# APLIKASI KEAMANAN LEMBAR HASIL STUDI MENGGUNAKAN ALGORITMA *MESSAGE DIGEST* 5
## Studi Kasus : Fakultas Teknik Universitas Muhammadiyah Bengkulu

Yovi Apridiansyah[1] , Muhammad Husni Rifqo[2]

[1,2]Program Studi Informatika, Fakultas Teknik, Universitas Muhammadiyah Bengkulu
Jl. Bali, Bengkulu 38119

[1]yoviapridiansyah@gmail.com
[2]kokoahzani@gmail.com

Abstrak: Keamanan komputer merupakan tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab (D.Howard, 1997). Dengan adanya keamanan komputer dapat mencegah tindak kejahatan dalam bidang komputer. Salah satu metode keamanan komputer yaitu dengan menggunakan Algoritma *Message Digest* 5 untuk keaman LHS dengan menerapkan *MD5 file* dapat di enkripsi dan didekripsi oleh *user*. Dengan menggunakan metode algoritma *missage digest* 5 yang mempunyai fungsi *hash* (prosedur terdefinisi atau fungsi matematika yang mengubah variabel dari suatu data yang berukuran besar menjadi lebih sederhana) kriptografi yang digunakan secara luas dengan *hash* value 128-bit. *MD5* dimanfaatkan dalam berbagai aplikasi keamanan, dan umumnya digunakan untuk menguji integritas sebuah *file*. Tujuan dari penelitian ini diharapkan informasi dari LHS tersebut dapat terjaga dengan baik tanpa dapat dimanipulasi oleh orang lain untuk merusak informasi yang ada. Dengan adanya aplikasi keamanan LHS menggunakan algoritma *MD5* diharapakan dapat mempermudah mahasiswa, pertama dengan adanya sistem keamanan LHS pada Fakultas Teknik Universitas Muhammadiyah Bengkulu ini informasi keaslian LHS tidak dapat dimanipulasi oleh pihak lain. Kedua, dengan adanya aplikasi keamanan ini dapat mempermudah mahasiswa dalam melihat lembar hasil studi mereka.
Kata Kunci : *Kriptografi, Enkripsi, Dekripsi, MD5*

***Abstarct: Computer security is measures the prevention of attacks for the user or a network userunresponsible (D.Howard, 1997). With the security of your computer can prevent crimes in the field of the computer. One of the computer security motede namely using the Missage Digest 5 algorithm for security LHS by applying MD5 files can be in the encryption and decrypted by the user. By using this method the missage digest 5 algorithm that have a hash function (Undefined selection procedure or function of mathematics which change the variables from a large amounts of data to be more simple) cryptographic used widely with hash value 128-bit. MD5 utilized in various security applications and generally used to testing file integrity. The purpose of this research is expected information from the LHS can be well maintained without can be manipulated by other people to damage the existing information. With the existence of the security applications using LHS MD5 hope algorithm can facilitate the students, first with the existence of the security system on the LHS Faculty of Engineering Muhammadiyah University of Bengkulu is genuine LHS information cannot be manipulated by the other party. The second, with the existence of this security application can facilitate the students in view of their study results sheet.***
***Keywords: cryptography, encryption, decrypt, MD5***

## I. PENDAHULUAN

Teknologi memiliki peran penting dalam perkembangan umat manusia, terutama ketika manusia mengelola organisasi. Konsep teknologi berimplikasi bahwa setiap kegiatan *admin*istrasi dan manajemen merupakan teknologi dan pasti memerlukan teknologi. Posisi teknologi tersebut semakin lebih penting ketika inovasi tersebut berhasil menggabungkan teknologi informasi dan telekomunikasi (misalnya internet). Penggunaan teknologi informasi dan komunikasi ternyata membuat kinerja organisasi lebih efektif, efisien dan kompetitif [1].

Dalam perkembangannya, bukan hanya informasi yang menjadi penting, tetapi perkembangan teknologi pun menjadi hal yang sangat penting khususnya teknologi keamanan komputer. Sebagai contoh, sekarang ini manusia berlomba-lomba membangun sebuah sistem untuk melindungi informasi yang mereka miliki dari ancaman virus ataupun orang lain yang berusaha untuk mengambil, memanipulasi ataupun hanya untuk sekedar merusak informasi itu.

