BAB I

PENDAHULUAN

I.1. Latar Belakang

Penyampaian pesan antar sesama manusia sangat penting di dalam kehidupan sehari-hari dan sudah merupakan kebiasaan yang dilakukan semua orang. Penyampaian pesan tidak hanya dilakukan dengan berbicara dengan bertatap muka, penyampaian pesan juga dapat dilakukan dengan menggunakan media-media elektronik yang digunakan misalnya *handphone*, komputer dan lain sebagainya. Pertukaran pesan menggunakan komputer dapat dilakukan dengan aplikasi *chatting*. Pertukaran menggunakan komputer membutuhkan lebih dari satu perangat komputer dan membutuhkan sebuah jaringan komputer untuk menghubungkan beberapa komputer tersebut. Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya (*printer*, CPU), berkomunikasi (surel, pesan instan), dan dapat mengakses informasi (peramban *web*). Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (*service*). (Syahib, dkk, 2017 : 197). Namun dalam pertukaran informasi menggunakan aplikasi *chatting* sangat rentan terhadap pencurian pesan, sebab pesan yang dikirim tidak memiliki keamanan tambahan, sehingga pesan yang dikirm dapat dengan mudah dicuri dan dibaca oleh pihak yang tidak diinginkan. Pengiriman lewat jaringan WLAN juga sangat rentan untuk dicuri oleh para pencuri informasi, pencuri dapat menyusup melalui alamat IP

yang masih kosong. Oleh karena itu perlu adanya keamanan saat pengiriman pesan *chatting* menggunakan sebuah teknik.

Teknik yang dapat digunakan adalah kriptografi. Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "Applied Cryptography", kriptografi adalah ilmu pengetahuan dan seni menjaga *message-message* agar tetap aman (*secure*). Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. (Azis, 2017 : 73). Namun untuk dapat menggunakan teknik kriptografi dibutuhkan sebuah metode. Metode yang peneliti gunakan yaitu *Hill Cipher*. *Hill Cipher* merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. (Pangaribuan dan Simbolon, 2017 : 3). Namun pada penelitian ini peneliti menambahkan metode *Caesar Cipher* pada hasil penyandian metode *Hill Cipher* sehingga penyandiannya menjadi lebih kuat dan lebih baik. *caesar cipher* merupakan teknik penyandian pertama di dunia dengan menggunakan teknik substitusi. Algoritma klasik ini juga dikenal dengan algoritma ROT3 Pada awalnya teknik ini digunakan oleh Julius Caesar untuk berkomunikasi dengan tentaranya di garis depan. Agar pesannya aman, Caesar melindungi data yang dikirim dengan melakukan pergeseran pada setiap huruf dalam pesannya atau pun mengubah huruh menjadi angka. (Rachman, 2018 : 122). Dengan latar belakang tersebut maka penulis menyimpulkan judul

"Penerapan Metode *Hill Cipher* Dan *Caesar Cipher* Pada Aplikasi *Wireless* LAN *Chatting*"

I.2. Ruang lingkup Permasalahan

Ruang lingkup permasalahan yang dapat diberikan untuk penelitian ini adalah sebagai berikut :

I.2.1. Identifikasi Masalah

Identifikasi masalah berdasarkan latar belakang yang telah dijelaskan di atas adalah sebagai berikut :

1. Tidak adanya keamanan pertukaran pesan *chatting* berbasis WLAN.
2. Dibutuhkan penerapan metode *Hill Cipher* dan *Caesar Cipher* untuk keamanan pesan *chatting* berbasis WLAN.
3. Dibutuhkan aplikasi yang dapat memberikan keamanan pesan *chatting* berbasis WLAN.

I.2.2. Perumusan Masalah

Perumusan masalah pada penelitian ini yaitu :

1. Bagaimana memberikan keamanan pesan *chatting* berbasis WLAN ?
2. Bagaimana penerapan metode *Hill Cipher* dan *Caesar Cipher* untuk keamanan pesan *chatting* berbasis WLAN ?
3. Bagaimana menghasilkan aplikasi Penerapan Metode *Hill Cipher* Dan *Caesar Cipher* Pada Aplikasi *Wireless* LAN *Chatting* ?

