BAB I

PENDAHULUAN

1.1 Latar Belakang

Berkembangannya teknologi saat ini sudah sangat pesat, begitupun dengan kebutuhan manusia terhadap informasi. “Informasi adalah data yang diolah menjadi bentuk yang lebih berguna bagi yang menerimanya” [1]. Dengan adanya informasi, manusia mendapatkan pengetahuan dan nilai yang bermanfaat untuk dirinya maupun orang lain. Pesan merupakan salah satu bentuk penyampaian informasi yang saat ini banyak digunakan.

“Pesan adalah suatu komponen dalam proses komunikasi berupa paduan dari pikiran dan perasaan seseorang dengan menggunakan lambang, bahasa/lambang-lambang lainnya disampaikan kepada orang lain" [2].

Pesan membawa sebuah informasi yang memiliki tingkat privasi yang berbeda. Tidak semua pesan dapat diketahui oleh publik, beberapa pesan memiliki tingkat privasi yang harus dijaga dari orang-orang yang tidak memiliki hak akses kepada pesan tersebut. Keamanan dalam pesan dibutuhkan, karena dalam pengiriman sebuah pesan masih belum terjamin kemananya, hal ini disebabkan pesan yang dikirim masih dalam bentuk *plaintext* (pesan asli). Maka dari itu dibutuhakan sebuah sistem keamanan pada layanan pesan yang mampu menjaga integritas dan keamanan isi pesan agar isi pesan (pesan asli) hanya dapat dibaca oleh penerima aslinya, untuk itu isi pesan yang akan dikirimkan terlebih dahulu harus dienkripsi dengan algoritma atau ilmu kriptiografi.

Ilmu kriptografi adalah ilmu mengenai teknik penyandian “naskah asli” atau disebut dengan istilah *plaintext*, yang susunannya diacak menggunakan suatu kunci

enkripsi menjadi “naskah acak yang sulit dibaca” atau disebut dengan istilah *chipertext*. Dengan dilakukan proses ini maka seseorang yang tidak memiliki kunci dekripsi tidak bisa membaca pesan asli [3].

Pada umumnya dalam ilmu kriptografi terdapat teknik kriptografi yang dikelompokan menjadi tiga kelompok berdasarkan sifat kuncinya, teknik yang pertama dikenal dengan teknik kriptografi tanpa kunci, teknik ini disebut teknik kriptografi klasik. Teknik berikutnya adalah teknik dengan kunci simetris, teknik ini menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, teknik ini memiliki performa yang cukup baik, namun memiliki kekurangan pada proses pengaturan kunci, dimana pihak yang akan bertukar informasi harus menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Teknik yang ketiga adalah teknik kriptografi kunci asimetris, pada teknik ini digunakan kunci yang berbeda dalam proses enkripsi dan dekripsi, pihak yang akan mengirimkan informasi melakukan enkripsi dengan menggunakan kunci publik dari penerima informasi, kemudian penerima pesan melakukan dekripsi dengan kunci *private* miliknya untuk mendapatkan pesan asli, tingkat keamanan teknik ini sangat ditentukan oleh permasalahan matematis yang digunakan. AES *(Advanced Encryption Standard)* dan ECC *(Elliptic-curve Cryptography)* merupakan salah satu teknik kriptografi asimetris.

AES *(Advanced Encryption Standard)* adalah teknik merahasiakan sandi atau data sesuai standarisasi dari FIPS *(Federation Information Processing Standard)* versi 197 dengan menggunakan algoritma Rijndael [4]. Algoritma AES ini dapat digunakan untuk enkripsi dan dekripsi pesan teks pada layanan keamanan pesan.

ECC *(Elliptic-curve Cryptography)* merupakan teknik kriptografi asimetris dengan menggunakan pendekatan permasalahan matematis *elliptic-curve discrete logarithm*, permasalahan matematis ini dipercaya lebih susah untuk dipecahkan, sehingga dipercaya memiliki tingkat keamanan yang baik pula [5].