Berbagai aplikasi sistem informasi dibidang pendidikan, antara lain: Sistem Informasi Akademik (SIA), *e-learning*, *e-library*, *e-assesment*, *etutor*, portal pendidikan dan berbagai aplikasi lainnya memberikan kemudahan kepada *stake holder* (mahasiswa, dosen, staff *admin*istrasi, eksekutif dan bagian luar kampus) disebuah perguruan tinggi untuk melaksanakan Tridharma perguruan tinggi dan meningkatkan kualitas pembelajaran dan pelayanan. SIA yang telah banyak diimplementasikan diberbagai kampus di Indonesia telah memberikan dampak kemudahan dari berbagai kampus untuk mengelola *admin*istrasi kegiatan akademik mahasiswa dan kampus, seperti informasi data mahasiswa, nilai, informasi jadwal, materi kuliah dari setiap dosen pengajar dan beberapa informasi lainnya [2].

Sistem informasi akademik di Universitas Muhammadiyah Bengkulu khususnya berupa layanan *online* (*website*) berperan aktif pada kegiatan penunjang kegiatan perkuliahan, dalam penelitian ini penulis mengimplementasikan keamanan LHS *online* yang ada pada Fakultas Teknik Universitas Muhammadiyah Bengkulu. Berdasarkan studi kasus pada sistem akademik yang ada pada Universitas Muhammadiyah Bengkulu, penelitian menerapkan bagaimana algoritma *MD5* untuk keamanan LHS. Penelitian ini penting dilakukan untuk keamanan LHS mahasiswa dari bentuk virus ataupun orang lain yang berusaha untuk mengambil, memanipulasi ataupun hanya untuk sekedar merusak informasi itu.

Dengan menggunakan metode algoritma *message digest* 5. Algoritma ini mempunyai fungsi *hash* (prosedur terdefinisi atau fungsi matematika yang mengubah variabel dari suatu data yang berukuran besar menjadi lebih sederhana) kriptografi yang digunakan secara luas dengan *hash value* 128-bit. *MD5* dimanfaatkan dalam berbagai aplikasi keamanan, dan umumnya digunakan untuk meguji integritas sebuah *file*. Dengan adanya sebuah sistem keamanan untuk LHS *online* ini diharapkan informasi dari LHS tersebut dapat terjaga dengan baik tanpa dapat dimanipulasi oleh orang lain untuk merusak informasi yang ada.

## II. LANDASAN TEORI

### A. *Enkripsi*

Proses utama dalam suatu algoritma kriptografi adalah enkripsi dan dekripsi. Enkripsi merubah sebuah *plaintext* ke dalam bentuk *ciphertext*. Pada mode ECB (*Elekctronic Codebook*), sebuah blok pada *plaintext* dienkripsi ke dalam sebuah blok *ciphertext* dengan panjang blok yang sama. Blok *cipher* memiliki sifat bahwa setiap blok harus memiliki panjang yang sama (misalnya 128 bit). Namun apabila pesan yang dienkripsi memiliki panjang blok terakhir tidak tepat 128 bit, maka diperlukan mekanisme *padding*, yaitu penambahan bit-bit *dummies* untuk menggenapi menjadi panjang blok yang sesuai; biasanya *padding* dilakukan pada blok terakhir *plaintext. Padding* bada blok terakhir bisa dilakukan dengan berbagai macam cara, misalnya dengan penambahan bit-bit tertentu. Salah satu contoh penerapan *padding* dengan cara menambahkan jumlah total *padding* sebagai *byte* terakhir pada blok terakhir *plaintext*. Misalnya panjang blok adalah 128 bit (16 *byte*) dan pada blok terakhir terdiri dari 88 bit (11 *byte*) sehingga jumlah *padding* yang diperlukan adalah 5 *byte*, yaitu dengan menambahkan angka nol sebanyak 4 *byte*, kemudian menambahkan angka 5 sebanyak satu *byte*. Cara lain dapat juga menggunakan penambahan karakter *end-of-file* pada *byte* terakhir lalu diberi *padding* setelahnya [2].

