Perancangan Aplikasi Pembelajaran Kriftografi Pada Algoritma Fungsi Hash Menggunakan Metode Computer Based Learning

Ainul Wardah
STMIK Budi Darma; Jl. Sisingamangaraja No. 338 Medan, 061-7875998
email : ainulwarda91@yahoo.com

Abstrak

Salah satu hasil dari kemajuan Teknologi Komputer telah memberikan dampak yang transformasional (perubahan yang sesuai) pada aspek kehidupan dan salah satu perubahan yang yang dapat dirasakan langsung adalah dalam bidang pendidikan. Sulitnya mendapatkan buku sangatlah mempengaruhi minat mahasiswa ataupun masyarakat untuk belajar mengenai kriptogafi, oleh sebab itu maka dirancang aplikasi pembelajaran ini. Aplikasi ini merupakan sekumpulan halaman yang menampilkan informasi data Teks, Gambar diam atau bergerak, animasi, Video, yang dirancang dalam satu rangkaian agar dapat menarik minat mahasiswa atau masyarakat.

Tujuan pembelajaran ini berfungsi untuk mempermudah para mahasiswa mempelajari kriptografi, dan hal ini merupakan suatu alternatif dalam mengatasi beberapa masalah seperti waktu yang terbatas, buku yang sulit dicari, ruang kelas yang kurang memadai, kurangnya minat para mahasiswa dalam belajar, dan meningkatkan kepuasaan belajar bagi pengguna serta dapat mengurangi suasana yang membosakan. Perancangan aplikasi pembelajaran dengan metode Computer Based Learning (CBL) yaitu metode yang dikembangkan dengan media komputer, dimana metode pengajaran secara langsung kepada pengguna melalui cara berinteraksi dalam topic pembelajaran yang telah dikemas dalam suatu aplikasi perangkat lunak.

Kata kunci : *Kriptografi, Fungsi Hash, Pembelajaran, CBL*

1. PENDAHULUAN

Pembelajaran menurut adalah sebagai proses penciptaan lingkungan yang memungkinkan terjadinya proses belajar. Jadi dalam pembelajaran yang utama adalah bagaimana mahasiswa belajar. Belajar dalam pengertian aktifitas mental mahasiswa dalam berinteraksi dengan lingkungan yang menghasilkan perubahan perilaku yang bersifat relatif konstant. Dari uraian di atas, apabila konsep tersebut di gabungkan maka multimedia pembelajaran dapat di artikan sebagai aplikasi multimedia yang di gunakan dalam proses pembelajaran, dengan kata lain untuk menyalurkan pesan(pengetahuan, keterampilan dan sikap)serta dapat merangsang pilihan, perasaan, perhatian, dan kemauan belajar sehingga secara sengaja proses belajar terjadi, bertujuan dan kembali[4].

Penerapan metode *Computer Based Learning* (CBL) dalam implementasi program pembelajaran kriptografi ini akan membantu mengarahkan dan memaksimalkan proses belajar mengajar. Sistem komputer dapat menyampaikan pembelajaran secara langsung kepada para mahasiswa melalui cara berinteraksi dengan mata kuliah yang di programkan ke dalam sistem, inilah yang di sebut pengajaran dengan bantuan komputer. Dosen terkadang mengalami kesulitan dalam menyampaikan bahan materi belajar pada mahasiswa, sementara itu keunggulan dari proses berbantuan komputer dapat mempermudah dosen dalam memberikan pengajaran materi kepada mahasiswa di dalam ruangan. Di mana mahasiswa dalam bentuk satu gambaran yang tidak nyata, selain itu mahasiswa juga dapat lebih bersemangat belajar di kampus untuk di

pelajari di rumah dengan komputer sebagai media pembantu untuk belajar. Revolusi dalam belajar bukannya meninggalkan kebiasaan membaca atau mendengar seperti halnya yang selama ini di lakukan. Pembuatan media ini nantinya di khususkan untuk pembelajaran kriptografi.

