# BAB I

# PENDAHULUAN

## I.1. Latar Belakang

Keamanan 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 (Paryati ; 2012 : 379).

Kriptografi hadir untuk meningkatkan aspek keamanan transmisi data. 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 keamanan dan kerahasiaan transmisi data merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi. Apalagi jika transmisi data 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 transmisi data yang dibajak tersebut akan memiliki kemungkinan rusak bahkan hilang yang akan menimbulkan kerugian material yang besar.

*One Time Pad* ini ditemukan pada tahun 1917 oleh *Major Yoseph Mouborgne* dan *Gilbert Vernam* pada perang dunia ke dua metode ini telah diklaim sebagai satu-satunya algoritma kriptografi sempurna yang tidak dapat dipecahkan.

Masalah keamanan dan kerahasiaan transmisi data merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi. Apalagi jika transmisi data 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 transmisi data yang dibajak tersebut akan memiliki kemungkinan rusak bahkan hilang yang akan menimbulkan kerugian material yang besar.

Alasan penulis mengambil judul penelitian "**Analisis Keamanan Transmisi Transmisi data Teks Melalui Websocket Menggunakan Algoritma**

**One-Time Pad**" karena tidak adanya implementasi algoritma one-time pad dalam pengembangan aplikasi Pengamanan Transmisi data.

## I.2. Ruang Lingkup Permasalahan

### I.2.1. Identifikasi Masalah

Permasalahan yang ada pada penelitian ini adalah :

1. Tidak ada sebuah aplikasi yang memiliki sistem keamanan transmisi data yang aman.
2. Belum ada perkembangan algoritma Algoritma one-time pad dalam sistem keamanan berkas atau transmisi data.

### I.2.2. Perumusan Masalah

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

1. Bagaimana merancang sebuah aplikasi yang memiliki sistem keamanan transmisi data yang aman ?
2. Bagaimana melakukan perkembangan algoritma one-time pad dalam sistem keamanan berkas atau transmisi data ?

### I.2.3. Batasan Masalah

Batasan masalah pada penelitian ini yaitu:

1. Data yang dibutuhkan dalam melakukan perancangan sistem adalah file teks, alamat ip, nomor port komputer, data kunci, data cipher.
2. Bahasa pemrograman yang digunakan untuk membuat aplikasi adalah *netbeans, javascript.*

## I.3. Tujuan dan Manfaat

### I.3.1. Tujuan

Adapun tujuan dari perancangan aplikasi ini adalah :

1. Merancang sebuah aplikasi dengan memanfaatkan sistem keamanan transmisi data yang dapat menjaga kerahasiaan dan keamanan transmisi data.
2. Merancang dan membangun sebuah aplikasi keamanan berkas atau dengan dengan menggunakan Algoritma one-time pad

### I.3.2. Manfaat

Manfaat dari penelitian ini adalah :

1. Aplikasi keamanan transmisi data dengan memanfaatkan sistem keamanan transmisi data dapat menjaga kerahasiaan dan keamanan pengiriman transmisi data pada aplikasi keamanan transmisi data sehingga pengirim pesan dapat merasa nyaman dan aman dalam melakukan transfer transmisi data atau pesan

2. Implementasi Algoritma one-time pad terhadap aplikasi keamanan transmisi data dirancang untuk penggunaan memori yang seminimal mungkin dengan kecepatan proses yang maksimal

## I.4. Metodologi Penelitian

Metodologi atau teknik yang digunakan dalam pengembangan dan pembuatan perangkat lunak meliputi metodologi konvensional (sebelum pertengahan 1970-an), struktural klasik (mulai pertengahan 1970-an), struktural modern (mulai pertengahan 1980-an) dan *post modern* (mulai akhir 1980-an).

### 1. Jenis data

Jenis penelitian pada skripsi ini adalah penelitian deskriptif yaitu penelitian yang menghasilkan data berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang dapat diamati

### 2. Sumber data

Salah satu pertimbangan dalam memilih masalah penelitian adalah ketersediaan sumber data. Penelitian kuantitatif lebih bersifat explanation (menerangkan, menjeleskan), karena itu bersifat *to learn about the people* (masyarakat objek), sedangkan penelitian kualitatif lebih bersifat *understanding* (memahami) terhadap fonemena atau gejala sosial**.** Transmisi data yang digunakan dalam penelitian ini diperoleh dari file teks, alamat ip, nomor port komputer, data kunci, data cipher.

### 3. Metode Pengumpulan data

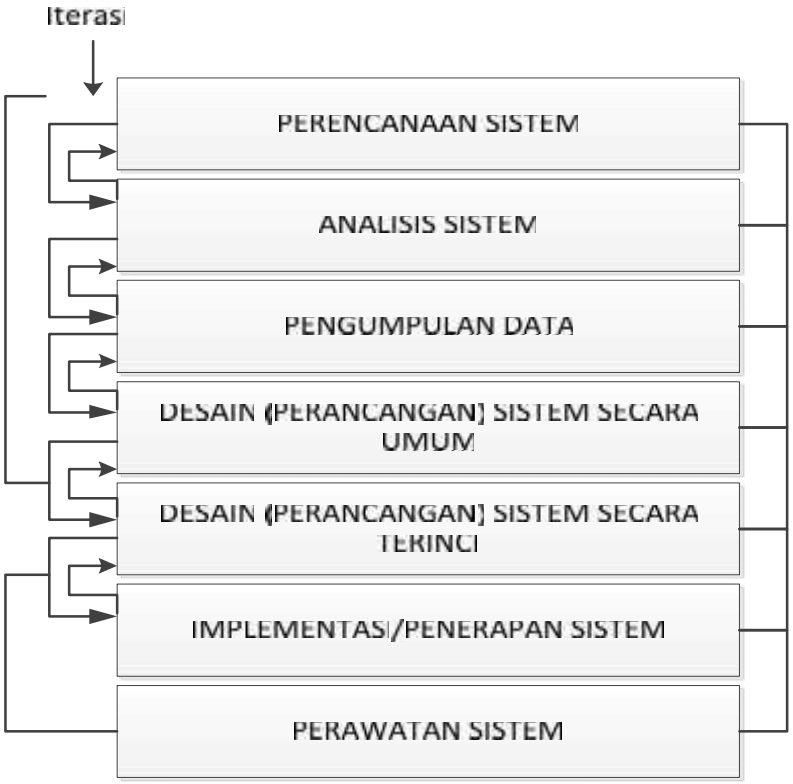
Untuk mendapatkan kelengkapan informasi yang sesuai dengan fokus penelitian maka yang dijadikan teknik pengumpulan transmisi data adalah teknik dokumentasi, dokumen merupakan catatan peristiwa yang sudah berlalu. Dokumen bisa berbentuk tulisan, gambar, atau karya-karya.

### 4. Analisis data

Analisis data dilakukan setelah peneliti melakukan pengumpulan transmisi data terhadap data yang akan dibutuhkan dalam melakukan Analisis Keamanan Transmisi data teks melalui websocket menggunakan algoritma one-time pad.

### 5. Alur Analisis

Untuk menganalisa transmisi data 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 keamanan transmisi data yang aman pada penyimpanan transmisi data atau berkas.
   b. Belum berkembangnya algoritma one-time pad dalam sistem keamanan berkas atau transmisi data.

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. Transmisi data yang digunakan dalam penelitian ini diperoleh dari file teks, alamat ip, nomor port komputer, data kunci, data cipher.
   b. Bahasa pemrograman yang digunakan untuk membuat aplikasi adalah *netbeans, javascript.*

3. Pengumpulan data

   Pengumpulan data adalah cara-cara yang dapat digunakan oleh peneliti untuk mengumpulkan data. Instumen sebagi alat bantu dalam menggunakan methode pengumpulan transmisi data 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 *javascript*
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 transmisi data 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 Keamanan Transmisi data teks melalui websocket menggunakan algoritma one-time padyang telah dirancang oleh penulis membutuhkan

implementasi metode untuk menyempurnakan keamanan transmisi data, metode yang digunakan oleh penelitian adalah *one-time pad*

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 Keaslian Penelitian

Berikut adalah beberapa jurnal penelitian terdahulu terkait judul penelitian skripsi ini pada tabel I.1 :

**Tabel I.1. Keaslian Penelitian**

| No | Peneliti | Judul | Hasil |
|---|---|---|---|
| 1 | Hengky Mulyono (2013) | Implementasi Algoritma One Time Pad Pada Penyimpanan Data Berbasis Web | Salah satu hal yang perlu diperhatikan dalam menjaga keamanan sebuah sistem adalah proses autentikasi. Proses ini dilakukan untuk memastikan bahwa user yang mengakses data maupun informasi pada sistem tersebut adalah user yang memiliki wewenang. Ada beberapa metode untuk melakukan autentikasi, salah satunya dengan menggunakan teknik penyandian data (kriptografi). Kriptografi diterapkan pada data maupun informasi dengan mengkodekan atau menyembunyikan data aslinya sehingga hanya pihak yang memiliki kunci yang dapat mengakses data atau informasi tersebut. Penelitian ini akan mengimplementasikan algoritma One Time Pad (OTP) untuk melakukan penyandian terhadap data dan informasi yang disimpan. Data atau |

| | | | |
|---|---|---|---|
| | | | informasi yang disimpan dalam aplikasi akan berbentuk ciphertext sehingga user akan mendapatkan kunci untuk mengakses data atau informasi tersebut. Pembuatan aplikasi ini diharapkan dapat menjaga kerahasiaan dan keamanan data dengan baik, dimana pihak yang dapat mengakses data atau informasi yang asli hanya pihak yang memiliki kunci |
| 2 | Febryaan Christy (2014) | Implementasi Modifikasi Kriptografi One Time Pad (OTP) untuk Pengamanan Data File | Media elektronik dan digital sudah menjadi tren untuk mengirimkan informasi baik yang bersifat umum maupun rahasia. Untuk menjaga keamanan data yang dikirim diperlukan pengamanan khusus. Pengamanan dalam penelitian ini menggunakan algoritma One Time Pad (OTP) yang dimodifikasi dengan melakukan tiga kali proses dan menggunakan bit shifting pada kunci dan plainteks. Kunci pada proses kedua dan ketiga digenerate agar bertambah sebanyak karakter dalam plainteks. Hasil dari penelitian ini adalah teknik kriptografi yang dapat diaplikasikan pada pengamanan file berbasis teks |

## I.6. Sistematika Penulisan

Adapun 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 tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang sedang dihadapi yaitu berupa pembahasan mengenai sistem jaringan, UML, ERD dan normalisasi.

**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 datang untuk sistem.