BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Pandemi *Covid-19* seolah merubah budaya kerja dan interaksi, yang sebelumnya berjalan secara konvensional menjadi serba *digital*. Salah satu contoh perubahan dapat terlihat pada proses registrasi peserta pelatihan dan sertifikasi yang ada di Universitas Pembangunan Jaya. Setiap calon peserta diwajibkan untuk mengisi formulir registrasi secara langsung melalui unit Jaya *Center for Advanced Learning* (JCAL). Adanya pembatasan dalam beraktivitas, saat ini proses registrasi sudah beralih ketahap *digital*, di mana peserta melakukan proses registrasi melalui *website* secara *online*. Dibalik kemudahan tersebut, ternyata ada dampak lain yang ditimbulkan, khususnya dalam hal pengamanan data peserta. Maraknya kasus pembobolan data dan sistem yang terjadi belakangan ini, membuat pihak pengelola JCAL perlu berhati-hati.

Berdasarkan referensi yang berhasil dikumpulkan dijumpai beberapa cara untuk melakukan proses pengamanan data, salah satunya menggunakan konsep enkripsi dan dekripsi. Oleh karena itu, penulis mempelajari dan menerapkan dua jenis algoritma pada sistem dari aplikasi, yaitu algoritma *advanced encryption standard* sebagai proses enkripsi dan dekripsi, dan algoritma *base64* sebagai proses *encoding* dan *decoding*.

Ilmu kriptografi sendiri merupakan proses untuk mengamankan suatu informasi dengan cara mengenkripsi informasi tersebut. Untuk penerapan kriptografi dalam sistem registrasi yang dilakukan secara *online*, maka algoritma *AES* dan *base64* memiliki kelebihan pada proses enkripsi pesan menggunakan *cipher key* dalam hal ini data hasil enkripsi menjadi susah untuk diretas, yang mana *cipher key* sendiri diperlukan untuk proses enkripsi dan dekripsi data. Namun, kelemahan dari penggunaan algoritma *AES* dan *base64* sebagai penerapan ilmu kriptografi adalah proses enkripsi yang sensitif terhadap perubahan di mana apabila ada satu huruf atau lebih yang diubah pada hasil enkripsi, maka data tidak dapat didekripsi dengan kata lain hasil enkripsi data rusak (*broken data*).

Masalah yang terjadi jika *data security system* tidak diterapkan, yaitu apabila terjadi *data leakage* pada sistem atau pada *server*, maka data rentan terhadap

pengaksesan secara ilegal, pengungkapan data oleh pihak yang tidak bertanggung jawab, dan manipulasi data. Hal-hal tersebut masuk dalam kategori kejahatan siber.

Algoritma *AES* dan *base64* dapat digunakan untuk membangun *data security system* dengan keamanan ganda sehingga hasil enkripsi menjadi sulit untuk diretas karena terdapat dua fase yang harus dilalui, yaitu *decoding* dan *decrypting*. Dengan adanya penerapan dari kedua algoritma tersebut maka sistem pada aplikasi dapat mengamankan informasi, terutama yang bersifat sensitif di mana isi dari informasi tersebut hanya boleh diketahui oleh pihak tertentu.

Dalam hal ini dengan adanya penerapan seni ilmu kriptografi pada aplikasi berbasis *web* maka informasi rahasia yang terdapat pada database dari *server* aplikasi dapat diamankan jika terjadi pembobolan data yang dilakukan oleh pihak yang tidak bertanggung jawab terutama dari kejahatan siber. Untuk sistem registrasi pelatihan dan sertifikasi yang dilakukan oleh peserta secara *online* pada aplikasi *web*, maka sistem keamanan data (*data security system*) merupakan hal yang penting dalam menjaga kerahasiaan informasi.

1.2. Identifikasi Masalah

Walaupun data yang dibobol dan diambil secara ilegal hanyalah merupakan *plaintext* atau teks biasa. Namun, data tersebut dapat dijual, dan dapat terjadinya *cyber extortion* atau pemerasan kepada pengguna yang datanya berhasil diretas oleh para kriminal siber.

Penyebab permasalahan tersebut karena data yang disimpan dalam database sama sekali tidak dienkripsi, yang mana mengakibatkan data mudah untuk dibobol (*data breaching*) dan diretas dari *server*. Oleh karena itu, untuk menjaga supaya pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak adalah dengan mempelajari ilmu kriptografi, dan algoritma yang dapat dipakai untuk kriptografi supaya *data security system* dapat dikelola pada sistem.

1.2.1. Rumusan Masalah

1. Bagaimana cara untuk melakukan proses pengamanan data hasil registrasi peserta pelatihan dan sertifikasi?

2. Bagaimana cara untuk menerapkan algoritma *advanced encryption standard* dan *base64* sebagai algoritma pengamanan data?

1.2.2. Batasan Penelitian

Penulis perlu menentukan dengan jelas apa yang akan dibuat dan dikerjakan, jika tidak maka nantinya penelitian skripsi ini tidak akan terselesaikan. Karena bidang pada perancangan aplikasi *web* luas, maka penulis merancang aplikasi berbasis *web* yang dapat untuk mengamankan data pribadi, dan informasi yang bersifat sensitif.