Algoritma fungsi *Hash* adalah sebuah fungsi yang memasukannya adalah sebuah pesan dan keluaran sebuah sidik pesan (*Message Fingerprint*). Sidk pesan sering disebut *message fingerprint.* Fungsi *Hash*dapat digunakan untuk mewujudkan beberapa layanan keamanan jaringan misalnya, untuk keutuhan data dan otentikasi pesa. Bab ini akan menjelaskan konsep dasar fungsi *hash* yang dipakai dalam sistem kriptografi dan membahas dasar fugsi *hash* yang banyak dipaka, yaitu MD5 dan SHA.

Berdasarkan latar belakang masalah di atas maka dapat diambil rumusan masalah yang akan diselesaikan yaitu Bagaimana mempelajari kriptografi fungsi *hash* agar lebih mudah dipahami , Bagaimana menerapkan *Computer Base Learning* (CBL)dalam pembelajaran kriptografi.

Adapun manfaat dari penelitian ini, adalah Mempermudah mahasiswa untuk mengetahui pembelajaran kriptografi algoritma fungsi *Hash*. Untuk menambah sumber pembelajaran serta memberi alternatif cara belajar yang menarik.

2. METODE PENELITIAN

2.1. Pembelajaran

Pembelajaran adalah proses interaksi peserta didik dengan pendidik dan sumber belajar pada suatu lingkungan belajar. Pembelajaran merupakan bantuan yang diberikan pendidik agar dapat terjadi proses pemerolehan ilmu dan pengetahuan, penguasaan kemahiran dan tabiat, serta pembentukan sikap dan kepercayaan pada peserta didik. Dengan kata lain, pembelajaran adalah proses untuk membantu peserta didik agar dapat belajar dengan baik.

Pembelajaran adalah kegiatan dosen secara terprogram dalam desain instructional, untuk membuat belajar secara aktif. Yang menekankan pada penyediaan sumber belajar. Dalam undang-undang no. 20 tahun 2003 tentang sistem pendidikan nasional pasal 1 ayat 20 dinyatakan bahwa pembelajaran adalah proses interaksi peserta didik dengan pendidik dan sumber belajar pada suatu lingkungan belajar[4].

Konsep pembelajaran adalah suatu proses dimana lingkungan seseorang secara disengaja dikelola untuk memungkinkan ia turut serta dalam tingkah laku tertentu dalam kondisi-kondisi khusus atau menghasilkan respon terhadap situasi tertentu. Pembelajaran merupakan subset khusus dari pendidikan. Pembelajaran mengandung arti setiap kegiatan yang dirancang untuk membantu mempelajari suatu kemampuan dan nilai yang baru. Proses pembelajaran pada awalnya meminta dosen untuk engetahuai kemampuan dasarnya, motivasinya, latar belakang akademisnya, latar belakang ekonominya dan lain sebagainya. Kesiapan dosen untuk mengenal karakteristik mahasiswa dalam pembelajaran merupakan modal utama penyampaian belajar dan menjadi indicator suksesnya pelaksanaan pembelajaran[4]..

Dapat ditarik kesimpulan bahwa pembelajaran adalah usaha dasar dari dosen untuk membuat mahasiswa belajar, dimana perubahan itu dengan didapatkannya kemampuan baru yang berlaku dalam waktu yang relative lama dan karna adanya usaha.

2.1.1 Komponen Pembelajaran

Interaksi merupakan cirri utama dari kegiatan pembelajaran, baik anatara yang belajar dengan lingkungan belajarnya, baik itu dosen, teman-temannya, tutor, media pembelaaran, atau sumber-sumber balajar yang lain. Cirri lain pembelajaran adalah yang berhubungan dengan komponen-komponen pembelajaran. Komponen pembelajaran mengelompokan komponen-komponen pembelajaran dalam tiga kategori utama, yaitu dosen, isi atau materi pembelajaran dan mahasiswa.

Interaksi antara tiga komponen utama melibatkan metode pembelajaran, media pembelajaran dan penataan lingkungan tempat belajar yang memungkinkan terciptanya tujuan yang telah direncanakan sebelumnya[8].

