

BAB I

PENDAHULUAN

1.1. Latar Belakang

Provinsi Kepulauan Bangka Belitung telah menjadi salah satu provinsi yang berkembang di Indonesia. Provinsi yang berdiri pada November tahun 2000 ini juga telah memiliki Perguruan Tinggi Negeri yaitu Universitas Bangka Belitung (UBB) yang diresmikan pada tahun 2006. Sebagai satu-satunya Universitas di Bangka Belitung, harapan UBB tentunya adalah menjadi Kampus Peradaban dan menjadi Universitas Riset dan Teknologi pada tahun 2035.

Sebagai satu satunya Universitas di Bangka Belitung, Pelayanan yang baik harus diberikan bagi mahasiswa/i. Namun terkadang pelayanan yang diberikan masih ada sedikit yang kurang baik secara teknis dan non teknis, misalnya AC yang sudah rusak di ruang kelas masih ada yang belum diganti, dosen yang jarang masuk kelas, toilet mahasiswa yang sering kotor, dan lain sebagainya. Hal ini tentunya harus menjadi perhatian dan perlu diperbaiki untuk kedepannya.

Pada salah satu fakultas di UBB yakni Fakultas Teknik, telah menyediakan kotak kosong untuk menampung kritik dan saran terhadap pelayanan di Fakultas Teknik. Akan tetapi, kotak tersebut sering tidak digunakan untuk mahasiswa yang ingin memberikan kritik dan sarannya. Hal ini dikarenakan kekhawatiran mahasiswa yang ingin memberikan kritik namun tak ingin diketahui oleh orang lain.

Web bisa menjadi alternative media untuk menyalurkan kritik dan saran. *Web* merupakan salah satu sumber daya internet yang berkembang pesat[1]. Beberapa perusahaan dan instansi telah menggunakan *web* sebagai media sarana untuk aktivitasnya. Dengan adanya aplikasi kritik dan saran berbasis *web*, proses pelayanannya bisa lebih mudah dan efektif. Namun tentunya ini masih belum aman karena *hacker* bisa saja menyadap pesan yang telah dikirimkan.

Untuk mengamankan pesan tersebut, diperlukanlah suatu sistem keamanan yang kuat. Pesan harus diproses dan diubah dalam bentuk kode sebelum dikirimkan. Ilmu yang mempelajari tentang cara-cara pengamanan data dikenal dengan istilah kriptografi[2]. Salah satu algoritma kriptografi yang bisa digunakan dalam sistem ini adalah algoritma RSA. Proses perumusan RSA didasarkan pada Teorema Euler, sedemikian sehingga menghasilkan kunci umum dan kunci pribadi yang saling berkaitan. Sehingga meskipun proses enkripsi dan dekripsi menggunakan dua kunci yang berbeda hasilnya akan tetap benar. Kunci umum dan kunci pribadi yang digunakan adalah suatu bilangan prima, dan disarankan bilangan prima yang besar. Hal ini digunakan untuk pencegahan usaha pemecahan teks rahasia, karena semakin besar bilangan prima yang digunakan sebagai kunci maka semakin sulit mencari bilangan besar sebagai faktornya[2].

Beberapa penelitian terdahulu yang menjadi referensi penulis untuk penelitian ini yaitu penelitian yang dilakukan oleh[3] yang berjudul Penerapan Kriptografi RSA Dalam Mengamankan File Teks Berbasis PHP“. Penelitian[4] yang berjudul “Rancang Bangun E-Voting Dengan Menggunakan Keamanan Algoritma *Rivest Shamir Adleman* (RSA) Berbasis *Web* (Studi Kasus : Pemilihan Ketua Bem FMIPA)”. Selanjutnya penelitian yang dilakukan oleh[5] yang berjudul “Optimasi Enkripsi *Password* Menggunakan Algoritma *Blowfish*”. Penelitian yang dilakukan oleh[6] yang berjudul “Enkripsi Dan Dekripsi File Dengan Algoritma *Blowfish* Pada Perangkat *Mobile* Berbasis *Android*”. Penelitian yang dilakukan oleh[7] yang berjudul “Implementasi Algoritma *Vigenere Cipher* dan *RSA Rebalanced* pada Pengamanan Citra dalam Skema Kriptografi *Hybrid*”. Penelitian yang dilakukan oleh[8] yang berjudul “Analisis Perbandingan Algoritma Kriptografi Klasik *Vigenere Cipher* Dan *One Time Pad*”. Penelitian yang dilakukan oleh[9] yang berjudul “Pengamanan Dokumen Menggunakan Metode RSA (*Rivest Shamir Adleman*) Berbasis *Web*”.

Meninjau permasalahan diatas, diperlukan aplikasi yang bisa menampung kritik dan saran tanpa bisa diketahui oleh orang lain. Oleh karena itu, penulis berencana melakukan penelitian untuk bahan laporan skripsi dengan judul “**Aplikasi Pelayanan**

Kritik dan Saran menggunakan Algoritma RSA di Fakultas Teknik Universitas Bangka Belitung Berbasis Web.”

1.2. Rumusan Masalah

Perumusan masalah dari penelitian ini adalah bagaimana membangun aplikasi pelayanan kritik dan saran menggunakan algoritma RSA berbasis *web*?

1.3. Batasan Masalah

Dalam penyusunan penelitian ini akan dibatasi pada masalah berikut :

1. Aplikasi yang dibuat berbasis *web*.
2. Aplikasi menggunakan algoritma RSA.
3. Aplikasi hanya membahas tentang proses enkripsi, proses dekripsi, dan proses pembangkitan kunci.
4. Program yang dibuat pada sistem ini yaitu proses enkripsi dan dekripsi pada sebuah pesan.

1.4. Tujuan dan Manfaat Penelitian

1.4.1. Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Aplikasi yang dibuat bisa mengamankan kritik dan saran mahasiswa dari orang yang tidak berhak.
2. Menerapkan metode algoritma RSA ke aplikasi berbasis web.

1.4.2. Manfaat Penelitian

Manfaat dari penelitian ini adalah :

1. Mahasiswa bisa mengirimkan kritik dan saran dengan aman.
2. Menciptakan inovasi baru di lingkup Fakultas Teknik Universitas Bangka Belitung.

1.5 Sistematika Penulisan

Sistematika penulisan yang disajikan pada penelitian ini antara lain :

BAB I PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang, rumusan masalah, serta tujuan dan manfaat penelitian.

BAB II LANDASAN TEORI

Di bab ini, penulis menguraikan tentang teori-teori yang berkaitan dengan judul.

BAB III METODOLOGI PENELITIAN

Pada bab ini, penulis menjelaskan tentang Metodologi Penelitian dalam pembuatan Aplikasi Pelayanan Kritik dan Saran menggunakan Algoritma RSA di Fakultas Teknik Universitas Bangka Belitung Berbasis *Web*.

BAB IV PEMBAHASAN DAN HASIL

Di bab ini, penulis membahas tentang permasalahan yang ada beserta penyelesaiannya mengenai aplikasi yang dirancang.

BAB V PENUTUP

Di bab ini, penulis menjelaskan tentang kesimpulan dan saran dari aplikasi yang dirancang.