### B. *Dekripsi*

Dekripsi merupakan proses kebalikan dari proses enkripsi, merubah *ciphertext* kembali ke dalam bentuk *plaintext*. Untuk menghilangkan *padding* yang diberikan pada saat proses enkripsi, dilakukan berdasarkan informasi jumlah *padding* yaitu angka pada *byte* terakhir setelahnya [3].

## III. LEMBAR HASIL STUDI (LHS)

Lembar Hasil Studi atau LHS adalah kartu yang menunjukkan nilai dan prestasi mahasiswa pada semester tertentu. Lembar Hasil Studi dapat didownload dan dicetak oleh mahasiswa bersangkutan pada system akademik tempat kuliah masing-masing. LHS yang dicetak oleh mahasiswa tidak dapat digunakan dalam proses *admin*istrasi akademik. Oleh karena itu, setiap semester, mahasiswa harus meminta LHS yang dicetak dan disahkan oleh program studi bersangkutan. Selain menyimpan nilai di *database*, program studi juga harus menyimpan LHS yang dicetak dan disahkan.

### A. Algoritma *Message Digest 5*

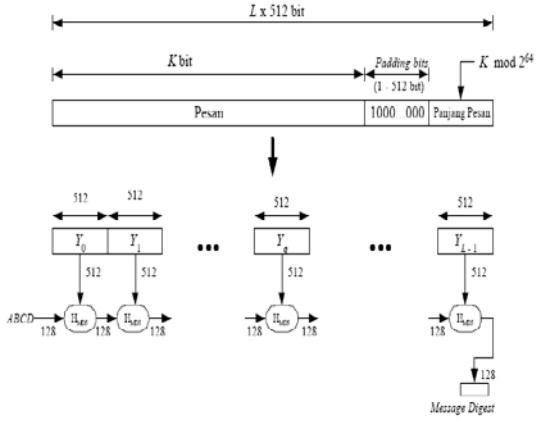
*MD5* merupakan singkatan dari *Message-Digest algortihm 5*, adalah fungsi *hash* (prosedur terdefinisi atau fungsi matematika yang mengubah variabel dari suatu data yang berukuran besar menjadi lebih sederhana) kriptografik yang digunakan secara luas dengan hash value 128-bit. *MD5* dimanfaatkan dalam berbagai aplikasi keamanan, dan umumnya digunakan untuk meguji integritas sebuah *file*. Enkripsi menggunakan *MD5* masih mendominasi sebagian besar aplikasi *PHP*. Enkripsi *MD5* dianggap *strong* karena enkripsi yang dihasilkannya bersifat ‘ *one way hash*’. Berapapun *string* yang di enkripsi hasilnya tetap sepanjang 32 karakter [4].

*Message Digest* 5 (*MD5*) juga merupakan salah satu dari serangkaian algoritma *Message Digest* yang didesain oleh Professor Ronald Rivest dari MIT. Saat kerja analitik menunjukkan bahwa pendahulu *MD5* -*MD4*- mulai tidak aman, *MD5* kemudian didesain pada tahun 1991 sebagai pengganti dari *MD4* (kelemahan *MD4* ditemukan

oleh Hans Dobbertin). *MD5* banyak digunakan pada bermacam macam aplikasi termasuk *SSL/TLS*, *IPSec* dan protokol-protokol kriptografi lainnya. *MD5* juga biasa digunakan pada implementasi *Timestamping Mechanism*, *Commitment Schemes*, dan aplikasi pengecekan integritas pada *online software*. *MD5* tidak memiliki sistem pengamanan seperti persamaan matematika, namun untuk setiap fungsi *hash* , domain D dan range R kita membutuhkan tiga hal berikut :

1. *Pre Image Resistance* : jika diberi suatu nilai y ε R, maka kita tidak akan dapat mencari suatu nilai x ε D dimana h(x)=y.
2. *Second Pre Image Resistance* : jika diberi suatu nilai x ε D, maka kita tidak akan dapat mencari nilai x' ε D dimana h(x)=h(x').
3. *Collision Resistance* : kita tidak akan dapat mencari nilai x,x' ε D dimana h(x)=h(x').