2.1.2 Tujuan Pembelajaran

Tujuan pembelajaran pada dasarnya merupakan harapan, yaitu apa yang diharapkan dari siswa sebagai hasil belajar. Memberi batasan yang lebih jelas tentang tujuan pembelajaran dan maksud yang dimonukasikan melalui pernyataan yang menggambarkan tentang perubahan yang digharapkan dari mahasiswa[7].

Tujuan pembelajaran adalah tujuan yang menggambarkan pengetahuan, kemapuan, keterampilan, dan sikap yang harus dimiliki mahasiswa sebagai akibat dari hasil pembelajaran yang dinyatakan dalam bentuk tingkah laku yang dapat diamati dan diukur. Tujuan pembelajaran juga merupakan rumusan secara terperinci apa saja yang harus dikuasai oleh siswa sesudah ia melewati kegiatan pembelajaran yang bersangkutan dengan berhasil[7].

2.1.3 Materi Pembelajaran

Materi pembelajaran pada dasarnya merupakan isi dari kurikulum, yakni berupa mata pelajaran atau bidang studi dengan topik/sub topic dan rincianya. Isi dari proses pembelajaran tercermin dalam materi pembelajaran yang dipelajari oleh mahasiswa.

Materi pembelajaran adalah substansi yang akan disampaikan dalam proses belajar megajar. Tanpa materi pembelajaran proses belajar mengajar tidak akan berjalan. Materi pembelajaran disusun secara sistematis dengan mengikuti prinsip psikologi. Agar materi pembelajaran itu dapat mencerminkan target yang jelas dari perilaku mahasiswa setelah mengalami proses belajar mengaja. Materi pembelajaran harus mempunyai lingkup dan urutan yang jelas. Karena itu, pemilihan materi pembelajaran tentu saja harus sejalan dengan ukuran-ukuran yang digunakan untuk memilih isi kurikulum bidang studi yang bersangkutan. (Syahril Bahri, Strategi Belajar Mengajar, 2010, 105).

2.1.4 Media Pembelajaran

Pembelajaran merupakan kegiatan yang melibatkan mahasiswa dan dosen dengan menggunakan berbagai sumber belajar baik dalam situasi kelas maupun diluar ruangan. Dalam arti media yang digunakan untuk pembelajaran tidak terlalu identik dengan situasi kelas dalam pola pengajaran konvensional namun proses belajar tanpa kehadiran dosen dan lebih mengandalkan media termasuk dalam kegiatan pembelajaran[5], yaitu :

1. Penggunaan media di ruangan
   Pada teknik ini media dimanfaatkan untuk menunjang tercapainya tujuan tertentu dan penggunaanya dipadukan dengan proses belajar mengajar dalam situasi ruangan. Dalam merencanakan pemanfaatan media tersebut dosen harus meliahat tujuan yang akan dicapai, materi pembelajaran yang mendukung tercapainya tujuan tersebut, serta strategi belajar mengajar yang akan sesuai untuk tercapainya tujuan tersebut.
2. Penggunaan media diuar Ruangan
   Media tidak secara langsun dikendalikan oleh dosen, namun digunakan oleh mahasiswa sendiri tanpa instruksi dosen atau melalu pengontrolan oleh orang tua mahasiswa. Penggunaan media di luar kelas dapat dibedakan menjadi dua kelompok utama, yaitu penggunaan media tidak terprogram dan penggunaan media secara terprogram.
3. Penggunaan media tidak terprogram
   Penggunaan media dapat terjadi dimasyarakat luas. Hal ini ada kaitanya dengan keberadaan media massa yang ada di masyarakat. Penggunaan media ini bersifat bebas yaitu bahwa media itu digunakan tanpa dikontrol atau diawasi dan tidak terprogram sesuai tuntutan kurikulum yang digunakan oleh dosen atau kampus.
4. Penggunaan media secara terprogram
   Media digunakan dalam suatu rangkaian yang diatur secara sistematis untuk mencapai tujuan disesuaikan dengan tuntutan kurikulum yang sedang berlaku. Peserta didik sebagai saran diorganisasikan dengan baik sehingga mereka dapat menggunkan media itu secara teratur, berkesinambungan dan mengikuti pola belajar mengajar tertentu.

