

APLIKASI MEDIA BANTU PEMBELAJARAN KRIPTOGRAFI DENGAN MENGUNAKAN ALGORITMA MESSAGE DIGEST 5 (MD5)

Zein¹, Ahmat Adil²

¹Mahasiswa Teknik Informatika, STMIK Bumigora Mataram

²Tenaga Pengajar STMIK Bumigora Mataram

JL. Ismail Marzuki Mataram, NTB

¹zeinstmik@gmail.com, ²adilahmat@gmail.com

Abstract

College of Informatics and Computer Management (STMIK) Bumigora Mataram, for Computer Network competencies are elective courses that network security system which addresses the cryptographic material using a lecture and power point as a medium while studying in the classroom. Those problems led to the idea to create teaching aids media applications using cryptographic message digest algorithm 5 (MD5). Cryptography is the science that is used to encrypt a message, so the message private. On the application every student can learn and try to direct the activities of the MD5 algorithm program in step by step. This algorithm has a characteristic that the message is converted into a message digest can not be restored into the original message. Two different messages always produce different hash values. So as to facilitate faculty to improve student comprehension. Based on the results of questionnaires to the lecturer stated that the application can assist the lecturer delivered material MD5 cryptographic algorithm. And the results of the questionnaire of the student that can be assisted in doing to learn anytime and anywhere as long as the application can access media learning aids such as web-based applications online.

Kata Kunci: *Instructional Media, Cryptography, Message Digest.*

I. PENDAHULUAN

Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Bumigora Mataram merupakan salah satu perguruan tinggi ilmu komputer di Provinsi Nusa Tenggara Barat (NTB) yang bergerak dibidang teknologi dan informasi.

Pada kompetensi jaringan komputer para mahasiswa disarankan untuk mengambil mata kuliah Sistem Keamanan Jaringan (SKJ) yang merupakan mata kuliah pilihan dari kompetensi jaringan komputer pada semester genap. Mata kuliah SKJ berjumlah 3 SKS dimana 2 SKS diberikan dalam bentuk teori dan 1 SKS diberikan dalam bentuk praktikum. Materi mata kuliah ini diberikan sebanyak 14 kali pertemuan dan pada sebagian materinya membahas tentang kriptografi terutama pada pertemuan ke 2 sampai dengan pertemuan ke 5, yakni sebanyak 4 kali pertemuan. Mata kuliah ini mempelajari materi tentang pengenalan konsep keamanan jaringan, Kriptografi, Konfigurasi *Access Control List (ACL)*, *IP Tables*, *Internet Protocol Security (IPsec)* dan *Simple Network Management Protocol (SNMP)* serta *Computer Information System Company (CISCO) Internetwork Operating System (CISCO IOS)*.

Dalam menyampaikan materi algoritma kriptografi di mata kuliah sistem keamanan jaringan, dosen masih menggunakan metode ceramah dan menggunakan perangkat lunak *microsoft office power point* sebagai media persentasi ketika ceramah dilakukan serta media papan tulis untuk menerangkan jika ada kekurangan pada *slide file* presentasi. Untuk menambah pemahaman, dosen memberikan mahasiswa tugas kelompok untuk membuat makalah tentang algoritma kriptografi tertentu dan harus dipresentasikan dengan menggunakan *microsoft power point* serta didiskusikan. Tugas tersebut akan dijadikan

sebagai nilai harian yang dimasukkan ke dalam komponen penilaian akhir.

Masalah lain yang ada adalah waktu pada saat menyampaikan materi di kelas tentang kriptografi, dosen pengampu mata kuliah hanya bisa menyampaikan sebagian kecil dari jenis algoritma kriptografi. Hal ini disebabkan karena keterbatasan waktu baik itu dalam mengulas materi ataupun contohnya.

Berdasarkan hasil wawancara dengan dosen pengampu mata kuliah sistem keamanan jaringan mengenai proses kegiatan belajar mengajar di kelas, diperoleh informasi bahwa masih diperlukan upaya yang lebih baik lagi untuk meningkatkan kualitas pemahaman mahasiswa, terutama dalam mempelajari ilmu kriptografi khususnya pada algoritma *Message Digest 5 (MD5)* yang sangat kompleks, karena hasil *hashing* dari algoritma ini berupa kombinasi huruf dan angka, dengan panjang 32 karakter atau 128-bit.

