BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi informasi berkembang semakin cepat khususnya dalam perkembangan komunikasi digital setelah munculnya internet. Internet menjadi sebuah sarana yang memberikan berbagai layanan, sehingga memungkinkan manusia untuk saling berkomunikasi dan saling berbagi informasi tanpa mengenal tempat, jarak dan waktu. Saat ini *e-mail* menjadi salah satu layanan internet yang sering digunakan di seluruh dunia dan khususnya di Indonesia. Dan *e-mail* telah menjadi layanan komunikasi alternatif yang bersifat formal. Banyak perusahaan atau instansi sering mengunakan layanan *e-mail* untuk mengirimkan data – data informasi yang penting dan rahasia. Walaupun menjadi alat komunisasi formal dan banyak digunakan, namun pada dasarnya cara kerja pengiriman data melalui *e-mail* menggunakan jalur publik yaitu internet, sehingga memungkinkan terjadinya penyerangan oleh para *cracker* seperti manipulasi, penyadapan serta pencurian informasi penting yang bisa disalahgunakan untuk kepentingannya masing – masing.

Perlu diingat juga bahwa transaksi pengiriman informasi dengan *e-mail* tidak menggunakan keamanan pada data yang dikirim, sehingga jika terjadi penyadapan pada jalur pengiriman data menggunakan teknik *sniffing*, maka akan mengakibatkan kebocoran informasi serta kerahasiaan informasi *e-mail* tersebut akan terancam. Disamping itu *e-mail* juga rentan diintip oleh orang yang tidak mempunyai hak atas *e-mail* si pengguna. Seperti pada pertengahan Januari 2019,

dikutip dari kompas.com telah terjadi peretasan terhadap 773 juta akun *gmail* (alamat) *e-mail* dan pencurian 21 juta *password* yang telah tersebar di internet [1].

PT. Bumimulia Bandung merupakan salah satu perusahaan yang menggeluti bidang industri plastik. Dengan demikian, sebagai perusahaan industri besar mereka memiliki banyak data–data yang bersifat rahasia sering juga data tersebut dikirimkan melalui *e-mail*. Adapun pengiriman data melalui *e-mail* saat ini yang sering dilakukan adalah pengiriman dokumen gaji karyawan yang dikirimkan oleh *general clerk* ke *e-mail* masing – masing karyawan pada setiap bulannya. Saat ini perusahaan tersebut belum memiliki fasilitas keamanan data yang dikirim melalui *e-mail*, sehingga masih rentan terjadi pencurian dan penyadapan informasi. Untuk mencegah hal tersebut, maka diperlukan keamanan berbasis kriptografi. Kriptografi adalah teknik yang dapat digunakan untuk melindungi kerahasiaan data supaya terhindar dari orang yang tidak memiliki hak atas data tersebut. Dengan metode enkripsi dan dekripsi sebagai konsep utamanya [2].

Seperti beberapa penelitian yang telah dilakukan sebelumnya, diantaranya tentang perancangan aplikasi penyandian pesan menggunakan kriptografi *blowfish* oleh A. Fauzi (2016) [2]. Pada penelitian ini menerangkan tentang proses enkripsi dan dekripsi file teks berformat .txt yang akan dikirim melalui e-mail, sehingga teks pada file teks tersebut dienkripsi menjadi bilangan binner yang tidak diketahui nilainya kemudian disimpan untuk dikirim melalui *e-mail.* Kemudian Penelitian Siswanto, dkk (2018) mengenai implementasi kriptografi TEA dan Base64 dalam mengamankan *e-mail*. Penelitian ini hanya dapat menenkripsi file berukuran 5MB ke bawah secara optimal [3]. Kemudian penelitian Gusri Indah Yana dan Rivalri Kristianto Hondro (2017) mengenai kompresi menggunakan

algoritma *Huffman* dan LZ78 penelitan ini membahas perbandingan efektifitas antara algortima kompresi *Huffman* dan LZ78. Penelitian tersebut menjelaskan bahwa metode *Huffman* lebih tepat digunakan daripada LZ78 untuk teknik kompresi data dalam bentuk teks [4]. Kemudian pada penelitian Indra Kelana Jaya, dkk (2019) menerangkan tentang analisa alokasi memori dan kecepatan kriptograpi simetris dalam enkripsi dan dekripsi antara algoritma AES dan *Blowfish* [5]. Kemudian penelitian A. M. Abdullah (2017) [6], dengan judul *Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data*. Menurut hasil yang diperoleh dari penelitiannya menunjukkan bahwa AES memiliki kemampuan untuk memberikan keamanan yang lebih banyak dibandingkan dengan algoritma lain seperti DES, 3DES, *Blowfish* dll.