Fungsi *hash* yang banyak digunakan dalam kriptografi *MD5* ini fungsi *hash* yang digunakan algoritma MD5. MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan *message digest* yang panjangnya 128 bit . Langkah-langkah dalam pembuatan *message digest* secara garis besar adalah sebagai berikut:




Gambar 1. Pembuatan *message digest* dengan algoritma *MD5*

Menilik dari gambar diatas, secara garis besar pembuatan *message digest* ditempuh melalui empat langkah, yaitu :

1. Penambahan bit-bit pengganjal (*padding bits*).
   - Pesan ditambah dengan sejumlah bit pengganjal sedemikian hingga panjang pesan (dalam satuan bit) kongruen dengan 448 modulo 512
   - Jika panjang pesan 448 bit, maka pesan tersebut ditambah dengan 512 bit menjadi 960 bit. Jadi, panjang bit-bit pengganjal adalah dari 1 sampai 512.
   - Bit-bit pengganjal terdiri dari sebuah bit 1 diikuti beberapa sisanya bit 0.
2. Penambahan nilai panjang pesan semula.
   - Pesan yang telah diberi bit-bit pengganjal selanjutnya ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula.
   - Jika panjang pesan > 264 maka yang diambil adalah panjangnya dalam modulo 264. Dengan kata lain, jika panjang pesan semula adalah *k* bit, maka 64 bit yang ditambahkan menyatakan *k* modulo 264.
   - Setelah ditambah dengan 64 bit, panjang pesan sekarang menjadi kelipatan 512 bit.
3. Inisialisasi penyangga (*buffer*) MD.
   - *MD5* membutuhkan 4 buah penyangga (*buffer*) yang masing-masing panjangnya 32 bit. Total panjang penyangga adalah 4 x 32 = 128 bit.
   - Keempat penyangga ini menampung hasil antara dan hasil akhir. Keempat penyangga ini diberi nama A, B, C, dan D. Setiap penyangga diinisialisasi dengan nilai-nilai (dalam notasi *HEX*) sebagai berikut :

A = 01234567

B = 89ABCDEF

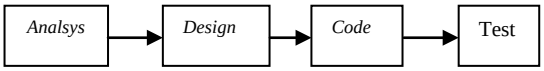
C = FEDCBA98

D = 76543210

Pengolahan pesan dalam blok berukuran 512 bit. Proses berikutnya adalah pesan dibagi menjadi L buah blok yang masing-masing panjangnya 512 bit ($Y_0$ sampai $Y_{L-1}$). Setelah itu setiap blok 512 bit diproses bersama dengan penyangga MD yang menghasilkan keluaran 128 bit, dan ini disebut $H_{MD5}$.

## IV. METODE PENELITIAN

Dalam penelitian ini model pengembangan sistem yang digunakan yaitu model incremental. *Incremental* model merupakan model pengembangan sistem pada *software engineering* berdasarkan *requirement software* yang dipecah menjadi beberapa fungsi atau bagian sehingga model pengembangannya secara bertahap. dilain pihak ada mengartikan model *incremental* sebagai perbaikan dari model *waterfall* dan sebagai standar pendekatan *topdown.*



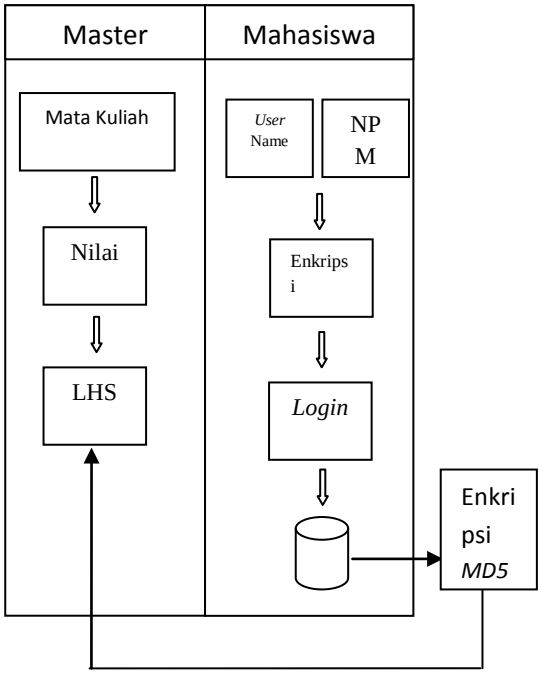

Gambar 2. Desain Pemodelan *Incremental*

### C. *Analisis*

Analisis data diartikan sebagai upaya mengolah data menjadi informasi, sehingga karakteristik atau sifat-sifat data tersebut dapat dengan mudah dipahami dan bermanfaat untuk menjawab masalah-masalah yang berkaitan dengan kegiatan penelitian.