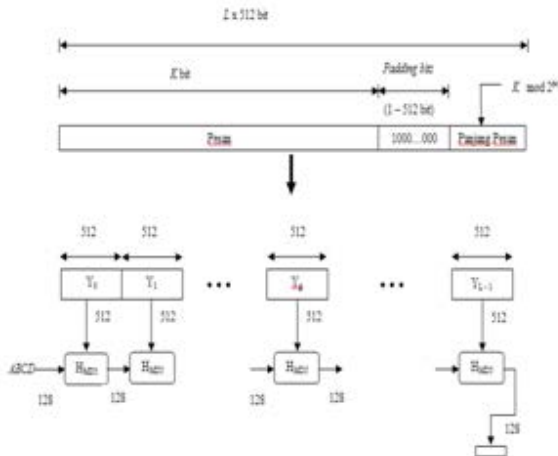
Oleh karena itu, diperlukan sebuah solusi alternatif yang dapat digunakan untuk mengatasi masalah yang muncul akibat kurangnya pemahaman mahasiswa terhadap proses kerja *step by step* dibalik layar dari algoritma tersebut. Salah satunya adalah dengan membuat sebuah aplikasi media bantu pembelajaran, yaitu aplikasi pembantu penyalur informasi yang semula berupa penjelasan secara lisan dan tulisan menjadi digital. Dengan begitu, para mahasiswa dalam mempelajari kriptografi tidak lagi dilakukan hanya dengan bertatap muka di kelas, melainkan bisa mempelajarinya secara mandiri baik didalam kelas maupun di tempat lain.

Dengan menerapkan aplikasi media bantu pembelajaran dimata kuliah sistem keamanan jaringan, diharapkan mampu membantu dosen untuk menjelaskan tentang proses kerja *step by step* dan contoh studi kasus

dari algoritma MD5 tersebut. Sehingga dapat mengatasi permasalahan yang muncul akibat masih sangat kurangnya pemahaman mahasiswa terhadap algoritma kriptografi MD5 ini dan akan mampu menjadi materi yang *easy learning* didalam mata kuliah sistem keamanan jaringan.

Definisi Algoritma Message Digest 5 (MD5)

MD5 adalah fungsi *hash* satu-arah yang dibuat oleh Ronald Rivest pada tahun 1991. MD5 merupakan perbaikan dari MD4 setelah MD4 berhasil diserang oleh kriptanalis. Algoritma MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan *message digest* yang panjangnya 128 bit [1].



Gambar 1. Pembatasan Message Digest dengan algoritma MD6

Langkah-langkah pembuatan *message digest* secara garis besar adalah sebagai berikut [1]:

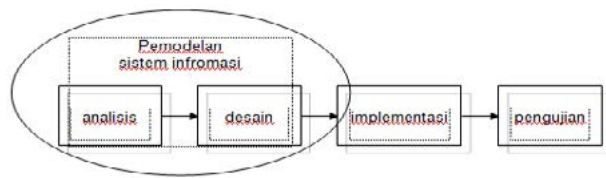
1. Penambahan Bit-Bit Pengganjal (*Padding Bits*)
2. Penambahan Nilai Panjang Pesan Semula
3. In Pengolahan pesan dalam blok berukuran 512 bit
4. Isialisasi Penyangga (*Buffer*) MD

Algoritma MD5 merupakan fungsi *hash* yang sering digunakan untuk mengamankan suatu jaringan komputer dan internet yang sengaja dirancang dengan tujuan sebagai berikut [2]:

1. Keamanan: Hal ini tidak bisa dielakan karena tidak satupun sistem algoritma yang tidak bisa dipecahkan. Serangan yang sering digunakan untuk menjebol algoritma *Hash* adalah dengan menggunakan *brute force*.
2. Kecepatan: *Software* yang digunakan mempunyai kecepatan yang tinggi karena didasarkan sekumpulan manipulasi operan 32 bit.
3. Simple: Tanpa menggunakan struktur data yang kompleks.

