

# BAB I

## PENDAHULUAN

### I.1 Latar Belakang

Ijazah merupakan selembar kertas atau bukti nyata yang berarti bagi seseorang yang telah menempuh atau menyelesaikan studi pendidikan baik itu tingkat dasar, menengah pertama, menengah atas, sarjana hingga program Magister. Akan tetapi pada zaman yang mutakhir ini, perkembangan teknologi yang ada sering dimanfaatkan kepentinagn pribadi. Untuk membuat segalanya serba mudah, pada aspek pendidikan pemanfaatan teknologi digunakan untuk pemalsuan ijazah. Kasus ijazah palsu marak diperbincangkan akhir-akhir ini. Karena untuk menentukan keaslian suatu ijazah hanya dengan melegalisir *photocopy* ijazah atau dengan menghubungi pihak sekolah atau lembaga yang mengeluarkan ijazah tersebut.

Masalah ijazah palsu merupakan salah satu aspek penting yang harus diperhatikan. Dalam hal ini, sangat terkait dengan betapa pentingnya keaslian ijazah tersebut sebagai salah satu bukti kelulusan seseorang dalam studi atau pendidikannya. Ijazah menjadi sangat penting dan dibutuhkan sebagai persyaratan melamar pekerjaan atau hanya sebagai identitas pendidikan seseorang.

Untuk menyelesaikan masalah tersebut, dibutuhkan suatu aplikasi yang dapat mengidentifikasi keaslian suatu ijazah dengan cepat dan akurat. Dengan memanfaatkan teknologi yang ada, identifikasi ijazah bisa mempercepat seseorang untuk mengecek suatu keabsahan ijazahnya. Menurut Saiful Azad dan AL-Sakib Khan Pathan (2015, hlm.184) bahwa MD5 dibagi menjadi 4 pengolahan blok tahap analog, yang disebut sebagai putaran, di mana setiap putaran terdiri dari 16 operasi serupa berdasarkan fungsi  $F$  non-linear, penambahan modular, dan rotasi kiri. Oleh karena ini, ada tiga jenis operasi di MD5 yaitu operasi bit-bijaksana Boolean, penambahan modular, dan operasi pergeseran sirkulus. Semua operasi yang sangat cepat pada mesin 32-bit, yang membuat MD5 cukup cepat. Pada penelitian sebelumnya yang berjudul "Studi Algoritma Rijndael Dalam Sistem Keamanan Data" oleh Eko Satrio menyimpulkan bahwa AES sangat aman untuk

melindungi data, karena panjang kunci dan variatif pada kunci AES bisa mencegah dari segala macam ancaman.

Penelitian ini akan mengaplikasikan metode enkripsi dan dekripsi menggunakan algoritma *Advanced Encryption Standard* (AES) dan algoritma *hash* pada *Message Digest 5* (MD5) untuk mengidentifikasi keaslian ijazah dengan menggunakan bahasa pemrograman berbasis web untuk kemudahan dalam mengakses. Secara umum, tujuan penelitian ini adalah mendapatkan suatu rancangan aplikasi identifikasi keaslian suatu ijazah yang cepat dan akurat, sehingga dapat dimanfaatkan berbagai pihak, instansi, lembaga pendidikan atau bahkan perorangan.

## I.2 Perumusan Masalah

Berangkat dari latar belakang dapat diuraikan rumusan masalah untuk mengidentifikasi keaslian suatu ijazah dengan membangkitkan nilai integritas dan mengenkripsi serta dekripsi informasi ijazah agar cepat dan akurat. Lalu di rumuskan dalam rumusan masalah sebagai berikut :

- a. Bagaimana mengimplementasikan fungsi *hash* dengan menggunakan metode *Message Digest 5* (MD5) untuk mengidentifikasi keaslian suatu ijazah dengan cepat dan akurat dalam pemrograman PHP berbasis web?
- b. Bagaimana menerapkan metode *Advanced Encryption Standard* (AES) untuk keamanan basis data ?

## I.3 Ruang Lingkup Penelitian

Dalam melakukan penelitian mengidentifikasi keaslian suatu ijazah dilakukan beberapa batasan-batasan sebagai berikut :

- a. Menerapkan metode *hash* pada web berbasis php dengan metode *Message Digest 5* (MD5).
- b. Menerapkan metode enkripsi dan dekripsi pada basis data dengan metode *Advanced Encryption Standard* (AES).
- c. Implementasi perancangan dibuat dengan menggunakan *software*, Netbeans, Xampp, Adobe Photoshop CS5 dan Web Browser.

- d. Aplikasi ini diperuntuhkan kepada pihak, instansi, lembaga pendidikan atau perorangan yang ingin mengetahui keaslian suatu ijazah.
- e. Aplikasi ini hanya untuk mengidentifikasi keaslian suatu ijazah dengan cepat dan akurat.

#### **I.4 Tujuan dan Manfaat Penelitian**

Adapun tujuan dan manfaat yang ingin dicapai oleh penulis dalam penelitian ini sebagai berikut :

- a. Dengan mengimplementasikan metode *Message Digest 5* (MD5) dapat mempercepat pihak – pihak yang ingin mengidentifikasi suatu ijazah.
- b. Dengan mengimplementasikan metode *Advanced Encryption Standard* (AES) pada mempersulit pihak – pihak yang ingin membaca data yang tersimpan dibasis data.
- c. Dengan menerapkan aplikasi ini, dapat meminimalisir ijazah palsu.
- d. Aplikasi dapat dikemabangkan dalam berbagai bidang yang khususnya mengutamakan kecepatan, keaslian dan keamanan.

#### **I.5 Luaran yang diharapkan**

Luaran yang diharapkan dari penelitian yang penulis kerjakan dengan memanfaatkan algoritma *Advanced Encryption Standard* (AES) dan *hash Message Digest5* (MD5) adalah agar penerapan model aplikasi ini dapat diterapkan atau direalisasikan dalam kehidupan nyata serta dengan mengidentifikasi keaslian suatu surat penting seperti ijazah dengan cepat dan akurat.

#### **I.6 Sistematika Penulisan**

Dalam penulisan ini, pembahasan disajikan dalam lima bab agar pembahasan lebih teratur dan jelas serta setiap bab diberikan uraian masalah dengan sistematika pembahasa sebagai berikut :

## BAB I PENDAHULUAN

Bab ini berisikan tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan dan manfaat, luaran yang diharapkan, serta sistematika penulisan pembuatan skripsi.

## BAB II LANDASAN TEORI

Pada bab ini menjelaskan tentang teori-teori pemecahan masalah yang berhubungan dan digunakan untuk mendukung dalam pembuatan skripsi ini.

## BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang cara metode penelitian, kerangka berfikir, identitas masalah, studi kepustakaan, perancangan, pengujian, implementasi, jadwal penelitian dll.

## BAB IV ANALISA, PERANCANGAN DAN IMPLEMENTASI

Bab ini menjelaskan analisi, perancangan dan implementasi algoritma *Message Digest 5* (MD5) untuk mempercepat identifikasi ijazah dan *Advanced Encryption Standard* (AES) untuk keamanan data, perancangan aplikasi dan juga menjelaskan hasil penelitian yang telah dilakukan.

## BAB V PENUTUPAN

Bab ini menjelaskan mengenai simpulan yang didapatkan setelah melakukan penelitian dan saran peneliti untuk pengembangan yang dilakukan oleh peneliti selanjutnya.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN