BAB I

PENDAHULUAN

1.1 Latar Belakang

Penggunaan komputer di era global elektronik tidak lepas dari pengiriman pesan/data dan tukar menukar. Melihat teknologi informasi yang semakin canggih pengiriman pesan melalui internet merupakan hal yang sering dan mudah dilakukan. Tetapi apakah pesan yang dikirim akan aman? Keamanan adalah prioritas utama dalam pengiriman pesan penting dan rahasia yang akan menjadi masalah bila dibaca oleh pihak yang memanfaatkan, sehingga memerlukan pengamanan yang sesuai agar terjamin kerahasiaannya dan diterima orang yang tepat. Program yang sering digunakan dalam hal merahasiakan pesan sebagai pengamanan data adalah dengan metode kriptografi.

Dalam pengamanan pesan tersebut diperlukan adanya proses mengubah informasi menjadi tidak dapat dibaca dan dimengerti. Dan proses untuk mengembalikan pesan yang tidak dapat terbaca menjadi pesan asli. Kriptografi juga mempunyai beberapa algoritma yang digunakan untuk mengamankan pesan atau mengenkripsi, mulai dari yang sederhana sampai yang modern. Di setiap algoritma mempunyai karakter dan tingkatan sendiri-sendiri. Algoritma enkripsi modern yang sudah banyak dikenal dengan model bit-nya adalah *Data Encryption Standard* (DES). Dengan kata lain proses pengenkripsian dan pendekripsian DES ini yang dilakukan secara manual akan mempunyai kesalahan yang besar, tanpa bantuan komputer. Pesan pasti gagal untuk dibaca ketika satu angka salah

perhitungannya. Meskipun saat ini standar tersebut telah digantikan dengan algoritma yang baru, yakni *Advance Encryption Standard* (AES).

Advance Encryption Standard (AES) merupakan algoritma kriptografi perkembangan dari DES bahwa sama-sama blok *cipher text* simetri juga. DES yang beroperasi pada blok 64 bit, sedangkan AES beroperasi pada blok 128 bits. Sehingga tingkat keamanan pesan nantinya akan lebih bisa menjaminnya. Dari kedua algoritma kriptografi tersebut, DES dan AES termasuk kategori algoritma simetri sehingga masih dalam lingkungan dan jenis yang sama. Walaupun tingkat keamanan sudah meningkat namun alur dari kedua algoritma tersebut masih selaras, sehingga masih punya kemungkinan untuk tingkat keamanan yang mudah ditebak. Untuk meningkatkan keamanan pesan dengan algoritma asimetri yang mempunyai kesulitan perhitungan algoritma diskret pada bilangan modulo prima yang besar, sehingga upaya untuk menyelesaikan masalah algoritma ini menjadi sangat sulit. Algoritma yang mempunyai algoritma tersebut adalah algoritma kriptografi ElGamal.

Melihat permasalahan tersebut, dalam teknologi komputer saat ini kita dapat mengembangkan aplikasi enkripsi dan dekripsi pesan. Diharapkan aplikasi enkripsi dan dekripsi pesan ini dapat membantu kita agar lebih mudah mengenkripsi dan mendekripsikan pesan menggunakan algoritma kriptografi DES, AES, dan ElGamal. Adapun dalam aplikasi enkripsi dan dekripsi yang ada sekarang ini masih kurang pengamanannya terhadap pesan yang tidak ingin diketahui banyak orang.

Berdasarkan latar belakang yang telah dipaparkan inilah penulis mencoba membuat aplikasi yang memudahkan proses enkripsi dan dekripsi pesan dengan menggabungkan algoritma DES, AES, dan ElGamal dan dari penelitian ini penulis mengangkat judul **"Implementasi Algoritma Kriptografi *Hybrid* (DES, AES, dan ElGamal) pada Aplikasi Desktop berbasis Python"**.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, maka perlu dirumuskan suatu masalah yang akan dipecahkan/diselesaikan pada penelitian/perancangan ini. Adapun pokok permasalahan dalam penelitian ini adalah sebagai berikut:

1. Bagaimana perhitungan dari masing-masing algoritma kriptografi (DES, AES, dan ElGamal) tanpa bantuan komputer?
2. Bagaimana melakukan enkripsi dan dekripsi pesan dengan masing – masing algoritma kriptografi (DES, AES, dan ElGamal) secara langsung *(automatic)* pada aplikasi yang dibuat?
3. Bagaimana melakukan enkripsi dan dekripsi pesan dengan algoritma kriptografi *hybrid* (DES dengan ElGamal) secara langsung *(automatic)* pada aplikasi yang dibuat?
4. Bagaimana melakukan enkripsi dan dekripsi pesan dengan algoritma kriptografi *hybrid* (AES dengan ElGamal) secara langsung *(automatic)* pada aplikasi yang dibuat?