II. METODOLOGI

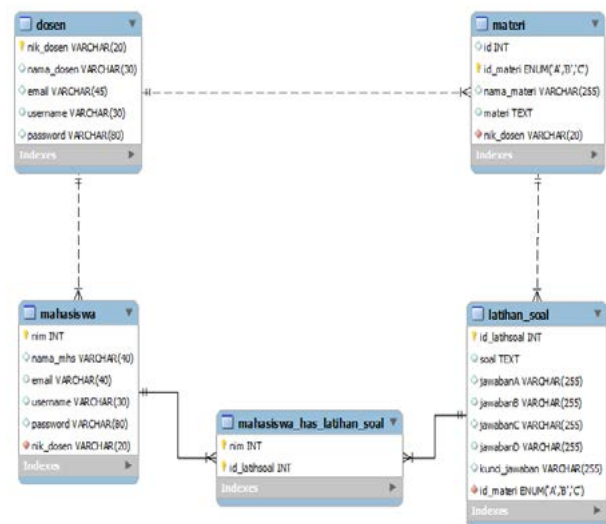
Metode penelitian yang digunakan dalam penulisan ini adalah metode Sekuensial Linier [3]. Adapun tahapannya sebagai berikut :



Gambar 2. Model Sekuensial Linier

a. Pengumpulan Data

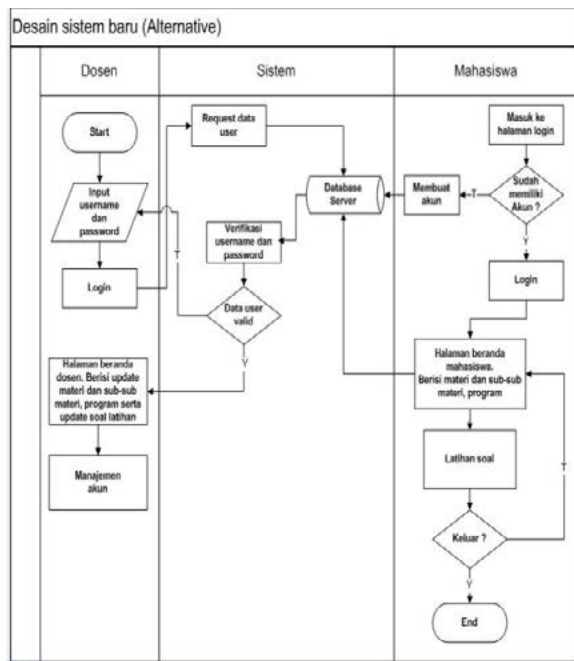
Teknik pengumpulan data yang dilakukan penulis adalah menganalisa dan mempelajari data-data yang telah dikumpulkan yaitu data hasil wawancara dengan dosen pengampu mata kuliah sistem keamanan jaringan dan memahami data dari berbagai sumber literatur untuk diproses ke tahapan berikutnya yaitu normalisasi data yang akan menghasilkan beberapa tabel-tabel dan relasi antar tabel. Relasi ini akan menggambarkan bagaimana table-table dalam database tersebut akan berelasi antara table yang satu dengan table yang lain, sehingga dapat ditentukan field yang saling berhubungan. Berikut ini merupakan gambar dari relasi antar tabel di dalam database:



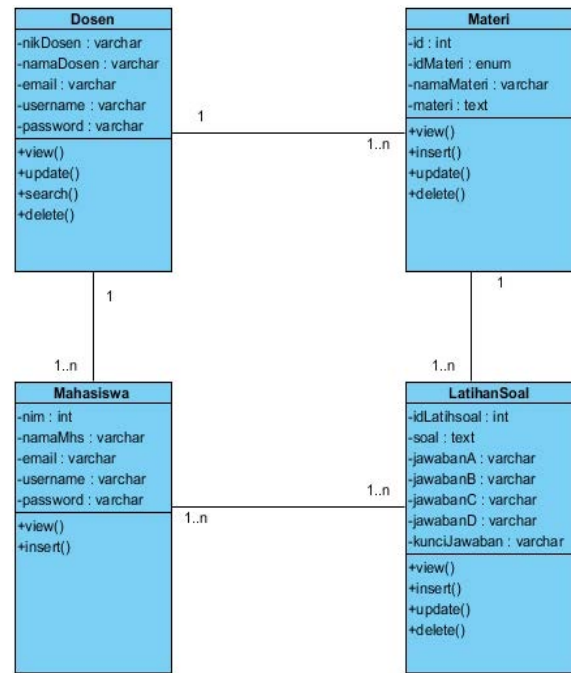
Gambar 3. Relasi Antar Tabel

b. Desain Sistem Baru (Alternatif)

