" karena tidak adanya implementasi algoritma *Merkle Hellman* dalam pengembangan aplikasi pengamanan pesan chat.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Sehubungan dengan permasalahan yang ada maka penulis mencoba untuk mengidentifikasi masalah adalah :

1. Masih lemahnya sistem keamanan data terutama dalam pengamanan pesan chat.
2. Berkembangnya tindakan penyalahgunaan informasi sehingga diperlukan pengembangan teknik keamanan yang dapat memberikan proteksi lebih baik agar kerahasiaan pesan terjaga.

I.2.2. Perumusan Masalah

Berdasarkan identifikasi yang ditemukan oleh penulis dalam melakukan penelitian ini, maka perumusan masalah dapat dirumuskan sebagai berikut :

1. Bagaimana merancang sebuah aplikasi yang memiliki sistem penyandian pesan yang aman ?
2. Bagaimana melakukan implementasi algoritma *Merkle Hellman* terhadap sebuah sistem pengiriman file teks ?

I.2.3. Batasan Masalah

Batasan masalah pada penelitian ini yaitu :

1. Pesan untuk masukan sistem yaitu teks, pesan kunci, pesan *cipher.*
2. Bahasa pemrograman yang digunakan untuk membuat aplikasi yaitu java
3. Pemodelan sistem dilakukan dengan UML 2.0.
4. Jenis teks yang akan di enkrip adalah jenis font teks.
5. Tidak membahas video dan gambar
6. Tidak membaca jenis simbol tertentu

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Tujuan penelitian ini yaitu :

1. Merancang sebuah aplikasi dengan memanfaatkan sistem penyandian informasi pesan yang dapat menjaga kerahasiaan dan penyandian informasi pesan.

2. Merancang dan membangun sebuah aplikasi penyandian pesan atau dengan dengan menggunakan Algoritma *Merkle Hellman*

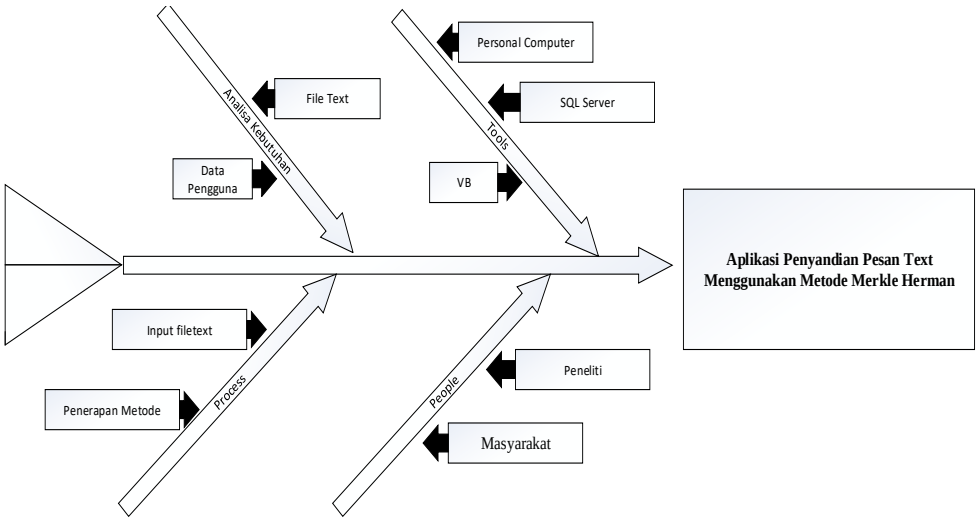
I.3.2. Manfaat

Manfaat penelitian ini yaitu :

1. Aplikasi penyandian pesan dengan memanfaatkan sistem penyandian pesan dapat menjaga kerahasiaan dan penyandian pengiriman pesan pada aplikasi penyandian pesan sehingga pengirim pesan dapat merasa nyaman dan aman dalam melakukan transfer pesan atau pesan
2. Implementasi Algoritma *Merkle Hellman* terhadap aplikasi penyandian pesan dirancang untuk penggunaan memori yang seminimal mungkin dengan kecepatan proses yang maksimal

I.4. Metodologi Penelitian

Untuk menganalisa pesan tersebut di atas maka digunakan alur analisis yang disusun dengan langkah – langkah berbentuk diagram alir seperti di bawah ini :



Gambar I.1. Prosedur Perancangan Sistem

Dari gambar diatas dapat dijelaskan sebagai berikut :

1. Perencanaan sistem

   Manfaat dari tahapan ini adalah untuk menentukan masalah-masalah atau kebutuhan yang timbul. Hal ini memerlukan pengembangan sistem secara menyeluruh agar ada usaha lain yang dapat di lakukan untuk memecahkan masalah tersebut. Adapun masalah yang timbul adalah :

   a. Tidak adanya sistem penyandian pesan yang aman pada penyimpanan pesan.
   b. Belum berkembangnya algoritma *Merkle Hellman* dalam sistem penyandian pesan.