Elliptic-curve dapat dikomunikasikan dengan metode lainnya yang telah ada sebelumnya, untuk keperluan tandatangan digital *elliptic curve* biasanya dikombinasikan dengan algoritma *DSA*, sedangkan untuk proses enkripsi dan dekripsi *elliptic-curve* biasanya digabungkan dengan algoritma El Gamal.

Pada tugas akhir ini akan diimplementasikan skema kriptografi penggabungan antara AES *(Advanced Encryption Standard)* dan ECC *(Elliptic-curve Cryptography)*, penggabungan ini bertujuan untuk mendapatkan performa dan tingkat keamanan yang lebih baik, karena dengan menggabungkan AES dan ECC akan memberikan *level security* yang lebih baik.

Berdasarkan uraian diatas maka perlunya dibangun sebuah sistem penyandian pesan teks pada layanan kemanan pesan yang akan penulis bahas dalam sebuah tugas akhir yang berjudul **" IMPLEMENTASI ALGORTIMA *ADVANCED ENCRYPTION STANDARD* (AES) DAN *ELLIPTIC-CURVE CRYPTOGRAPHY* (ECC) PADA KEAMANAN LAYANAN PESAN".**

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah di jelaskan diatas, penulis memiliki beberapa rumusan masalah terkait dengan permasalahan tersebut, yaitu :

Bagaimana menerapkan kombinasi algoritma AES *(Advanced Encryption Standard)* dan ECC *(Elliptic-curve Cryptography)* pada proses penyandian layanan pesan teks ?

1.3 Tujuan Penelitian

Adapun tujuan dari pembuatan tugas akhir ini yaitu :

Perancangan aplikasi penyandian layanan pesan teks yang menerapkan kombinasi algoritma AES (Advanced Encryption Standard) dan ECC (Elliptic-curve Cryptography)

1.4 Manfaat Penelitian

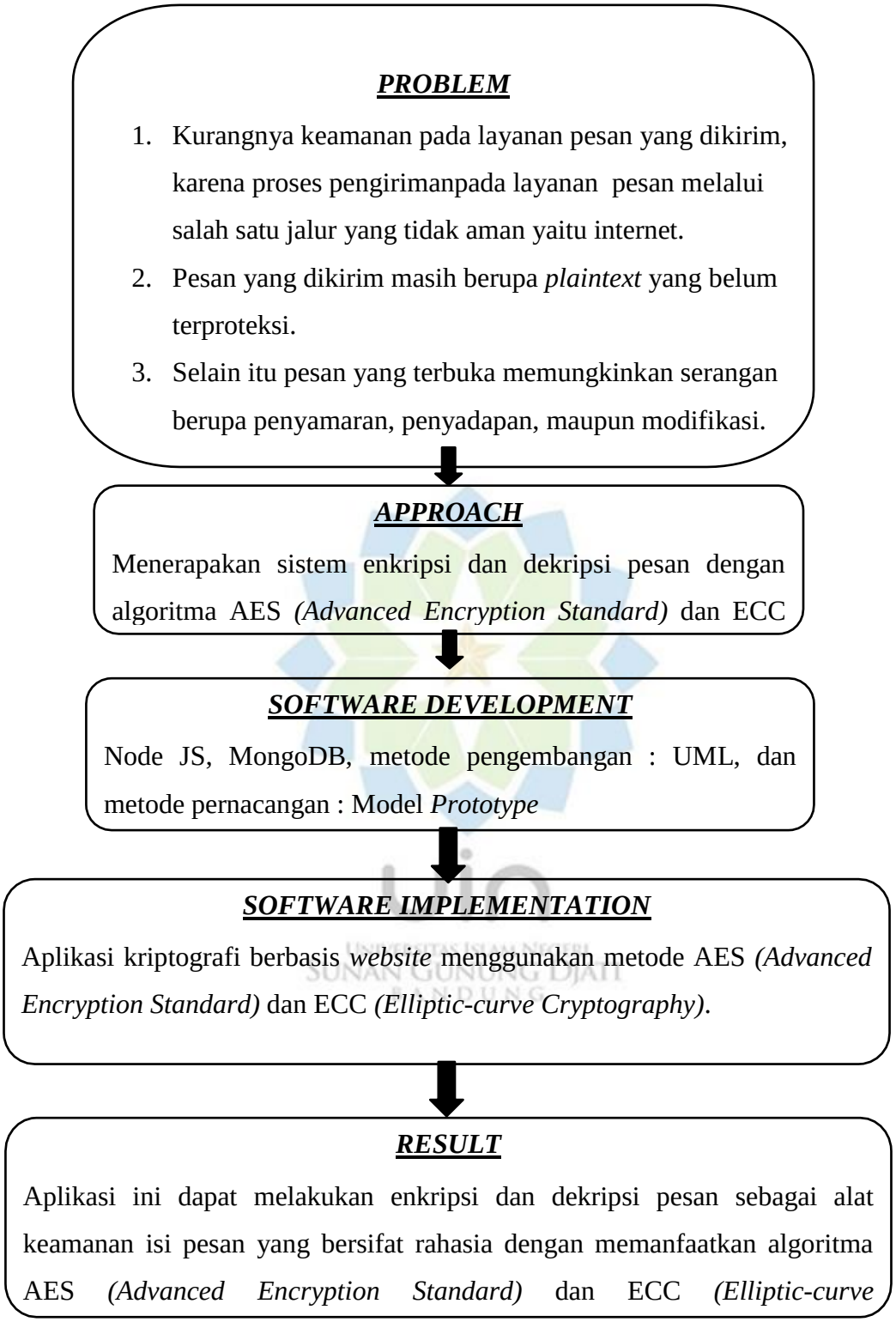
Adapun manfaat dari penelitian Implementasi Algortima *Advanced Encryption Standard* (AES) dan *Elliptic-curve Cryptography* (ECC) pada keamanan layanan pesan adalah untuk menghasilkan sebuah perangkat lunak berbasis *website* yang dapat mengamankan data terutama dalam layanan pesan.