Namun pada beberapa penelitian masih memiliki kekurangan seperti pada penelitian yang dilakukan oleh Achmad Fauzi, diantaranya pengaplikasiannya masih di desktop, proses enkripsi hanya pada file berformat .txt dan belum terkoneksi langsung dengan *e-mail* dalam pengiriman pesannya. Kemudian pada penelitian yang dilakukan Indra Kelana Jaya, dkk bahwa ukuran *plaintext* yang telah dienkripsi dengan algoritma AES ukurannya bertambah besar, sehingga pada saat *ciphertext* dikirim akan membutuhkan waktu yang lama serta pemakaian alokasi memori yang dipakai pun menjadi besar.

Berdasarkan beberapa penelitian sebelumnya dapat disimpulkan bahwa metode AES (*Advanced Encryption Standard*) memiliki tingkat keamanan enkripsi pesan dan file yang aktual dibandingkan dengan metode kriptografi yang telah ada baik dari segi perhitungan waktu proses, keamanan *key*, serta mempunyai desain yang sederhana. Namun masih memiliki kekurangan yaitu penggunaan alokasi

memori yang dipakai besar untuk hasil enkripsi. Untuk menanggapi kekurangan tersebut, pada penelitian ini dilakukan pengembangan penyandian pesan dan file dengan menggunakan metode kriptografi AES. Untuk membedakan dengan penelitian sebelumnya, maka sistem akan dibuat agar dapat terkoneksi langsung dengan *e-mail* melalui *Simple Mail Transfer Protocol* (SMTP), sehingga *ciphertext* dapat dikirim langsung ke *e-mail* yang dituju. Serta mengkompresi *ciphertext* dengan metode kompresi *Huffman lossless* dalam satu kali eksekusi. Dan menambahkan file format txt, docx, doc, pdf, xls dan xlsx agar dapat dienkripsi. Berdasarkan latar belakang tersebut, maka penelitian tugas akhir ini berjudul **"Penyandian Pesan dan File Pada *E-Mail* Menggunakan Kombinasi Kriptografi *Advanced Encryption Standard* (AES) dan Teknik Kompresi *Huffman*"**.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang dipaparkan di atas, penulis memiliki beberapa rumusan masalah terkait dengan permasalahan tersebut, yaitu :

1. Bagaimana menerapkan kombinasi metode *Advanced Encryption Standard* (AES) dan teknik kompresi *Huffman* pada proses penyandian pesan teks pada *e-mail* ?
2. Berapa nilai akurasi dari pesan teks hasil enkripsi dan dekripsi menggunakan kombinasi metode *Advanced Encryption Standard* (AES) dan *Huffman* ?
3. Berapa selisih perbedaan performa waktu yang dibutuhkan antara teknik enkripsi dan dekripsi terhadap *plaintext* ?

1.3 Tujuan Penelitian

Tujuan dari pembuatan tugas akhir ini yaitu :

1. Menerapkan kombinasi metode *Advanced Encryption Standard* (AES) dan teknik kompresi *Huffman* pada proses penyandian pesan teks pada *e-mail* melalui SMTP (*Server Mail Transfer Protocol*).
2. Untuk mengetahui nilai akurasi proses enkripsi dan dekripsi menggunakan kombinasi metode *Advanced Encryption Standard* (AES) dan metode *Huffman.*
3. Untuk mendapatkan nilai selisih waktu yang dibutuhkan dalam proses enkripsi dan dekripsi *plaintext* yang dikirimkan.

