BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi jaringan komputer menyebabkan keterkaitannya satu komputer dengan komputer lainnya. Hal ini tidak hanya membuka banyak peluang dalam pengembangan aplikasi komputer tetapi juga membuat peluang adanya ancaman terhadap pengubahan dan pencurian data.

Sebuah aplikasi yang melintasi jaringan publik seperti internet diasumsikan dapat diakses oleh siapapun termasuk orang-orang atau pihak-pihak yang memang berniat untuk mencuri atau mengubah data. Oleh karena itu, untuk melindungi data terhadap akses, pengubahan dan penghalangan yang tidak dilakukan oleh pihak yang berwenang, peranti keamanan data yang melintas di jaringan komputer harus disediakan.

FBI, dari data *Internet Crime Complaint Center* (IC3) tercatat sejak April 2014 hingga June 2015. IC3 mendapatkan 992 laporan kasus *ransomware* di mana pada kasus ini *CryptoWall* sebagai pembuat masalah. Skema penipuan keuangan ini menargetkan individu dan pembisnis, awal mulanya korban mengklik iklan, email, atau lampiran yang terinfeksi, atau mengunjungi situs web yang terinfeksi. Setelah perangkat korban terinfeksi dengan varian *ransomware*, file korban menjadi terenkripsi.

Dalam penyediaan pengamanan diperlukannnya sebuah Keamanan Jaringan dimana bertujuan untuk menanggulangi ancaman serta mencegah terjadinya penyusupan. Dalam penyedian Keamanan Jaringan tersebut adapun rancangan perangkat desktop *JAVA*. Menerapkan kriptografi *hybrid* dengan algoritma RSA, AES 128 dan SHA1 sebagai pondasi Keamanan Jaringan yang di gunakan. Sehingga diharapkan aplikasi *dekstop* ini dapat menjaga kerahasiaan file document serta informasi-informasi penting.

Berdasarkan latarbelakang yang telah dijabarkan di atas, maka penulis mengangkat skripsi dengan judul **"Analisis Dan Perancangan Kriptografi *Hybrid* Dengan Algoritma RSA, AES128, dan SHA1 Untuk Pengiriman File Document".**

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 merancang aplikasi kriptografi *hybrid* (RSA, AES128 dan SHA1) untuk pengiriman file (document)?

1.3 Batasan Masalah

Agar masalah yang diteliti tidak menyimpang maka diperlukan suatu batasan masalah. Dalam suatu penelitian ini peneliti membatasi masalah yang diteliti, yaitu pada aplikasi pengamanan pengiriman email enkripsi dan dekripsi pesan dengan algoritma kriptografi *hybrid* (RSA, AES128, dan SHA1). Adapun

batasan masalah pada penelititan ini adalah sebagai berikut :

1. Aplikasi ini berbasis *desktop Windows.*
2. Aplikasi ini hanya menggunakan algoritma meliputi: (RSA, AES128, dan SHA1) saja dalam proses enkripsi dekripsi pesan dan (document).
3. Krtiptografi *Hybrid* yang dimaksud adalah penggabungan algoritma simetri dan asimetri (RSA dengan AES128) kemudian menerapkan *digital signature* dengan fungsi *hash* SHA1.
4. Inputan ke apliksi berupa teks tertulis dan file (document) yang bisa dienkripsi dan didekripsi .
5. Peneliti tidak berfokus sepenuhya 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* (RSA, AES128, dan SHA1) dengan menggunakan Windows 10.
7. Pembuatan program pendukung aplikasi kriptografi *Hybrid* (RSA, AES128, dan SHA1) menggunakan bahasa pemrograman *JAVA.*
8. Pembuatan program menggunakan aplikasi pendukung yaitu (*NetBeans 8.0.1*).
9. Algoritma kriptografi, bahasa pemrograman, sistem operasi, dan program pendukung selain yang disebutkan tidak dibahas dan tidak digunakan dalam penelitian ini.
10. Proses enkripsi dan dekripsi pada aplikasi ini memiliki batasan-batasan

pada tiap proses algortima dan akan dijelaskan 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 kedalam lingkungan permasalahan yang sebenarnya dengan cara terlibat langsung dalam proses pembuatan aplikasi.
4. Memperluas serta meningkatkan kemampuan mahasiswa sebagai bekal untuk memasuki 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* (RSA, AES128, dan SHA1) mampu digunakan sebagai aplikasi yang bisa merahasiakan pesan dan file (document) yang sulit dipecahkan dengan perhitungan tanpa bantuan komputer.
2. Menghasilkan sebuah program aplikasi berbasis *desktop* yang berfungsi untuk mengenkripsi dan dekripsi pesan dan file (document) dengan algoritma kriptografi *Hybrid* (RSA, AES128, dan SHA1) berbasis *JAVA*.
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. Dapat memberikan perlindungan terhadap informasi pesan maupun file (document) agar tidak mudah untuk diakses oleh pihak-pihak yang tidak bertanggung jawab.
2. Pengguna aplikasi tidak perlu khawatir lagi terhadap pihak yang sengaja ingin mencuri data dan informasi penting di karenakan file documen anda sudah aman dengan proses enkripsi.

3. Dapat digunakan sebagai bahan kajian untuk mengembangkan teknologi informasi terutama faktor yang berhubungan dengan keamanan.

1.6 Metode Penelitian

Penulis melakukan beberapa metode penelitian dan mengumpulkan data untuk memperoleh jawaban atas permasalahan yang penulis ungkapkan. Adapun metode-metode yang penulis lakukan adalah sebagai berikut:

1.6.1 Metode Pengumpulan Data

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

1.6.1.1 Metode Studi Kepustakaan

Untuk mendukung perancangan aplikasi ini penulis menggunakan metode studi kepustakaan sebagai referensi. Pustaka yang digunakan antara lain *journal*, *website* atau penelitian sebelumnya yang berkaitan dengan penelitian ini.

1.6.1.2 Metode Browsing

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

1.6.1.3 Metode Wawancara

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

1.6.2 Metode Analisis

Metode analisis yang digunakan dalam penelitian ini adalah analisis SWOT.

1.6.2.1 Analisis SWOT

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

1.6.2.2 Analisis Kebutuhan Sistem

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

1.6.2.3 Analisis Kelayakan Sistem

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

1.6.3 Metode Perancangan

Metode perancangan yaitu dengan menggunakan perancangan UML (*Unified Modelling Language*), dan User Interface.

1.7 Sistematika Penulisan

Sistematika laporan disusun menggunakan dasar-dasar penulisan karya ilmiah. Metode ini dilakukan agar dalam penyusunan laporan menjadi lebih teratur dan mudah dipahami. Sistematika penulisan laporan pada skripsi adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas tentang tinjauan pustaka dan dasar-dasar teori yang digunakan.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini menjelaskan tentang analisis sistem, analisis kebutuhan sistem, analisis kelayakan sistem dan perancangan sistem yang diusulkan.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini membahas mengenai hasil program yang akan diimplementasikan ke dalam perangkat computer.

BAB V PENUTUP

Bab ini berisi tentang Kesimpulan dari keseluruhan laporan dan saran yang membangun untuk menambah kesempurnaan aplikasi.