Berdasarkan beberapa pengertian, dapat disimpulkan bahwa media pembelajaran merupakan peralatan yang membawa pesan-pesan untuk mencapai tujuan pembelajaran.

2.1.5 Teori-Teori Pembelajaran

Terdapat beberapa teori pembelajaran, sebagai berikut :

1. *Behavioristik*
   Pembelajaran selalu member stimulus kepada siswa agar menimbulkan respon yang tepat yang penulis inginkan. Hubungan stimulus dan respon ini diulangkan menjadi sebuah kebisaan. Selanjutnya bila mahasiswa menemukan kesulitan atau masalah, pengajar menyuruhnya untuk mencoba dan mencoba lagi(*trial and error)* sehingga akhirnya diperoleh hasil.
2. *Kognitivisme*
   Pembelajaran adalah dengan mengaktifkan indera mahasiswa agar memperoleh pemahaman sedangkan pengaktifan indera dilaksanakan dengan jalan menggunakan media alat bantu.
3. *Humanistik*
   Dalam pembelajaran ini mengajar sebagai pembimbing memberikan pengarahan agar mahasiswa dapat mengaktualisasikan dirinya sendiri sebagai manusia yang unik untuk mewujudakan potensi-potensi yang dalam dirinya sendiri. Dan siswa perlu melakukan sendiri berdasarkan inisiatif sendiri yang melibatkan pribadinya secara utuh (perasaan maupun intelektual) dalam proses belajar, agar dapat memperoleh hasil.
4. Sosial Pemerhatian Permodelan
   Proses pembelajaran melalui proses pemerhatian dan permodelan Bandura (1986) mengenal pasti empat unsure dalam proses pembelajaran melalui pemerhatian atau pemodelan, yaitu pemerhatian (*attention*), mengingat (*retention*), reproduksi (*reproduction*), penangguhan (*reinforcement*) dan motivasi (*motivation*).

   Implikasi dar pada kaedah ini berpendapat pembelajaran dan pengajaran dapat dicapai melalui beberapa cara yang berikut :
   1. Penyampaian harus interaktif dan menarik.
   2. Demonstansi pengajar hendaklah jelas, menarik, mudah dan tepat.
   3. Hasilan pengajar atau contoh-contoh seperti ditunjukan hendaklah mempunyai mutu yang tinggi.

2.2 Computer Based Learning (CBL)

Pada awalnya komputer digunakan hanya sebagai alat untuk menghitung. para peneliti melihat adanya kebutuhan komputer untuk pembelajaran. Akhirnya diadakan penelitian yang berfokus pada komputer untuk pendidikan. Dalam perkembangannya komputerlah yang paling populer dipakai sebagai alat bantu pembelajaran secara elektronik. Karena itu dikenal dengan istilah CBL(Computer Based Learning) atau dalam bahasa Indonesia disebut sebagai pembelajaran berbasis komputer. Saat pertama kali komputermulai diperkenalkan khususnya pada pembelajaran, maka ia akan menjadi dikenal atau populer di kalangan mahasiswa karena berbagai variasi teknik mengajar yang bisa dibuat dengan bantuan komputer tersebut.

CBL adalah pembelajaran yang sepenuhnya menggunakan komputer, siswa berhadapan dan berinteraksi secara langsung dengan komputer. Interaksi antara komputer dengan mahasiswa ini terjadi secara individual dan belajar secara mandiri tanpa bantuan dosen. Maka dalam topik ini istilah yang tepat digunakan ialah CBL *(Computer Based Learning)* yang mana segala jenis belajar mahasiswa yang berhubungan dengan belajar. Karena kata "learning' disini dianggap masih sebaga istialh yang umum karena istilah kata 'learning" itu sendiri secara alamiah mencakup situasi dimana komputer digunakan sebagai alat pembelajaran, tetapi tidak untuk menyampaikan informasi atau mengajar mahasiswa. Adapun tahap-tahap yang dilakukan dsalam penelitian CBL tentunya mempunyai tahap-tahap yang dilakukan untuk menemukan masalah serta hasilnya.(Rahmad Setiadi dan Akhril Agus 2003: 3).