1.4 Manfaat Penelitian

Adapun manfaat dari penyandian pesan dan file pada *e-mail* menggunakan kombinasi algoritma *Advanced Encryption Standard* (AES) dan Teknik Kompresi *Huffman* adalah untuk mengamankan informasi yang dikirim melalui *e-mail,* sehingga mencegah terjadinya manipulasi, pencurian serta kebocoran informasi yang dikirim, dan untuk mengetahui tingkat keakuratan dan kecepatan proses kriptografi dan kompresi dari kedua algoritma sehingga dapat memberikan saran kepada peneliti selanjutnya.

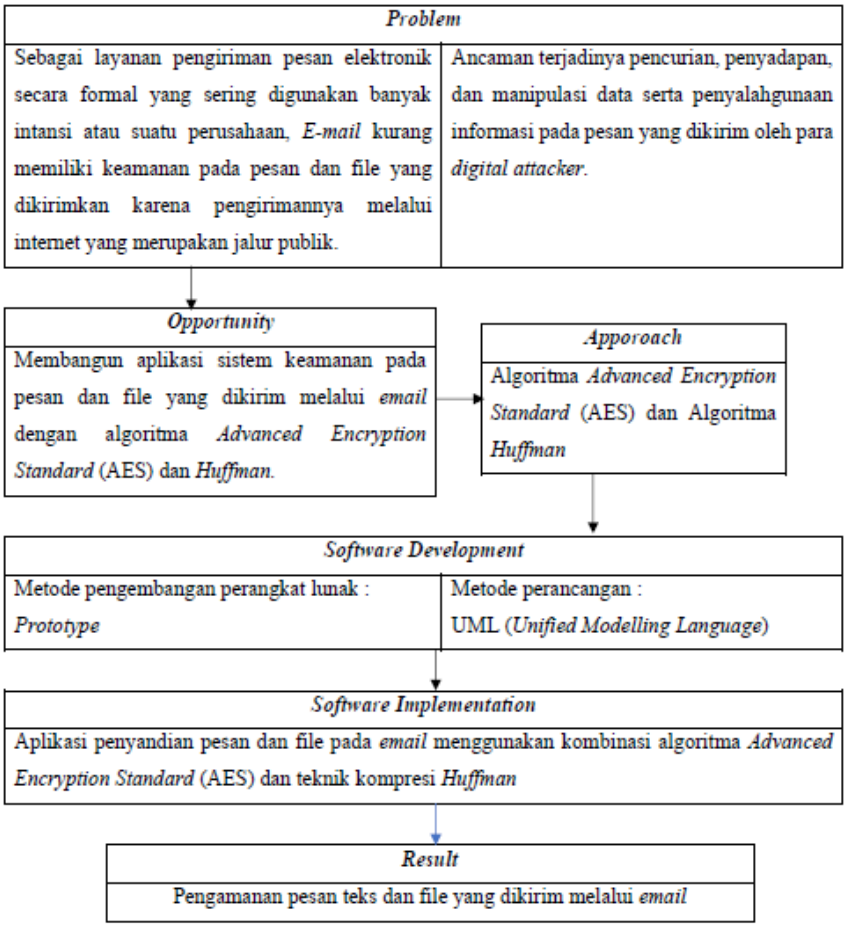
1.5 Batasan Masalah

1. Pemrograman yang digunakan adalah berbasis *web.*
2. Metode kriptografi yang dipakai pada penelitian ini yakni metode *Advanced Encryption Standard* (AES) 128 bit.
3. Metode kompresi yang digunakan adalah metode *Huffman lossless.*

4. *Output* dari aplikasi ini adalah *plaintext* yang akan dikirimkan langsung ke *e-mail* akan disandikan menjadi sebuah *ciphertext* yang kemudian akan didekripsi menjadi sebuah file asli dengan menggunakan kunci AES.
5. Keamanan kriptogafi hanya diterapkan pada *plaintext*-nya saja, bukan pada jalur pengirimannya.
6. File text yang digunakan sebagai penyembunyian pesan ialah berformat docx, doc, txt, pdf, xls dan xlsx.
7. Pada penelitian ini tidak membahas proses kriptanalis *(Cryptanalyst).*

1.6 Kerangka Pemikiran

Untuk kerangka pemikiran pada aplikasi ini akan dijelaskan pada Gambar 1.1.