1.5 Batasan Masalah

1. *Input* berupa pesan teks.
2. Tugas akhir ini tidak menangani masalah pengiriman file atau transfer file.
3. Bahasa pemrograman yang digunakan adalah *Node JS*.
4. Output dari aplikasi berupa *plaintext* yang dapat dibaca oleh penerima.

1.6 Kerangka Pemikiran

Kerangka pemikiran merupakan uraian tentang bagaimana peneliti mengalirkan jalan pemikiran secara logis dalam rangka memecahkan masalah yang telah di rumuskan.



Gambar 1. 1 Kerangka Pemikiran

1.7 Metodologi Pengerjaan Tugas Akhir

1.7.1 Tahap Pengumpulan Data

Untuk mengumpulkan berbagai data yang di butuhkan untuk kelancaran penyusunan tugas akhir ini ada tahap tahap yang perlu di lakukan sebagai berikut:

1. Wawancara (interview)

   Melakukan survei terhadap beberapa orang untuk mencari kekurangan dari ekripsi dan dekripsi pesan ini dan tanya jawab dengan orang tersebut untuk menentukan kebutuhan apa saja yang perlu di terapkan.

2. Studi Literatur

   Metode pengumpulan data dalam penelitian ini adalah studi pustaka yaitu pengumpulan data dengan cara mengumpulkan materi-materi literatur dari perpustakaan yang bersumber dari buku-buku, jurnal ilmiah, dan situs di internet yang berkaitan dengan judul penelitian.

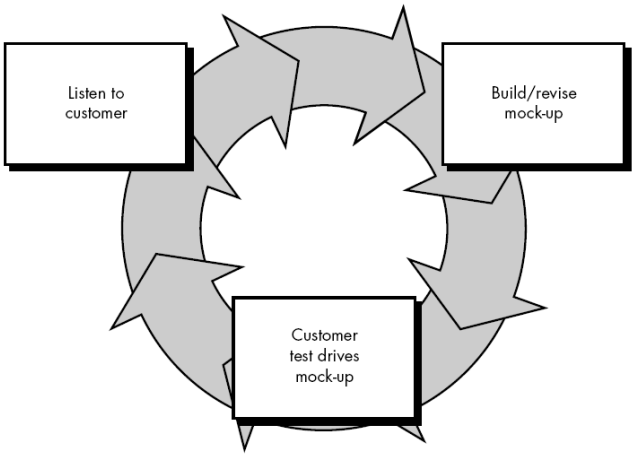
3. Pemodelan Sistem

   Dalam pemodelan sistem dilakukan perancangan aplikasi menggunakan metode *Unified Modeling Language* (UML), kemudian di implementasikan pada pembangunan aplikasi berbasis *website.*