Berikut adalah tahap-tahap penelitian pada CBL :

1. Penggunaan komputer dalam pendidikan adalah untuk latihan dan praktek dalam aritmatika dan membaca.
2. Penggunaan komputer dapat digunakan sebagai dosen, sebagai alat. Disini, peran "tradisional" komputer dalam pendidikan dibalik. Dalam rangka untuk mengajarkan komputer, mahasiswa harus belajar dan mengerti bahasa komputer, dengan demikian para mahasiswa harus dapat bekerja dengan bahasa pemrograman.
3. Memberikan arah pada guru tentang di mana dan bagaimana menggunakan komputer dalam pembelajaran.
4. Perangkat lunak pendidikan akan menampilkan peningkatan kognisi yang memungkinkan manusia untuk memperpanjang/mempertajam kemampuan kognitif mereka melalui aplikasi komputerkomputer dalam pendidikan.

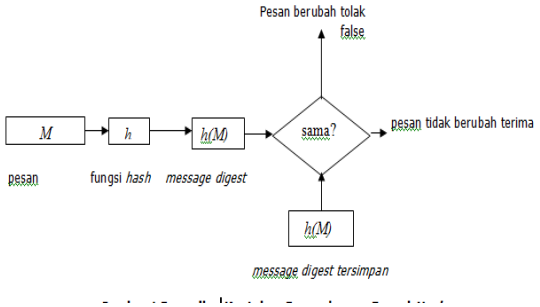
2.3. Kriptografi

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan peyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi[5].

2.3.1 Algoritma Fungsi Hash

Fungsi *Hash* adalah sebuah fugsi yang masukannya adalah sebuah pesan dan keluaran sebuah sidik pesan dan keluaran sebuah sidik pesan (*Message Fingerprint*). Sidik pesan sering disebut *message digest*. Fungsi *Hash* dapat digunakan untuk mewujudkan beberapa layanan keamanan jaringan misalnya, untuk keutuhan data dan otentikasi pesan.

Pengirim pesan dan penerima pesan dan penerima pesan memiliki cara sehingga keutuhan data dapat diselidiki. Fungsi *hash* dapat digunakan untuk mewujudkan layanan keutuhan data. Misalnya *M* merupakan pesan *h* adalah fungsi *hash*, maka *y = h (M)* disebut dengan sidik pesan *x* atau sering juga disebut dengan *message digest.* Sebuah *message digest* umumnya berukuran pendek, yaitu sekitar 160 bit[5].



Gambar 1. Pengujian Keutuhan Pesan dengan Fungsi Hash

Dengan menggunakan sebuah fungsi *hash h*. Sebelum pesan *M* disebarkan/dikirimkan sebuah *message digest y*lama = *h* (*M*) disimpan sebagai acuan. Misalnya didapatkan kembali *M* setelah disebarkan apabila ingin menguji apakah *M=M* hitung kembali *message digest* baru *y*baru =*h (M)* disimpulkan pesan tidak berubah bila *y*lama = *y*baru.

Contoh soal:

25 mod 11 = 3

Jika key bernilai negatif, maka bagi key dengan N untuk mendapatkan sisa r :

Untuk r = 0, maka Key mod N = 0

Untuk r < > 0, maka key mod N = N-r

2.3.2 Kode Otentikasi Pesan (Message Authentication Code)

Fungsi *hash* dapat dipakai untuk mewujudkan layanan otentikasi pesan dengan memberikan keluaran kode otetikasi pesan atau dikenal dengan MAC. Fungsi *hash* yang dipakai pada

otentikasi pesan dapat memiliki masukan sebuah kunci sehingga disebut juga *hash* dengan kunci. Misalnya *Alice* dan *Bob* telah berbagi kunci rahasia K dan sebuah fungsi *hash h*. ketika *Alice* mengirim sebuah pesan *M,* maka Alice juga menyertakan nilai $y = h\text{K}(M)$. *Bob* menerima *M* dan *y* dan memverifikasikan apakah $y = hK(M)$ jika benar, maka *Bob* dapat memastikan bahwa pesan tidak berubah dan memang berasal dari *Alice*. (Rifki Sadikin, Kriptografi Untuk Keamanan Jaringan, 2012, 310).