Dalam penelitian ini penulis menawarkan sistem baru sebagai alternative dari sistem lama, berikut ini adalah gambar desain sistem baru (alternatif):



Gambar 4. Desain Sistem Alternatif



Gambar 5. Class Diagrams

Berikut ini merupakan penjelasan dari desain sistem alternatif:

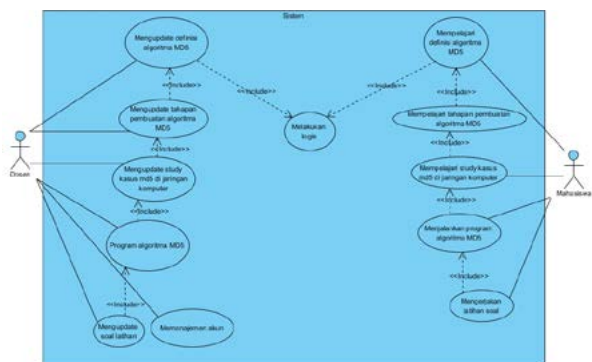
1. Dosen melakukan proses login dengan memasukkan *username* dan *password*.
2. Sistem melakukan verifikasi terhadap *username* dan *password* yang dimasukkan *user* dengan data *user* yang tersedia.
3. Jika login gagal, maka dosen kembali melakukan aktifitas no. 1.
4. Jika login berhasil, maka dosen akan diantarkan ke halaman beranda dosen yang berisi menu *update* materi, program, *update* latihan soal dan manajemen akun.
5. Sedangkan pada bagian mahasiswa melakukan *login* dengan memasukkan *username* dan *password*. Jika tidak mempunyai *username* dan *password*, maka dapat memilih menu membuat akun.
6. Setelah mahasiswa memiliki akun dan berhasil melakukan proses *login*, maka akan ke halaman beranda mahasiswa yang berisikan tentang materi, program dan latihan soal.
7. Setelah mahasiswa mempelajari materi, mengujicoba program dengan memasukkan *plaintext* hingga mengeluarkan hasil serta mengikuti latihan soal, maka mahasiswa dapat keluar dengan mengklik *button* keluar. Jika tidak, mahasiswa dapat kembali ke menu yang diinginkannya.

c. Class Diagrams

Class diagrams merupakan diagrams yang selalu ada di permodelan sistem berorientasi obyek. Class diagrams menunjukkan hubungan antar class dalam sistem yang sedang dibangun dan bagaimana mereka saling berkolaborasi untuk mencapai suatu tujuan [4]. Dalam permodelan sistem ini, terbentuk class diagrams sebagai berikut:

d. Use Case Diagrams

Use case diagrams menjelaskan urutan kegiatan yang dilakukan actor dan sistem untuk mencapai suatu tujuan tertentu. Walaupun menjelaskan kegiatan namun use case hanya menjelaskan apa yang dilakukan actor dan sistem, bukan bagaimana actor dan sistem melakukan kegiatan tersebut [4]. Dalam perancangan sistem ini penulis menggambarkan use case diagrams sebagai berikut:

