



### **Hak cipta dan penggunaan kembali:**

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

### **Copyright and reuse:**

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

## **BAB II**

### **LANDASAN TEORI**

Analisis dalam skripsi ini akan dilakukan dengan berlandaskan studi literatur sebagai berikut :

#### **2.1 BPMI / Biro Penjaminan Mutu Internal**

Merupakan salah satu instansi yang ada didalam UMN yang bertugas untuk menjamin supaya setiap proses dan bagian mengimplementasikan penjaminan kualitas di setiap prosesnya. Ruang lingkup kerja BPMI mencakup satu universitas tempat instansi itu berada. BPMI akan bekerja sama dengan seluruh fakultas, biro dan LPPM (Lembaga Penelitian dan Pengabdian Masyarakat). Fungsi dari BPMI adalah sebagai berikut ([www.spmi.umn.ac.id](http://www.spmi.umn.ac.id)):

1. BPMI berperan dalam proses Akreditasi untuk mendapatkan status dan peringkat akreditasi dengan Badan Akreditasi Nasional Perguruan Tinggi (BAN-PT) dan Lembaga Akreditasi Mandiri (LAM) Perguruan Tinggi.
2. BPMI menyampaikan luaran yang diperlukan SPME.
3. BPMI mempersiapkan, membangun, dan menyimpan mutu UMN dalam pangkalan.

#### **2.2 SPMI / Sistem Penjaminan Mutu Internal**

Adalah struktur organisasi UMN yang melaksanakan kegiatan penjaminan mutu secara keseluruhan ([www.spmi.umn.ac.id](http://www.spmi.umn.ac.id)). SPMI juga memiliki siklus kegiatan kerja yang telah ditentukan, berikut ini adalah siklusnya:

1. Penetapan Standar Pendidikan Tinggi dengan menentukan dan dokumentasi standar-standar yang ditetapkan di lingkungan UMN.
2. Pelaksanaan Standar Pendidikan Tinggi di lingkungan UMN.
3. Melakukan evaluasi atas pelaksanaan Standar Pendidikan Tinggi di lingkungan UMN dengan membandingkan Standar Pendidikan Tinggi dan pelaksanaannya.

4. Pengendalian Standar Pendidikan Tinggi yang ditetapkan oleh UMN dengan melakukan identifikasi permasalahan dan analisis faktor-faktor penyebab kurang terlaksananya Standar Pendidikan Tinggi di UMN.
5. Peningkatan Standar Pendidikan Tinggi dengan memperbaiki dan meningkatkan standar yang sudah ditetapkan sebelumnya di UMN.
6. Setiap siklus berlaku satu semester sesuai dengan jadwal dan kegiatan proses pembelajaran di UMN.

SPMI mempunyai sistem dokumentasi dalam menjalankan penjaminan mutu. Sistem dokumentasi tersebut akan menggunakan dokumen-dokumen berikut ini :

1. Dokumen dasar yang menjadi rujukan pengembangan sistem yaitu: Visi, Misi dan tujuan UMN, Statuta, Organisasi dan Tata Kerja UMN, Rencana strategis UMN, dan Pedoman proses pembelajaran.
2. Dokumen SPMI, yaitu: Kebijakan Mutu, Standar Mutu, Prosedur Mutu, Instruksi Kerja, dan Formulir SPMI.
3. Dokumen Audit, yang meliputi: Prosedur Mutu pelaksanaan Audit internal mutu, Prosedur mutu penilaian kinerja UMN, dan Laporan hasil audit internal.

### **2.3 MD5/ Message Digest 5 Algorithm**

Algoritma kriptografi yang menghasilkan summary sebuah pesan (file, stream data) dengan menggunakan *hash function*. Contoh dari *Message Digest* bisa dipergunakan pada pengubahan pesan penting. MD5 merupakan salah satu fungsi dari *hash* yang yang populer, MD5 bekerja dengan cara mengubah data yang telah diinput ke dalam fungsi menjadikan data tersebut mempunyai sebuah panduan sehingga data yang diubah bisa digunakan sebagai panduan untuk menentukan input tersebut.

