

BAB I

PENDAHULUAN

1.1 Latar Belakang

Saat ini pencurian data melalui plagiasi dan modifikasi sering kita temui dalam kehidupan digital. Dokumen yang banyak digunakan adalah dokumen dengan ekstensi *docx*. Hal ini dikarenakan dokumen dengan ekstensi *.docx* merupakan salah satu dokumen yang mudah dalam proses pembuatan serta penyimpanannya. Untuk menjaga kerahasiaan, integritas, pengenalan identitas pengirim dan pencegahan penyangkalan pengiriman data dokumen, maka diperlukan sebuah alat bantu untuk melindungi dokumen tersebut. Hal ini menjadi masalah utama dalam persaingan dunia bisnis. Oleh karena itu untuk menjaga integritas data tersebut dibutuhkan sebuah sistem keamanan berupa penyandian atau pengkodean data sebelum proses pengiriman dilakukan, yang bertujuan untuk mengamankan data penting yang bersifat rahasia agar tidak dengan mudah dibaca dan diubah isi dari pesan tersebut oleh pihak yang tidak berkepentingan (Karima dan Saputro, 2016).

Dokumen harus sangat dijaga kerahasiaannya, apalagi data itu sangat penting bagi suatu perusahaan, institusi, negara, daerah, dan milik pribadi. Banyaknya penyadap dan kejahatan internet yang terjadi saat ini dengan adanya perkembangan teknologi membuat orang dengan mudah mengakses internet membuat banyak peluang untuk melakukan tindakan kejahatan. Berkembangnya bidang keilmuan kriptografi dapat mengatasi kejahatan dengan didukung oleh teknologi canggih saat ini. Adanya kesadaran untuk menjaga suatu dokumen penting harus sangat diperhatikan kerahasiaan dan keamanannya pada saat melakukan kegiatan-kegiatan yang dilakukan terutama kegiatan pengiriman dokumen.

Keamanan data pada lalu lintas jaringan adalah suatu hal yang diinginkan semua orang untuk menjaga *privacy*. Supaya data yang dikirim aman dari orang yang tidak bertanggung jawab dengan menyembunyikan data memakai algoritma kriptografi logis yang menyembunyikan pesan dari orang yang tidak berhak atas

pesan tersebut sehingga terhindar dari *interruption*, *interception*, *modifikasi*, dan *fabrication* (Ariyus, 2006). Oleh karena itu dibutuhkan suatu metode yang dapat mengamankan dokumen saat dikirim. Untuk menjaga keamanan data dokumen tersebut maka dapat diterapkan algoritma kriptografi berupa enkripsi yang dapat diubah menjadi teks yang tidak bisa dibaca jika tidak dideskripsi, maka orang tidak akan bisa mengetahui apa isi dari dokumen tersebut. Dengan demikian data dokumen akan tetap terjaga saat dikirim. .

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut dapat diketahui bahwa pengiriman data melalui jaringan publik rentan terhadap keamanan data, oleh karena itu perlu dilakukan pengamanan data agar tetap terjamin integritas datanya. Sehingga dalam penelitian ini masalah yang diangkat oleh peneliti adalah bagaimana mengamankan data yang bertipe *.docx* dan *.txt*.

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah sebagai berikut:

1. Data yang diamankan adalah *file* bertipe *.docx* dan *.txt*.
2. Aplikasi yang dibuat menggunakan bahasa pemrograman berbasis *web* dan *php*.
3. Isi dari *file docx* hanya berisi teks murni (tidak terdapat tabel, simbol, gambar).

1.4 Tujuan Dan Manfaat

Berdasarkan permasalahan pada penelitian ini, maka tujuannya adalah untuk mengamankan data dengan format *.docx* dan *.txt*. Adapun manfaat dari penelitian ini adalah mengamankan *file* data dengan format *.docx* dan *.txt*.

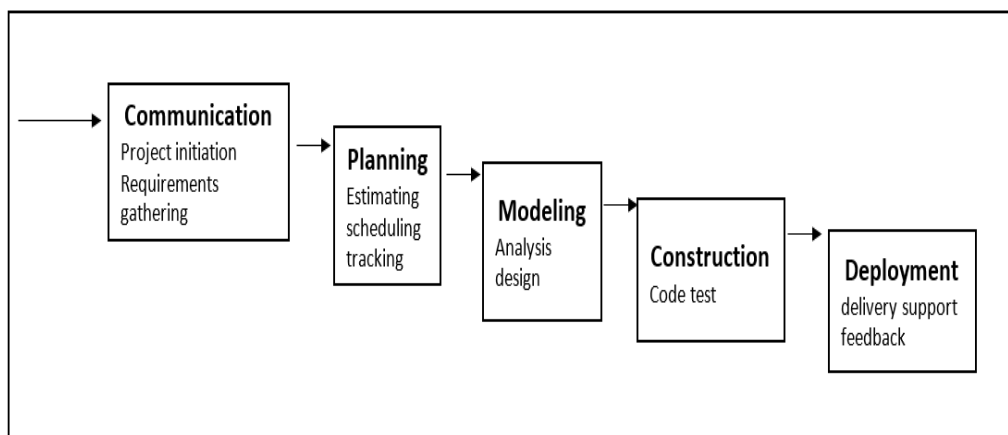
1.5 Metodologi Pengembangan Sistem

Pada metodologi penelitian terdapat tahap yang dilakukan pada penelitian yaitu sebagai berikut :

1. Berdasarkan klasifikasi penelitian berdasarkan tujuan dan manfaatnya, penelitian ini merupakan jenis penelitian terapan. Penelitian ini dilakukan untuk menerapkan metode *Elgamal* pada proses enkripsi dan dekripsi pada *file office* dengan format *.docx* dan *.txt*.

2. Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan dalam penelitian ini adalah model *waterfall*. Model ini melakukan pendekatan kepada pengembangan perangkat lunak yang sistematis dan sekuensial yang mulai pada tingkat dan kemajuan sistem pada *communication*, *planning*, *modelling*, *construction* dan *deployment* (Pressman, 2010). Adapun ilustrasinya sebagai berikut :



Gambar 1.1. Model Waterfall
(Sumber : Pressman, 2010)

1.6 Sistem Penulisan

Sistematika penulisan yang digunakan dalam penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas tentang pendahuluan yang mencakup uraian tentang latar belakang, rumusan masalah, ruang lingkup, tujuan dan manfaat, metodologi penelitian serta sistematika penulisan dijelaskan pada bab ini.

BAB II LANDASAN TEORI

Dalam bab ini dibahas mengenai beberapa teori yang dipakai untuk mendukung penelitian.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini menguraikan kebutuhan dasar yang diperlukan selama proses perancangan perangkat lunak (*software*), meliputi pembahasan mengenai sistem enkripsi dan deskripsi file *.docx* dan *.txt* menggunakan algoritma *Elgamal* serta menguraikan tentang gambaran secara umum dari desain dan tampilan tampilan perangkat lunak(*software*) yang dibangun.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini menjelaskan tentang spesifikasi *hardware* dan *software* yang dibutuhkan dalam menjalankan aplikasi, prosedur operasional, rencana implementasi, serta evaluasi dari percobaan yang dilakukan

BAB V KESIMPULAN DAN SARAN

Bab ini yang telah didapat setelah melakukan proses pembuatan aplikasi sistem, serta saran-saran yang diajukan untuk pengembangan sistem.