1.3 Batasan Masalah

Agar masalah yang diteliti tidak keluar atau tidak menyimpang maka diperlukan suatu batasan masalah. Dalam penelitian ini peneliti membatasi masalah yang diteliti, yaitu pada aplikasi enkripsi dan dekripsi pesan dengan algoritma kriptografi *hybrid* (DES, AES, dan ElGamal). Adapun batasan masalah pada penelitian ini adalah sebagai berikut:

1. Aplikasi ini berbasis *desktop* (Linux maupun Windows).
2. Aplikasi ini hanya menggunakan algoritma kriptografi meliputi: DES, AES, dan ElGamal saja dalam proses enkripsi deskripsi pesan.
3. Kriptografi *Hybrid* yang dimaksud adalah penggabungan algoritma simetri dan asimetri antara lain: DES dengan ElGamal dan AES dengan ElGamal.
4. Inputan ke aplikasi hanya pesan teks tertulis saja yang bisa dienkripsi dan didekripsi.
5. Peneliti tidak berfokus pada pembuatan program pendukung aplikasi tetapi pada implementasi dan hasil analisa dari program yang dibuat.
6. Sistem operasi yang digunakan peneliti dalam pembuatan aplikasi kriptografi *hybrid* (DES, AES, dan ElGamal) dengan menggunakan Linux Mint 17.
7. Pembuatan program pendukung aplikasi kriptografi *hybrid* (DES, AES, dan ElGamal) menggunakan bahasa pemrograman Python.

8. Algoritma kriptografi, bahasa pemrograman, sistem operasi, dan program pendukung selain yang disebutkan tidak dibahas dan tidak digunakan dalam penelitian ini.
9. Proses enkripsi dekripsi pada aplikasi ini memiliki batasan-batasan pada tiap proses algoritma dan akan dijelasakan pada bab implementasi dan pembahasan.

1.4 Maksud dan Tujuan Penelitian

Untuk menunjang penguasaan ilmu yang telah diberikan oleh lembaga pendidikan Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta, yang berorientasi pada Teknologi Informasi dan Komputerisasi. Adapun maksud dan tujuan yang ingin dicapai dari penelitian ini adalah:

1.4.1 Internal

Pengertian tujuan internal yang dimaksud adalah dilihat dari sisi penulis. Dalam hal ini penulis sebagai Mahasiswa Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta adalah sebagai berikut:

1. Sebagai prasyarat untuk memperoleh gelar Strata-1 Jurusan Teknik Informatika di Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
2. Menerapkan ilmu teoritis yang didapat selama mengikuti pendidikan di Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.

3. Sebagai tolak ukur, sejauh mana ilmu yang didapat diperkuliahan dapat diterapkan ke dalam lingkungan permasalahan yang sebenarnya dengan cara terlibat langsung dalam proses pembuatan aplikasi.
4. Memperluas serta meningkatkan kemampuan mahasiswa sebagai bekal untuk memasuki persaingan dunia kerja.

1.4.2 Eksternal

Bagi masyarakat luas dan dunia pendidikan pada umumnya penelitian ini mempunyai tujuan sebagai berikut:

1. Adanya implementasi dan hasil analisa yang mampu ditunjukkan sebagai bukti bahwa algoritma kriptografi *hybrid* (DES, AES, dan ElGamal) mampu digunakan sebagai alat merahasiakan pesan yang sulit dipecahkan dengan perhitungan *manual* tanpa bantuan komputer.
2. Menghasilkan sebuah program aplikasi berbasis *desktop* yang berfungsi untuk mengenkripsi dan mendekripsi pesan teks dengan algoritma kriptografi *hybrid* (DES, AES, dan ElGamal) berbasis Python.
3. Sebagai bahan penelitian yang dapat dikembangkan dan diperbaiki pada penelitian berikutnya.

1.5 Manfaat Penelitian

Manfaat yang akan didapat dari penelitian ini adalah sebagai berikut:

1. Bagi Peneliti
    a. Peneliti dapat belajar dan mengimplementasikan materi yang didapat selama mengikuti perkuliahan yang berguna sebagai bekal pengalaman memasuki dunia kerja.
    b. Adanya implementasi dan hasil analisis yang mampu ditunjukkan sebagai bukti sehingga mampu dikembangkan lebih baik daripada penelitian sebelumnya.
2. Bagi Akademik
    a. Dapat dijadikan pembanding atau literature penyusunan skripsi dimasa yang akan dating.
    b. Memanfaatkan referensi perpustakaan dan penambah ide-ide baru untuk dikembangkan.
3. Bagi Pembaca dan Masyarakat
    a. Dapat digunakan sebagai alat pembuat pesan rahasia dan pemecah rahasia dengan aplikasi enkripsi dan dekripsi menggunakan algoritma kriptografi *hybrid* (DES, AES, dan ElGamal).
    b. Menjadi solusi dalam pembuatan pesan rahasia dengan aplikasi *desktop* kriptografi *hybrid* (DES, AES, dan ElGamal) secara cepat, mudah, dan aman.