I.2.3. Batasan Masalah

Batasan masalah pada penelitian ini berdasarkan latar belakang adalah sebagai berikut :

1. Aplikasi hanya untuk menerapkan metode *hill cipher* dan *caesar cipher* pada aplikasi *wireless* LAN *chatting*.
2. Aplikasi hanya dapat berjalan pada sistem operasi *windows*.
3. *Input* aplikasi ini berupa pesan teks.
4. *Output* aplikasi ini berupa hasil penerapan metode *hill cipher* dan *caesar cipher* pada aplikasi *wireless* LAN *chatting*.
5. Pembuatan Aplikasi ini menggunakan bahasa pemrograman *Visual Basic* 2010.
6. Perancangan Aplikasi ini menggunakan pemodelan UML.
7. Metode yang digunakan adalah metode *Hill Cipher* dan *Caesar Cipher*.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Adapun tujuan penelitian ini adalah sebagai berikut :

1. Mengamankan *Wireless* LAN *chatting*.
2. Menerapkan metode *Hill Cipher* dan *Caesar Cipher* untuk keamanan pesan *chatting* berbasis WLAN.
3. Menghasilkan aplikasi Penerapan Metode *Hill Cipher* Dan *Caesar Cipher* Pada Aplikasi *Wireless* LAN *Chatting.*

I.3.2. Manfaat

Adapun manfaat penelitian ini adalah sebagai berikut :

1. Pesan *chatting* berbasis WLAN memiiliki keamanan pertukaran pesan yang baik.
2. Mengetahui dan memahami penerapan metode *Hill Cipher* dan *Caesar Cipher* untuk keamanan pesan *chatting* berbasis WLAN.
3. Mendapat wawasan dalam pembuatan perangkat lunak jaringan dan keamanan jaringan.

I.4. Metodologi Penelitian

Metode merupakan suatu cara yang sistematik untuk mengerjakan suatu permasalahan. Penelitian ini akan melalui beberapa tahapan. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut :

Pada tahap ini dilakukan dengan mempelajari teori dasar yang mendukung penelitian, pencarian dan pengumpulan data-data yang dibutuhkan. Untuk mengumpulkan data yang dibutuhkan, maka penulis memakai teknik :

1. Penelitian Kelapangan (*Field Research*)

1. Wawancara (*Interview*)

   Peneliti melakukan wawancara dengan ahli kriptografi dan jaringan untuk mencari pemahaman yang berkaitan tentang jarngan dan kriptografi.

2. Sampel (*Sampling*)

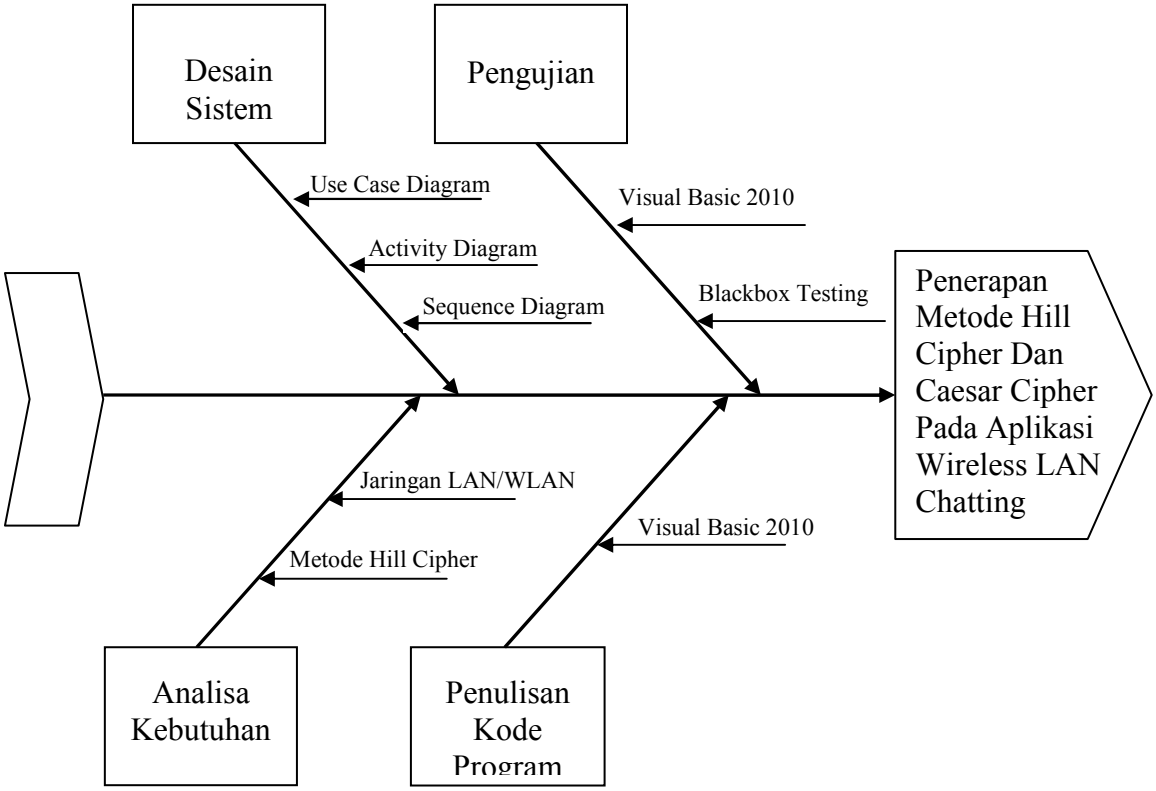
   Peneliti mengumpulkan data-data yang tersedia untuk contoh pembuatan penelitian ini.