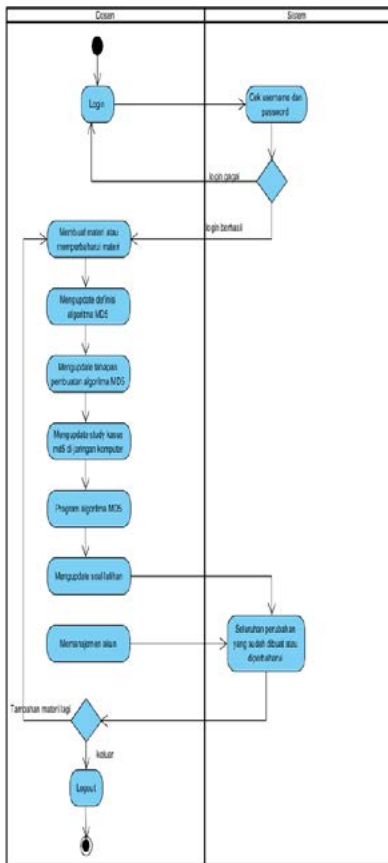


Gambar 6. Use Case Diagrams

e. Activity Diagrams

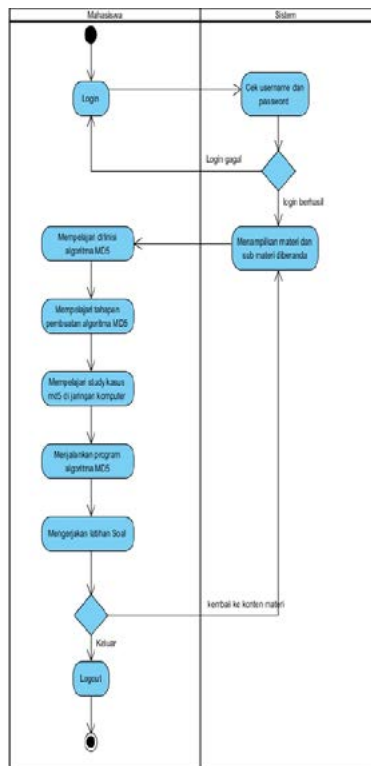
Activity Diagrams adalah teknik untuk menggambarkan logika procedural, proses bisnis, dan jalur kerja [5]. Dalam perancangan sistem ini penulis menggambarkan activity diagrams sebagai berikut:

1. Activity Dosen



Gambar 7. Activity Diagrams Dosen

2. Activity Mahasiswa



Gambar 8. Activity Diagrams Mahasiswa

III. HASIL DAN PEMBAHASAN

a. Halaman Register

Mahasiswa melakukan register (pendaftaran) akun

ke aplikasi.

Buat Akun Anda

Keterangan :
 Masukkan data diri anda dengan yang benar

The form is titled 'SILAHKAN MEMBUAT AKUN ANDA'. It contains the following fields:
 - NIM: 200510011 ✓
 - Nama: zein ✓
 - Email address: zeinm@gmail.com ✓
 - Username: zein ✓
 - Password: [masked] ✓
 - Ulangi password: [masked] ✓
 - A blue 'Daftar' button is at the bottom.

Gambar 9. Halaman Register

b. Halaman Login

Mahasiswa login untuk masukkan ke beranda mahasiswa

SILAHKAN SIGN IN

The login page has the following elements:
 - Username field: zein ✓
 - Password field: [masked] ✓
 - A dropdown menu showing 'Mahasiswa' ✓
 - A blue 'Masuk' button at the bottom.

Keterangan :

Gunakan akun yang valid untuk memperoleh akses ke sistem.
 Jika belum memiliki akun silahkan mendaftar terlebih dahulu.

Gambar 10. Halaman Login

c. Mempelajari definisi algoritma MD5

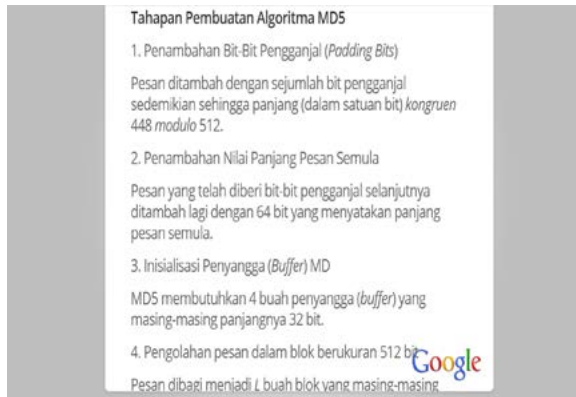
Mahasiswa mempelajari definisi dari algoritma md5, melalui slide-slide presentations yang tampil dilayar monitor.



Gambar 11. Halaman Definisi MD5

d. Mempelajari tahapan pembuatan MD5

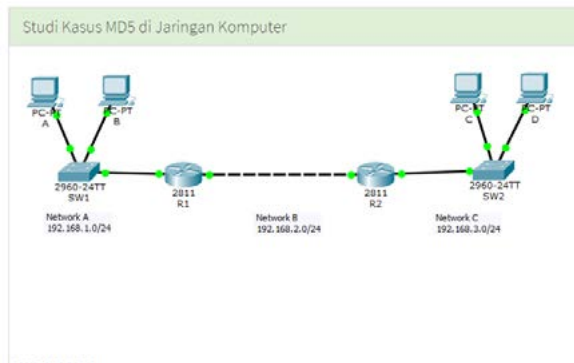
Setelah teori-teori diatas dipelajari, lanjut ke lebih dalam lagi mengenai md5 yaitu mempelajari tahapan-tahapan dalam pembuatan algoritma md5.