4. Model Proses Pengembangan Perangkat lunak

   Metode pengembangan perangkat lunak yang digunakan pada penelitian ini yaitu menggunakan metode *prototype*. *Prototyping* merupakan salah satu metode pengembangan perangkat lunak yang banyak digunakan. Dengan metode *prototyping* ini pengembang dan pelanggan dapat saling berinteraksi selama proses pembuatan sistem.

Gambar 1.2 menunjukkan secara keseluruhan arsitektur yang dimiliki *prototype.*



Gambar 1. 2 Arsitektur Prototype *[6]*

Adapun tahapan dalam siklus pegembangan *prototype* yaitu:

1. Analisis kebutuhan. Tahap analisis kebutuhan (*requirements*) dilakukan untuk mengidentifikasi tentang siapa yang akan menggunakan sistem dan apa yang dibutuhkan oleh pengguna dari sistem.
2. Perancangan sistem. *System design* atau perancangan sistem merupakan tahap dimana sistem digambarkan ke dalam model- model tertentu berdasarkan hasil analisis pada tahap sebelumnya.
3. Pengkodean. Untuk membangun sistem ke dalam bentuk asli, maka hasil perancangan diterjemahkan ke dalam kode-kode tertentu.
4. Pengujian. Pengujian (*testing*) perlu dilakukan dalam setiap pengembangan sistem. Tujuannya yaitu untuk mengukur apakah sistem yang telah dikembangkan berjalan dengan baik dan benar serta sesuai dengan kebutuhan pengguna.

5. Implementasi Setelah semua tahap berjalan dengan baik dan hasil pengujian menunjukkan hasil yang sesuai dengan kebutuhan, maka sistem dapat diimplentasikan dan siap digunakan oleh pengguna dengan tetap melakukan pemeliharaan (*maintenance*) secara berkala untuk menjaga kesehatan *system*.

1.8 Sistematika Penulisan

Sistematis penulisan pada skripsi ini di bagi kedalam beberapa bab, yang masing-masing bab sudah mempunyai tujuan-tujuannya. Berikut penjelasanya :

BAB I PENDAHULUAN

Bab I (satu) pendahuluan yang membahas permasalahan yang berhubungan dengan penyusunan laporan tugas akhir diantaranya latar belakang, rumusan masalah, Batasan masalah, sistematika penulisan, tujuan dan manfaat penelitian.

BAB II LANDASAN TEORI

Bab II (dua) landasan teori menjelaskan teori-teori yang berhubungan dengan masalah yang di kemukakan pada penelitian ini, dan juga teori-teori yang di gunakan dalam perancangan dan implementasi.

BAB III METODELOGI PENELITIAN

Bab III (tiga) ini membahas mengenai metode penelitian dan kebutuhan perangkat lunak dan perangkat keras yang di gunakan.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab IV (empat) disini di bahas teknik implementasi serta pengujian sistem yang sudah selesai, termasuk preview dari hasil akhir pada aplikasi.

BAB V PENUTUP

Bab V (lima) berisi kesimpulan dan saran untuk pengembangan aplikasi ke tahapan yang lebih lanjut dalam upaya untuk memperbaiki dan mengembangkan aplikasi yang lebih baik.

DAFTAR PUSTAKA

Daftar Pustaka berisi semua sumber tertulis atau tercetak yang pernah di kutip dan di gunakan pada proses penyusunan.

LAMPIRAN

Berisi semua dokumen yang di gunakan dalam proses penyusunan dan perancangan seperti source code, kelengkapan dokumen dan lain sebagainya.