Gambar 1.1 Skema Kerangka Pemikiran

1.7 Metodologi Pengerjaan Tugas Akhir

Berikut ini merupakan metodologi yang digunakan dalam penelitian ini diantaranya :

1.7.1 Tahap Pengumpulan Data

Adapun metode pengumpulan data yang digunakan kali ini terdiri tiga tahapan, diantaranya :

1. Wawancara

   Wawancara yang dilakukan yaitu berupa wawancara dengan staff dan karyawan PT.Bumimulia Bandung.

2. Studi Literatur

   Penulis akan melakukan studi literatur diantaranya dengan cara memahami dan mempelajari berbagai literatur, *paper*, buku-buku, referensi serta jurnal-jurnal yang berkaitan dengan sistem yang akan dibuat.

3. Observasi

   Observasi yang dilakukan yaitu dengan cara melakukan survey dan penelitian langsung terhadap permasalahan yang diangkat.

1.7.2 Tahap Pengembangan Perangkat Lunak

Dalam pembuatan sistem pada penelitian ini menggunakan metode *prototype*. *Prototype* adalah suatu metode untuk pengembangan perangat lunak, yang berbentuk model fisik kerja sistem dengan fungsi sebagai versi awal dari sistem [7].

Berikut ini adalah tahapan dalam metode *Prototype* yang akan dilakukan, diantaranya :

a. *Listen to customer*

Tahap ini mencangkup pengumpulan ide dari kebutuhan sistem yang akan dibuat. Untuk membangun suatu sistem agar sesuai kebutuhan, maka dapat dengan cara melakukan wawancara kepada customer atau bisa dengan melihat sistem yang sudah ada dan sedang berjalan untuk mendapatkan ide pokok masalah.

b. *Revise / Build mockup*

Setelah mengetahui kebutuhan, maka selanjutnya melakukan perancangan dan pembuatan *prototype* sistem (*blue print*). *Prototype* yang dibangun harus cocok atau sesuai dengan kebutuhan yang telah ditentukan pada tahap sebelumnya.

c. *Customer test drives mockup*

Kemudian, pada tahap ini dilakukan pengujian oleh *user* terhadap *prototype* dari sistem, sekaligus melakukan evaluasi atau perbaikan terhadap kekurangannya. Pengembang kemudian melakukan kembali tahap pertama untuk mendengarkan keluhan dari user serta melakukan revisi atau perbaikan terhadap *prototype* dari sistem yang tidak cocok dengan kebutuhan *user*, apabila sudah tidak ada revisi bisa dilanjutkan ke tahap berikutnya.

1.8 Sistematika Penulisan

Pada sistematika penulisan tugas akhir ini memiliki lima bab yang terdiri dari masing-masing bab berisi sub-bab untuk memberikan gambaran umum pada setiap pembahasan yang akan dibahas. Berikut penejelasan mengenai bab-bab tersebut :

BAB I PENDAHULUAN

Pada bab ini membahas latar belakang, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metodologi penelitian serta sistematika penelitian.

BAB II LANDASAN TEORI

Pada bab ini membahas terkait teori-teori yang menunjang dalam penyusunan tugas akhir ini berdasarkan studi literatur.

BAB III ANALISIS DAN PERANCANGAN

Pada bab ini membahas mengenai analisis dan perancangan, dimana membahas analisis sistem yang akan dibangun sampai tahap perancangan sistem. Untuk perancangan sistem meliputi arsitektur sistem, perancangan antarmuka, perancangan *database*, pemodelan sistem dan rancangan pengujian.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Pada bab ini membahas mengenai hasil implementasi atau penerapan analisis, perancangan yang telah disusun pada bab sebelumnya dan pengujian pada sistem yang telah dirancang dan dibangun.

BAB V PENUTUP

Pada bab ini membahas terkait kesimpulan dari hasil penelitian yang telah dikakukan serta saran dari penulis yang bisa dimanfaatkan untuk pengembangan penelitian selanjutnya agar dapat melanjutkan pencapaian kinerja yang lebih baik lagi.