Gambar 12. Halaman Pembuatan MD5

e. Mempelajari studi kasus MD5 di jaringan

Mahasiswa juga dapat mengetahui tentang penerapan algoritma md5 di jaringan komputer. Penerapan tersebut baik yang ada di perangkat keras jaringan maupun perangkat lunak (aplikasi berbasis jaringan).



Gambar 13. Halaman Studi Kasus MD5

f. Mahasiswa mencoba program MD5

Saat mencoba program algoritma md5, setiap mahasiswa akan memasukkan *plaintext* dan mengikuti proses selanjutnya sampai dengan menghasilkan *hashing* sebanyak 32 karakter *hexadecimal* atau 128 bit. Misalkan mahasiswa memasukkan *plaintext* kata “mataram”, maka program akan memprosesnya secara *step by step*, hingga menghasilkan 32 karakter *hexadecimal* atau 128 bit tersebut.

DEMO MD5

1. Masukkan Plaintext atau kata yang ingin dihashing
 mataram

KONVERSI
 Plainteks/pesan yang menjadi masukkan di dalam MD5 akan dikonversi terlebih dahulu menjadi data biner. Di bawah ini adalah representasi pesan yang dimasukkan dalam bentuk biner.

```
01101101 01100001 01101000 01100001 01100010 01100001 01101101
```

2. Penambahan Bit Pengganjal
 Tahap ini merupakan tahap pertama dalam proses MD5, dimana pesan akan diberi bit pengganjal. Untuk melihat proses ini, silahkan tekan tombol "TAHAP1".

TAHAP1
 Panjang pesan yang Anda masukkan adalah 56 bit. Pesan ini kemudian akan diberi bit pengganjal (padding) sehingga panjangnya kongruen $448 \pmod{512}$. Karena panjang pesan adalah 56 maka pesan akan diberi bit pengganjal (dipadding) sebanyak 392. Karena $448 \pmod{512} = 448$, Pesan ini akan diberi bit pengganjal yang bernilai 1 sebanyak 1 dan bit yang bernilai 0 sebanyak 391.

3. Penambahan Bit Pengganjal 64 bit
 Setelah operasi penambahan bit pengganjal selesai, pesan akan ditambahkan 64 bit yang merupakan representasi nilai atau panjang asli pesan. Untuk melihat 64 bit yang ditambahkan dalam kasus ini silahkan tekan tombol "TAHAP2".

TAHAP2
 Dalam kasus ini, 64 bit yang ditambahkan yaitu 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00111. Penambahan 64 bit ini akan membuat panjang pesan menjadi 512 bit. Setelah operasi penambahan bit pengganjal (padding), maka pesan akan terlihat seperti berikut ini.

```
01101101 01100001 01101000 01100001 01100010 01100001 01101101 10000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00111000
```

4. Inisialisasi Periyangga MD
 Setelah tahap 1 dan 2 selesai, maka tahapan selanjutnya dalam proses MD5 yaitu penginisialisasian periyangga (buffer dari MD). Dalam Algoritma MD5 terdapat 4 buah periyangga (buffer) yang secara berurutan dinamakan A,B,C,dan D. Masing-masing periyangga memiliki panjang 32 bit. Sehingga total seluruh periyangga adalah 128 bit. Keempat periyangga ini berfungsi untuk menyimpan hasil proses dan hasil akhir dari MD. Setiap periyangga diinisialisasi dengan nilai-nilai (dalam notasi hexadecimal) sebagai berikut.

A= 67452301
 B= efcab8d9
 C= 58baf6fe
 D= 10325476

5. Pengolahan Pesan Dalam Blok 512 Bit
 Setelah tahap ketiga selesai, tahap selanjutnya adalah pengolahan pesan yang dilakukan dalam blok-blok yang memiliki panjang masing-masing 512 bit. Berikut adalah gambar yang memperlihatkan hal tersebut.

Pengolahan Pesan Dalam Blok 512 Bit (Proses MD5)

OPERASI DASAR PADA MD5
 Adapun operasi dasar yang dilakukan oleh fungsi g untuk tiap round yaitu:
 Round 1 : (b AND c) OR (b AND d)
 Round 2 : (b AND d) OR (c AND d)
 Round 3 : b + c + d
 Round 4 : c + (b OR d)

Untuk melihat hasil akhir dari pengolahan pesan dalam blok 512 bit ini, silahkan tekan tombol "TAHAP4" di bawah ini.