Dengan MD5 ini akan dihasilkan serangkaian data yang terdiri dari huruf dan angka yang sudah diacak dan disusun, menjadikan data yang telah diinput menjadi bentuk yang tidak teratur dan sepanjang 32 karakter. MD5 pertama kali di kenalkan oleh R Rivest pada tahun 1992 (Md. Alam Hossain, 2012), MD5 dibangun untuk mengembangkan algoritma sebelumnya yakni MD4.

Kelemahan MD5 adalah tabrakan antar data yang disebabkan oleh MD5 itu sendiri.

#### **2.4 Hash Code**

adalah salah satu cara untuk menerima data dan mengeluarkan bentuk data yang pasti (Mark Stevens, 2012). *Hash code* juga mempunyai nama lain yaitu *Message digest*. Salah satu cara yang paling efisien dalam melakukan kriptografi digital adalah dengan menggunakan *hash code*. Data yang telah diubah oleh *hash code* kemudian akan dimasukkan ke dalam tabel, di dalam tabel tersebut akan di sortirkan data-data yang memungkinkan pengguna untuk mencari data yang diinginkan secara cepat. Dengan tabel tersebut juga dapat dicocokkan data yang telah diubah menjadi kode. Perubahan data ini sering kali dilakukan untuk melancarkan pembacaan beberapa data yang dianggap sulit untuk diterjemahkan.

#### **2.5 PHP/ PHP Hypertext Preprocessor**

Adalah *open source* yang sering digunakan untuk mengembangkan aplikasi web dan bisa digabungkan dengan HTML (Kalpesh Adhatrao, 2013). PHP merupakan salah satu bahasa yang banyak digunakan dalam pengembangan *website*, oleh karena itu banyak aplikasi yang dapat berinteraksi dengan bahasa PHP. Ada banyak dari keuntungan dari penggunaan PHP berikut adalah beberapa dari keuntungan tersebut (Petr Sladek, 2011):

1. Tidak perlu aplikasi tertentu
2. *Browser* cukup untuk melakukan akses ke dalam PHP
3. PHP mendukung file XML

#### **2.6 Studi Pendahuluan**

Dalam studi ini, penulis mempelajari dari beberapa jurnal yang telah diterbitkan dan membandingkan metode yang dipakai oleh jurnal-jurnal tersebut. Tabel di bawah ini akan menjelaskan perbedaan jurnal tersebut.

No	Tahun	Pengarang	Judul	Kesimpulan
1.	2011	Piyush Gupta, Sandeep Kumar	<i>A COMPARATIVE ANALYSIS OF SHA AND MD5 ALGORITHM</i>	MD5 lebih cepat dalam waktu pengubahan data.
2.	2012	Md. Alam Hossain, Md. Kamrul Islam, Subrata Kumar Das and Md. Asif Nashiry	<i>CRYPTANALYZIN G OF MESSAGE DIGEST ALGORITHMS MD4 AND MD5</i>	Merekomendasikan MD5 dibandingkan MD4.
3.	2013	Mary Cindy Ah Kioon, Zhao Shun Wang and Shubra Deb Das	<i>SECURITY ANALYSIS OF MD5 ALGORITHM IN PASSWORD STORAGE</i>	Memperlambat komputasi MD5 sehingga menjadi lebih sulit di pecahkan.

Tabel 2. 1 Perbandingan Jurnal

Berdasarkan tabel di atas model aplikasi ini akan menggunakan cara yang di sarankan oleh jurnal nomor tiga agar data yang telah di ubah di tambahkan isinya sehingga data tersebut semakin sulit untuk di pecahkan. Hal baru yang akan penulis lakukan adalah mengubah data yang akan di MD5, bukan *password* melainkan menggunakan tanggal, waktu, *penggunaname*, serta nama file yang telah di *upload* ke dalam *database* serta menempelkan MD5 ke dalam PICA yang di *upload* ke dalam *database*.