3. Penelitian Perpustakaan (*Library Research*)

   Pada metode ini penulis mengutip dari beberapa bacaan yang berkaitan dengan pelaksanaan skripsi yang dikutip dapat berupa teori.

2. *Fish Bone* Metode Penelitian

Berikut adalah *Fish Bone* metode penelitian yang digunakan dalam penulisan skripsi ini.



Gambar III.1. *Fish Bone* Metode Penelitian

Keterangan :

1. Analisa Kebutuhan

Pada tahap ini dilakukan pengumpulan data-data mengenai jaringan, kriptografi beserta metode *Hill Cipher* dan *Caesar Cipher*. Pada tahapan ini juga

ditentukan *software* dan *hardware* yang akan digunakan untuk mengimplementasikan dan menguji hasil penelitian.

Berikut adalah *software* yang digunakan :

a. Sistem operasi *windows* 7

b. *Visual Basic* 2010

Berikut adalah *hardware* yang digunakan :

a. *Laptop/ Computer*

b. *Hardisk*

2. Desain Sistem

Pada tahap ini dilakukan desain perangkat lunak menggunakan pemodelan UML yaitu *use case diagram*, *class diagram*, *activity diagram* dan *sequence diagram*.

3. Penulisan Kode Program

Kode program merupakan terjemahan *design* dalam bahasa yang bisa dikenali komputer. Pada tahap ini desain sistem diimplementasikan ke dalam kode program. Pemrograman ditulis menggunakan *visual basic* 2010.

4. Pengujian Program

Pengujian program merupakan langkah yang dilakukan setelah penulisan kode program. Pengujian program dilakukan untuk mengetahui hasil dari perancangan sistem yang telah dibuat dan untuk mengetahui kekurangan sistem dengan menggunakan *blackbox testing* untuk pengujian secara teori dan menggunakan *visual basic* 2010 untuk pengujian secara praktek. Apabila terdapat kekurangan

sistem atau program tidak berjalan dengan baik, maka akan dilakukan perbaikan sampai seluruh program berjalan dengan baik.

5. Hasil

Pada tahapan ini penelitian ini sudah menghasilkan Penerapan Metode *Hill Cipher* Dan *Caesar Cipher* Pada Aplikasi *Wireless* LAN *Chatting*.

I.6. Kontribusi Penelitian

Kontribusi yang dihasilkan penelitian ini yaitu :

1. Penelitian ini dapat menjadi referensi terbaru bagi peneliti berikutnya.
2. Penelitian ini dapat menjadi ide baru untuk peneliti berikutnya.
3. Penelitian ini dapat memberikan keamanan para pengguna *chatting* berbasis WLAN.

I.7. Sistematika Penulisan

Sistematika penulisan yang diajukan dalam skripsi 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 teori dasar yang berhubungan dengan program yang dirancang serta bahasa pemrograman yang digunakan.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan analisa masalah program yang akan dirancang dan rancangan program yang digunakan pada penulisan Skripsi ini.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini mengemukakan tentang hasil implementasi sistem yang dirancang mencakup uji coba sistem, tampilan serta perangkat yang dibutuhkan. Analisa sistem dirancang untuk mengetahui kelebihan dan kekurangan sistem yang dibuat.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini berisikan berbagai kesimpulan yang dapat dibuat berdasarkan uraian yang telah disimpulkan dan saran.