TAHAP4

539dc351a591a1d6d643416f02b43a33

Reset

3. Berapakah jumlah output yang dihasilkan, dari hasil proses hashing yang dilakukan oleh algoritma kriptografi md5?
 A. 64 karakter atau 512 bit
 B. 32 karakter atau 228 bit
 C. 16 karakter atau 64 bit
 D. 512 karakter atau 512 bit

4. Apa yang dimaksud dengan Fungsi hash satu arah (one way hash)?
 A. Fungsi hash satu arah adalah pesan yang sudah diubah menjadi message digest tidak dapat dikembalikan lagi menjadi pesan semula
 B. Fungsi hash satu arah adalah pesan yang sudah diubah menjadi message digest dapat dikembalikan lagi menjadi pesan semula
 C. Fungsi hash satu arah adalah pesannya yang sudah diubah menjadi message digest
 D. Jawaban B dan C benar

5. Dari persamaan dibawah ini, pilih jawaban yang menurut anda paling benar?
 A. Algoritma kriptografi
 B. Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut
 C. Algoritma kriptografi merupakan algoritma untuk mengubah jumlah IP Address pada teknologi jaringan komputer
 D. Semua jawaban benar

6. Sebutkan salah satu tempat dimana pesan-pesan dari algoritma kriptografi md5 pada jaringan komputer?
 A. MD5 digunakan pada teknologi alat jaringan yaitu HUB
 B. MD5 digunakan pada CISCO IOS Router untuk menggantikan routing protocol OSPF
 C. MD5 digunakan pada teknologi kabel jaringan yaitu Fiber Optik (FO)
 D. Semua jawaban salah

7. Berikut ini manakah langkah-langkah yang benar dalam pembuatan message digest secara garis besar?
 A. Penambahan bit-bit penggalan (padding bit), perubahan nilai panjang pesan semula, inisialisasi penyangga (buffer) MD, pengolahan pesan dalam blok berukuran 512 bit
 B. Pengalihan pesan dalam blok berukuran 512 bit, inisialisasi penyangga (buffer) MD, perubahan nilai panjang pesan semula, penambahan bit-bit penggalan (padding bit)
 C. Penambahan nilai panjang pesan semula, inisialisasi penyangga (buffer) MD, pengolahan pesan dalam blok berukuran 512 bit, penambahan bit-bit penggalan (padding bit)
 D. Inisialisasi penyangga (buffer) MD, pengolahan pesan dalam blok berukuran 512 bit, penambahan bit-bit penggalan (padding bit), penambahan nilai panjang pesan semula

8. Apa saja aspek keamanan yang dimiliki oleh kriptografi?
 A. Kerahasiaan, integritas data, otentikasi, tidak penyangkalan
 B. Kerahasiaan, verifikasi, tidak penyangkalan
 C. Kerahasiaan, integritas data, otentikasi, tidak penyangkalan
 D. Jawaban A dan C benar

Koreksi

Jawaban Anda

jawaban yang benar untuk no:1 adalah B jawaban anda adalah A = SALAH

jawaban yang benar untuk no:2 adalah B jawaban anda adalah A = SALAH

jawaban yang benar untuk no:3 adalah B jawaban anda adalah A = SALAH

jawaban yang benar untuk no:4 adalah A jawaban anda adalah A = BENAR

jawaban yang benar untuk no:5 adalah B jawaban anda adalah B = BENAR

jawaban yang benar untuk no:6 adalah A jawaban anda adalah B = SALAH

jawaban yang benar untuk no:7 adalah B jawaban anda adalah A = SALAH

jawaban yang benar untuk no:8 adalah A jawaban anda adalah A = BENAR

Koreksi

Gambar 14. Halaman Uji coba MD5

g. Mahasiswa mengerjakan latihan soal

Bagian terakhir yaitu mahasiswa dapat mengerjakan latihan soal, ada 8 jumlah soal yang dikerjakan. Setelah semua telah dijawab, maka mahasiswa dapat langsung memilih *button* koreksi untuk mengetahui hasil jawabannya dan mengetahui jawaban benar yang aslinya.