### D. *Design*

Dalam tahapan *architecture design* ini merupakan perancangan software yang terbuka agar dapat diterapkan sistem pembangunan per-bagian pada tahapan selanjutnya. Dalam studi kasus penelitian ini yaitu Aplikasi Keamanan Lembar Hasil Studi Menggunakan Algoritma Message Digest 5 (Studi Kasus Fakultas Teknik Universitas Muhammadiyah Bengkulu).




Gambar 3. Skema Enkripsi *MD5*

### E. *Code*

Dalam tahapan *code* ini merupakan lanjutan dari proses *design* yang telah dikerjakan, untuk aplikasi keamanan lembar hasil studi menggunakan algoritma messege digest 5 studi kasus Fakultas Teknik Universitas Muhammadiyah Bengkulu yaitu menggunakan bahasa pemprograman *PHP MySQL*, *Java* dan *Eclipse* yang merupan aplikasi tambahan untuk algoritma *message di*gest 5. Diharapkan nantinya dengan menggunakan program-program yang telah disebutkan diatas algoritma *message disgest* 5 dapat bekerja dengan baik dalam keamanan LHS.

Contoh Aplikasi Enkripsi MD5 misalnya, kata “supono” akan di enkripsi menggunakan *message digest* 5 akan berubah menjadi “9008a28a8a5d07db3091d9114a839268″.
Jumlahnya akan menjadi 32 karakter, berapapun *input*, akan menghasilkan output enkripsi sejumlah 32.

F. *Test*

Dalam tahapan *test* ini merupakan proses lanjutan dari pengkodean program yang di buat. Dalam tahapan ini *user* melakukan pengujian dengan metode pengujian yang dipakai adalah *black box testing*. *black box testing* atau *test* fungsional adalah pengujian program yang dilakukan oleh pengembang (Programmer) dengan memberikan *input* tertentu dan melihat hasil yang didapatkan dari *input* tersebut. dengan kata lain, *black box testing* terfokus pada fungsionalitas sistem. dalam melaksanakan *black box* testing, penulis menggunakan beberapa kriteria yang akan diujikan. kriteria-kriteria tersebut antara lain :

1. Kemampuan *Interface* sistem untuk menjalankan fungsinya.
2. Kemampuan sistem untuk menjalankan fungsi *interface*.
3. Kemampuan sistem untuk menangani *input-input form* yang berada di luar *boundary* sistem.
4. Kemampuan sistem untuk menangani masalah keamanan.

## V. HASIL DAN PEMBAHASAN

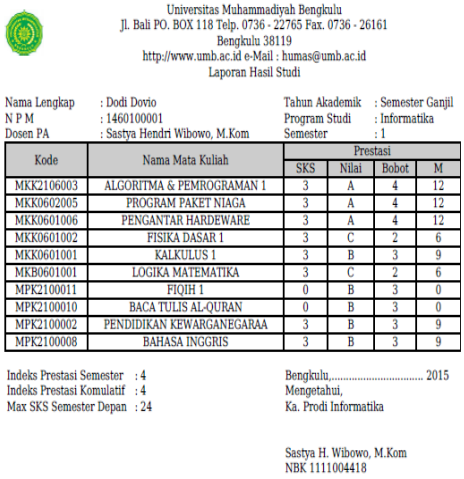
Pada tahap implementasi sistem, rancangan dan desain sistem diimplementasikan dengan bahasa pemrograman menggunakan bahasa pemrograman PHP MySQL.

A. *Menu Utama*


Gambar 4. Tampilan Menu Utama Aplikasi

Tampilan menu utama ini terdapat master data yang terdiri dari sub menu Mahasiswa, Mata Kuliah Prodi dimana pada masing-masing sub menu tersebut untuk proses *input* data. Transkip Nilai yang terdiri dari Nilai mata kuliah dan LHS mahasiswa pada sub menu ini merupakan proses *input* data mata kuliah dan hasil LHS yang akan dicetak.