2. Analisa Sistem.

   Tahap analisa bertitik tolak pada kegiatan-kegiatan dan tugas-tugas dimana sistem yang berjalan di pelajari lebih mendalam, konsepsi dan usulan dibuat untuk menjadi landasan bagi sistem yang baru yang akan dibangun.

a. Pesan yang digunakan dalam penelitian ini diperoleh dari file teks, alamat ip, nomor port komputer, pesan kunci, pesan cipher.
b. Bahasa pemrograman yang digunakan untuk membuat aplikasi adalah *visual basic*.

3. Pengumpulan pesan

   Pengumpulan pesan adalah cara-cara yang dapat digunakan oleh peneliti untuk mengumpulkan pesan. Instumen sebagi alat bantu dalam menggunakan methode pengumpulan pesan merupakan sarana yang dapat diwujudkan dalam benda, misalnya angket, perangkat tes, pedoman observasi, skala dan sebaginya.

4. Desain (Perancangan) Sistem Secara Umum.

   Pada tahap ini akan membahas mengenai desain sistem yang digunakan oleh penulis, membahas mengenai aplikasi-aplikasi yang digunakan dalam pembuatan desain program.

   a. Bahasa pemrograman yang digunakan untuk membuat aplikasi adalah *visual basic*
   b. PC dengan *Processor* corei3 1,6 Ghz, Memori 1,5GB, Kartu Grafik 512 MB

5. Desain (Perancangan) Sistem Secara Terinci

   Pada tahap ini sebagian besar kegiatan yang berorientasi ke komputer dilaksanakan. Spesifikasi perangkat keras dan perangkat lunak yang telah disusun pada tahap sebelumnya ditinjau kembali dan disempurnakan. Rencana pembutan program dilaksakan dan juga testing programnya. Testing

program menggunakan metode *blackbox testing*. *Black box testing* adalah pengujian yang dilakukan hanya mengamati hasil eksekusi melalui pesan uji dan memeriksa fungsional dari perangkat lunak. Jadi dianalogikan seperti kita melihat suatu koatak hitam, kita hanya bisa melihat penampilan luarnya saja, tanpa tau ada apa dibalik bungkus hitam nya. Sama seperti pengujian black box, mengevaluasi hanya dari tampilan luarnya (*interface* nya), fungsionalitasnya.tanpa mengetahui apa sesungguhnya yang terjadi dalam proses detilnya (hanya mengetahui *input* dan *output*).

6. Implementasi Sistem

   Analisis Penyandian Pesan teks melalui websocket menggunakan algoritma *Merkle Hellman*yang telah dirancang oleh penulis membutuhkan implementasi metode untuk menyempurnakan penyandian pesan, metode yang digunakan oleh penelitian adalah *Algoritma Merkle Hellman*

7. Pemeliharaan Sistem

   Tujuan tahapan ini adalah untuk melakukan evaluasi sistem secara tepat dan efisien, menyempurnakan proses pemeliharaan sistem dengan selalu menganalisa kebutuhan informasi yang dihasilkan sistem tersebut

I.5. Konstribusi Penelitian

Konstribusi dari penelitian ini yaitu aplikasi penyandian pesan dengan memanfaatkan sistem penyandian pesan dapat menjaga kerahasiaan dan penyandian pengiriman pesan pada aplikasi penyandian pesan sehingga pengirim pesan dapat merasa nyaman dan aman dalam melakukan transfer pesan atau pesan

Implementasi Algoritma *Merkle Hellman* terhadap aplikasi penyandian pesan dirancang untuk penggunaan memori yang seminimal mungkin dengan kecepatan proses yang maksimal.

I.6. Sistematika Penulisan

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

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode 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 yaitu berupa pembahasan mengenai sistem keamanan.

BAB III : ANALISIS DAN PERANCANGAN

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 program yang dirancang serta kelebihan dan kekurangan sistem yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan di masa yang akan pesanng untuk sistem.