Latihan Soal

1. Tujuan dari algoritma md5 (fungsi hash) yang digunakan untuk mengamankan suatu jaringan komputer dan internet adalah?
 A. Keamanan, kecepatan dan Simple
 B. Kecepatan, efisiensi dan efektif
 C. Efektif dan efisien
 D. Keamanan dan efektif

2. Algoritma kriptografi dibagi menjadi tiga bagian berdasarkan kunci, manakah yang termasuk dalam bagian-bagian dari algoritma kriptografi tersebut?
 A. Algoritma Simetri (menggunakan satu kunci untuk enkripsi dan dekripsi)
 B. Algoritma Asimetris (menggunakan kunci yang berbeda untuk enkripsi dan dekripsi)
 C. Fungsi Hash satu arah (one way hash)
 D. Semua jawaban benar

Gambar 15. Halaman Latihan Soal dan Jawaban

Hasil Analisa

Analisa mengenai hubungan panjang karakter (pesan) yang dimasukkan sebagai *plaintext* terhadap proses *hashing*, yaitu:

Adapun hubungan antara panjang pesan atau *plaintext* yang dimasukkan dan proses *hashing* yang terdapat di algoritma *message digest* (MD5) adalah berbanding lurus. Dimana semakin panjang pesan yang dimasukkan maka proses yang dilakukan akan semakin banyak. Karena panjang pesan yang dimasukkan menentukan berapa blok 512 bit yang dibentuk oleh MD5. Semakin banyak blok yang dibentuk, maka proses MD5 akan semakin banyak.

IV. SIMPULAN DAN SARAN

4.1. Simpulan

Berdasarkan uraian hasil dan pembahasan pada bab sebelumnya, maka penulis dapat mengambil beberapa kesimpulan dari penulisan ini, sebagai berikut:

- a. Aplikasi media bantu pembelajaran ini, dapat membantu dosen pengampu mata kuliah sistem keamanan jaringan dalam memberikan materi khusus materi kriptografi tentang algoritma MD5 secara *online* kepada setiap mahasiswa yang mengambil mata kuliah tersebut. Karena sebelum mahasiswa memasuki bab yang membahas materi kriptografi, setiap mahasiswa akan diarahkan untuk mengakses aplikasi media pembelajaran tersebut untuk belajar secara mandiri.
- b. Dengan adanya fitur uji coba langsung program algoritma MD5 yang sifatnya aplikatif secara *step by step*, diharapkan mahasiswa dapat memahami dengan mudah cara bekerja atau tahapan-tahapan dalam melakukan *hashing* dengan menggunakan algoritma md5 tersebut.
- c. Dengan memanfaatkan aplikasi berbasis *web online*, maka mahasiswa dapat terbantu dalam melakukan proses belajar dimana dan kapan saja selama bisa mengakses aplikasi media bantu pembelajaran tersebut.

4.2. Saran

Setelah melihat kesimpulan di atas, penulis sadar bahwa dalam penulisan ini belum sempurna, sehingga penulis memberikan saran sebagai berikut:

- a. Terdapat beberapa algoritma yang memiliki fungsi *hashing (hashing function)*, disarankan untuk memilih algoritma lain dengan fungsi *hashing* untuk bisa membandingkan dengan algoritma yang telah digunakan oleh penulis pada penelitian ini.
- b. Menambahkan beberapa algoritma kriptografi lainnya, baik algoritma enkripsi dekripsi atau algoritma *hashing* lainnya sehingga mahasiswa yang mengambil mata kuliah sistem keamanan jaringan dapat mempelajari lebih banyak lagi algoritma-algoritma kriptografi yang bekerja di jaringan komputer dan menyatukannya dalam satu aplikasi media bantu pembelajaran.

REFERENSI

- [1] Munir, Rinaldi. 2006. *Kriptografi*. Bandung : Informatika Bandung.
- [2] Ariyus, Dony. (2008). *Pengantar Ilmu Kriptografi (Teori, Analisis dan Implementasi)*. Yogyakarta : Andi
- [3] Simarmata, Janner. (2010). *Rekayasa Web*. Yogyakarta, Andi Offset.
- [4] Hermawan, J. (2004). *Analisa-Desain dan Pemrograman Berorientasi Obyek dengan UML dan VB.NET*. Yogyakarta: Penerbit ANDI Yogyakarta.
- [5] Flower, M. (2004). *UML Distilled Edisi 3 Panduan Singkat Bahasa Pemodelan Objek Standar*. Yogyakarta: Penerbit ANDI.