Gambar 5. Tampilan *Input* Data Mahasiswa



Universitas Muhammadiyah Bengkulu
Jl. Bali PO. BOX 118 Telp. 0736 - 22765 Fax. 0736 - 26161
Bengkulu 38119
http://www.umb.ac.id e-Mail : humas@umb.ac.id
Laporan Hasil Studi

Nama Lengkap : Dodi Dovio
N P M : 1460100001
Dosen PA : Sastya Hendri Wibowo, M.Kom
Tahun Akademik : Semester Ganjil
Program Studi : Informatika
Semester : 1

| Kode | Nama Mata Kuliah | Prestasi | | | |
|---|---|---|---|---|---|
| | | SKS | Nilai | Bobot | M |
| MKK2106003 | ALGORITMA & PEMROGRAMAN 1 | 3 | A | 4 | 12 |
| MKK0602005 | PROGRAM PAKET NIAGA | 3 | A | 4 | 12 |
| MKK0601006 | PENGANTAR HARDEWARE | 3 | A | 4 | 12 |
| MKK0601002 | FISIKA DASAR 1 | 3 | C | 2 | 6 |
| MKK0601001 | KALKULUS 1 | 3 | B | 3 | 9 |
| MKB0601001 | LOGIKA MATEMATIKA | 3 | C | 2 | 6 |
| MPK2100011 | FIQIH 1 | 0 | B | 3 | 0 |
| MPK2100010 | BACA TULIS AL-QURAN | 0 | B | 3 | 0 |
| MPK2100002 | PENDIDIKAN KEWARGANEGARAA | 3 | B | 3 | 9 |
| MPK2100008 | BAHASA INGGRIS | 3 | B | 3 | 9 |

Indeks Prestasi Semester : 4
Indeks Prestasi Komulatif : 4
Max SKS Semester Depan : 24

Bengkulu..... 2015
Mengetahui,
Ka. Prodi Informatika

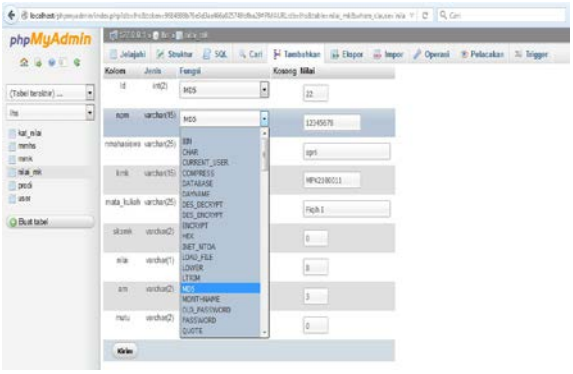
Sastya H. Wibowo, M.Kom
NBK 1111004418

Gambar 6. LHS Mahasiswa

Proses selanjutnya simpan file pdf LHS mahasiswa ke local disk c- xampp-htdocs-lhsencrypt- passwordpdf-hasil. Setelah file pdf tersimpan maka proses selanjutnya yaitu enkripsi file agar kerahasian dalam informasi LHS dapat terjaga dengan aman.


Gambar 7. Proses Enkripsi LHS

Adapun proses enkripsi menggunakan algoritma *MD5* sebagai berikut :