1.6 Metode Penelitian

Peneliti menjabarkan cara-cara memperoleh data-data yang digunakan untuk kebutuhan penelitian.

1.6.1 Metode Analisis

Metode analisis yang digunakan dalam penelitian ini adalah analisis SWOT.

1.6.1.1 Analisis SWOT

Analisis SWOT adalah singkatan dari (*Strengths, Weakness, Opportunities, Threats*) yaitu penganalisa kekuatan, kelemahan, peluang serta ancaman dalam hasil penelitian ini.

1.6.1.2 Analisis Kebutuhan Sistem

Analisis kebutuhan sistem adalah beberapa kebutuhan dalam sistem untuk mendukung jalannya proses pembuatan dan kinerja aplikasi yang dibuat.

1.6.1.3 Analisis Kelayakan Sistem

Analisis kelayakan adalah untuk menentukan layak tidaknya aplikasi yang dibuat. Analisis kelayakan yang digunakan adalah dari segi teknologi, operasional, dan hukum.

1.6.2 Metode Pengumpulan Data

Metode pengumpulan informasi dan data yang digunakan dalam penelitian ini diantaranya:

1.6.2.1 Metode Studi Kepustakaan

Metode studi kepustakaan yaitu teknik pengumpulan data yang dilakukan dengan penelaahan terhadap literature – literature, buku – buku pendukung, catatan, dan laporan-laporan untuk mendapatkan konsep teori mengenai masalah yang diteliti.

1.6.2.2 Metode Browsing

Metode *browsing* yaitu teknik pengumpulan rujukan yang bersumber dari internet dengan mengunjungi situs yang berhubungan dengan penelitian ini.

1.6.2.3 Metode Wawancara

Metode wawancara yaitu melakukan tanya jawab langsung dengan pihak yang terkait dengan masalah yang diteliti.

1.6.3 Metode Perancangan

Metode perancangan yang digunakan dalam penelitiaan ini antara lain:

1.6.3.1 UML

UML ini sebagai penjelasan secara grafis mengenai elemen-elemen yang ada dalam sistem penelitian ini. Diagram-diagram dalam

UML ada 4, yakni: *Use Case Diagram, Activity Diagram, Squence Diagram,* dan *Class Diagram.*

1.6.3.2 Flowchart

Flowchart adalah bagan yang menggambarkan prosedur dalam penyelesaian masalah.

1.7 Sistematika Penulisan

Pada bagian ini merupakan urut-urutan dan sistematika penulisan yang dilakukan. Adapun sistematika penulisan yang digunakan oleh penulis diuraikan ke dalam lima bab, yaitu:

BAB I

PENDAHULUAN

Dalam bab ini penulis menuliskan materi yang menjadi penyempurnaan dati latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan laporan.

BAB II

LANDASAN TEORI

Bab landasan teori merupakan tinjauan pustaka yang dijadikan dasar dari analisis dan pengembangan (pembahasan), mengurangi teori-teori yang mendasari laporan, metode penelitian, dan pembahasan secara detail. Sehingga pada bab ini dapat berupa pembahasan dari referensi yang

dijadikan rujukan, definisi-definisi atau model yang langsung berkaitan dengan ilmu atau keperluan penelitian.

BAB III

ANALISIS DAN PERANCANGAN

Dalam bab ini penulis menguraikan tentang gambaran obyek penelitian serta data yang dipergunakan untuk memecahkan masalah-masalah yang dihadapi, berkaitan dengan kegiatan penelitian. Selanjutnya dalam bab ini menguraikan analisi permasalahan yang terdapat pada kasus yang diteliti. Analisis yang diuraikan meliputi analisis terhadap masalah sistem yang dibuat, analisis hasil solusinya, analisis kebutuhan terhadap sistem yang dibuat, dan analisis kelayakan system yang dibuat. Perancangan system yang akan dibuat dengan membuat rancangan untuk sistem yang akan diujikan.

BAB IV

IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini penulis memaparkan hasil-hasil dari tahapan penelitian, tahap analisis, desain, implementasi desain, hasil uji coba, dan implementasi sistemnya, secara teoritik. Penjelasan teoritik yang digunakan adalah teoritik kualitatif, kuantitatif, atau secara statistic.

BAB V

KESIMPULAN DAN SARAN

Dalam bab ini penulis mampu menjawab pertanyaan dalam rumusan masalah, hipotesis, dan bukti-bukti yang dihasilkan dan akhirnya akan ditarik kesimpulan apakah hipotesis yang diajukan itu diterima atau sebaliknya.