Berikut beberapa batasan dalam penelitian ini.

1. Sistem keamanan data diterapkan pada sistem registrasi peserta pelatihan dan sertifikasi yang sudah dikembangkan sebelumnya oleh penulis.
2. Metode pengamanan data enkripsi menggunakan algoritma *advanced encryption standard* dan *base64*.
3. Proses enkripsi dan dekripsi berlangsung disisi *client* dengan menggunakan beberapa *field* diantaranya, nomor identitas, nama lengkap, tanggal lahir, nomor telepon, nama instansi, pekerjaan, program studi, nama *pentrasfer* di rekening, nama bank *pentransfer*, tanggal *transfer*, dan nominal *transfer*.
4. Pengujian dilakukan disisi *client* dan *server* dengan membuktikan bahwa proses enkripsi dan dekripsi sudah berhasil dilakukan melalui indikasi, berupa *alert* bahwa data telah berhasil tersimpan pada database *system*.

1.3. Tujuan Penelitian

1. Menerapkan algoritma *advanced encryption standard* dan *base64* untuk seni ilmu kriptografi dalam mengamankan data pribadi pendaftar dari *cybercriminals*.
2. Mengamankan data yang terdapat pada database *system* dari *cyberattack*, jika data dari database *system* terjadi *data leakage* maka tetap aman karena telah terenkripsi.
3. Menerapkan algoritma *base64 encoding* untuk mengubah *ciphertext* menjadi *binary text* dalam *format string American standard code for information interchange* untuk tujuan *double security*.

4. Merancang *data security system* dengan penerapan algoritma *advanced encryption standard* dan *base64*, maka dengan ini hasil enkripsi (*encipher*) akan menjadi semakin susah untuk didekripsi (*decipher*) dan diretas oleh *cybercriminals*.

1.4. Manfaat Penelitian

Adapun manfaat penelitian yang diharapkan adalah sebagai berikut ini.

1. Manfaat untuk calon pengguna

   Dapat memberikan solusi dalam pengamanan data-data pribadi pengguna aplikasi dengan menerapkan algoritma kriptografi pada sistem registrasi yang dilakukan secara *online*.

2. Manfaat untuk ilmu pengetahuan

   Dengan pelaksanaan penelitian ini diharapkan diperoleh pengetahuan tentang bagaimana membangun aplikasi sistem registrasi pendaftaran pelatihan dan sertifikasi dengan menerapkan algoritma *advanced encryption standard* 256 *bit* dan algoritma *base64 encoding*.

3. Manfaat untuk peneliti

   Dengan pelaksanaan penelitian ini diharapkan penulis memperoleh pengetahuan dan keterampilan tentang bagaimana cara membangun aplikasi sistem registrasi pendaftaran pelatihan dan sertifikasi dengan menerapkan algoritma *advanced encryption standard* 256 *bit* dan algoritma *base64 encoding*.

1.5. Kebaruan

Penerapan algoritma *advanced encryption standard* 256 *bit* dan algoritma *base64 encoding* digunakan sebagai bentuk penerapan algoritma pengamanan data hasil registrasi peserta pelatihan dan sertifikasi. Hal ini merupakan kontribusi kebaruan yang dikembangkan oleh penulis setelah tahap pengembangan aplikasi *web* dilakukan. Dengan adanya mekanisme pengamanan data diharapkan dapat memberikan jaminan terhadap kualitas data dan juga dapat meminimalisir terjadinya serangan dari pihak yang tidak bertanggung jawab.

1.6. Kerangka Penulisan

Kerangka penulisan dalam skripsi ini terdiri dari 6 bab yang terdiri dari bab pendahuluan, tinjauan pustaka, metode penelitian, perencanaan, hasil dan pembahasan, dan diakhiri dengan penutup. Lebih rinci kerangka penulisan disusun sebagai berikut ini.

1. BAB I PENDAHULUAN

   Bab ini berisi latar belakang masalah, identifikasi masalah, tujuan penelitian, manfaat penelitian, kebaruan, dan kerangka penulisan.
2. BAB II TINJAUAN PUSTAKA

   Bab ini berisi gambaran mengenai pencapaian terdahulu, dan tinjauan teoritis yang dijadikan oleh penulis sebagai preferensi pada penelitian.
3. BAB III METODE PENELITIAN

   Bab ini menjelaskan mengenai paradigma penelitian, dan metode penelitian.
4. BAB IV PERENCANAAN

   Bagian ini berisi langkah-langkah penelitian, dan rancangan pengujian mengenai algoritma kriptografi yang diterapkan oleh penulis pada aplikasi berbasis *web*.
5. BAB V HASIL DAN PEMBAHASAN

   Pada bab ini berisikan beberapa pembahasan hasil dari uraian perancangan, dan pembahasan hasil dari uraian uji coba.
6. BAB VI PENUTUP

   Bab ini terdiri dari kesimpulan, dan saran dari seluruh penelitian yang telah dilakukan.