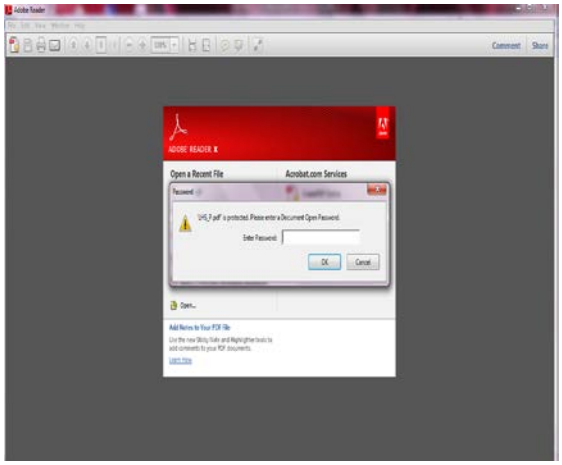



Gambar 8. Proses Enkripsi LHS *PhpMyAdmin*

Dari gambar diatas dapat dijelaskan bahwa proses enkripsi menggunakan algoritma *MD5* dapat digunakan langsung menggunakan *PhpMyAdmin* yang merupakan perangkat lunak gratis yang ditulis dalam *PHP*, dimaksudkan untuk menangani *admin*istrasi *MySQL* melalui Web. *PhpMyAdmin* mendukung berbagai operasi pada *MySQL* (mengelola *database*, tabel, kolom, hubungan, indeks, pengguna, perizinan , dll) dapat dilakukan melalui antarmuka pengguna yang sering digunakan, karena didalam phpmy*admin* telah terdapat langsung untuk proses enkripsi algoritma *MD5* sehingga lebih memudahkan pengguna untuk melakukan proses pengenkripsian. Dengan menambahkan sedikit koding berikut :

```
$password = $idnpm;
$origFile=
"./hasil/".$idnpm.".pdf";
$destFile=
"./hasil/".$idnpm."_P.pdf";
pdfEncrypt($origFile, $password,
$destFile );
unlink($origFile);
```

Setelah proses enkripsi selesai maka *file pdf* telah terekripsi dan terjaga keamanan LHSnya.



Gambar 9. Enkripsi PDF LHS

## VI. PENGUJIAN SISTEM

Pada penelitian ini pengujian sistem menggunakan Blackbox testing merupakan salah satu metode pengujian perangkat lunak yang berfokus pada sisi fungsionalitas, khususnya pada *input* dan output aplikasi (apakah sudah sesuai dengan apa yang diharapkan atau belum). Tahap pengujian atau testing merupakan salah satu tahap yang harus ada dalam sebuah siklus pengembangan perangkat lunak (selain tahap perancangan atau desain).

Tabel 1 Pengujian *Black box*

| No | Skenario Pengujian | Hasil Yang diharapkan | Hasil Pengujian | Kesimpulan |
|---|---|---|---|---|
| 1 | Tombol Mahasiswa | Masuk ke *form* pengisian data mahasiswa | Sesuai harapan | Valid |
| 2 | Tombol Mata Kuliah | Masuk Ke *form* mata kuliah | Sesuai harapan | Valid |
| 3 | Tombol Prodi | Masuk ke halam prodi untuk pengisian data prodi | Sesuai harapan | Valid |

| | | | | |
|---|---|---|---|---|
| 4 | Tombol Nilai Mata Kuliah | Masuk ke pengisian data nilai mahasiswa | Sesuai harapan | Valid |
| 5 | Tombol LHS Mahasiswa | Masuk ke halaman untuk melihat hasil LHS mahasiswa | Sesuai harapan | Valid |

## VII. Penutup

Dari hasil penelitian ini dapat ditarik kesimpulan sebagai berikut :

1. Dengan adanya sistem keamanan LHS pada Fakultas Teknik Universitas Muhammadiyah Bengkulu ini informasi keaslian LHS tidak dapat dimanipulasi oleh pihak lain.
2. Dengan adanya aplikasi keamanan ini dapat mempermudah mahasiswa dalam melihat, lembar hasil studi mereka.

Dari kesimpulan di atas maka penulis mengajukan saran yang diharapkan dapat membantu dalam kelancaran dan penerapan aplikasi Implementasi Algoritma *MD5* Untuk Keamanan LHS yang baru, agar tampilan pada aplikasi yang di buat oleh Penulis dpat diperbaiki untuk proses yang lebih baik karena aplikasi yang penulis buat masih jauh dari sempurna, oleh karena itu masih banyak yang harus dikembangkan dalam rancangan ini. Misalnya penggunaan *action script* yang masih sederhana serta sedikitnya pengetahuan yang dimiliki oleh penulis tentang program *PHP MySQL*.

## REFERENSI


[1] Akadun 2009. *Teknologi Informasi Administrasi*. Bandung : Alfabeta

[2] Kurniawan, Yusuf. (2004). *Kriptografi Keamanan Internet dan Komunikasi* Bandung: INFORMATIKA.

[3] Rinaldi Munir. 2006. *Strategi Algoritmik.* Laboratorium Ilmu dan Rekayasa komputasi-Institut Teknologi Bandung.

[4] Saipul Bahri. 2012. *Studi dan Implementasi Pengamanan Basis Data Menggunakan Metode Enkripsi MD5 (Message-Digest Algorihm).*