2.3.3 Kriteria Keamanan Fungsi Hash

Fungsi *hash h* yang dipakai pada sistem kriptografi harus memenuhi beberapa syarat sehingga dapat dianggap aman, yaitu ketahanan terhadap serangan *preimage* , ketahanan terhadap *second preimage* dan ketahan terhadap serangan *collsion*. Makna ketahanan disini adalah jika diberikan persoalan *preimage* dan *collision* pada fungsi *hash h,* maka persoalan itu semuanya susah untuk diselesaikan. *Preimage* fungsi *hash h* diharuskan bersifat satu arah, yaitu jika diberikan pesan M, maka dapat dihitung dengan mudah $y = h(M)$. Namun jika diberikan *y* dan dungsi *hash h,* maka sulit bagi penyerang untuk menemukan *M*.

Second Preimage Permasalahan *second preimage* adalah jika diberikan sebuah pesan *M* dan fungsi *hash h,* maka temukan M' sehingga $h(M) = h(M')$. Sebuah fungsi *hash* untuk sistem kriptografi harus tahan terhadap serangan *second preimage* atau dalam kata lain sulit bagi penyerang untuk menyelesaikan persoalan *second preimage*.

Persoalan : ***Second Preimage***
Diberikan : sebuah fungsi *hash h* dan sebuah pesan *M*
Temukan : M' yang M = M' sehingga $h(M) = h(M')$

3. HASIL DAN PEMBAHASAN

3.1. Pembahasan

Proses pembelajaran merupakan suatu proses yang didalamnya terdapat peserta didik, pendidik dan sumber atau bahan belajar pada suatu lingkungan belajar. Aktifitas pembelajaran akan berjalan dengan lancar apabila ada ketiga aspek tersebut ada.Penyampaian materi yang baik dan lebih sfesifik merujuk tujuan pembelajaran akan membuat peserta didik merasa tertarik untuk mempelajari materi yang disampaikan oleh dosen. Selain mengajarkan materi agar kepada peserta didik, sebaiknya juga dilakukan tes atau ujian sesuai dengan materi yang disampaikan untuk mengetahui seberapa paham peserta didik mengerti tentang materi yang disampaikan pendidik, sehingga dengan demikian tujuan pembelajaran dapat diukur tercapai atau tidak.

Pada CBL, komputer menjadi pembelajaran (*center of learning*) di mana mahasiswa berperan lebih aktif dalam mempelajari suatu materi dengan media utama komputer. Adapun penerapan metode *Computer Based Learning* (CBL) tersebut adalah sebagai berikut :

1. Tutorial
   Pada menu tutorial berisi materi-materi atau pengertian dan penjelasan tentang pembelajaran kriptografi yang berguna untuk menjawab soal-soal.
   a. Materi Kriptografi
      Kriptografi adalahilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi kerahasiaan, keutuhan data dan otentikasi entitas.
   b. Fungsi *Hash*
      Fungsi *hash* adalah fungsi yang melakukan pemetaan pesan dengan panjang sembarangan ke sebuah teks khusus yang disebut *message digest* dengan panjang tetap. Fungsi *hash* umumnya dipakai sebagai nilai uji (*check value*) pada mekanisme keutuhan data.
   c. Enkripsi
      Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Enkripsi dapat digunakan untuk keamanan, tetapi teknik lain masih diperlukan untuk membuat

komunikasi yang aman, terutama untuk memastiksn integritas dan autitentikasi dari sebuah pesan.

d. Deskripsi
Deskripsi adalah proses untuk mengubah kebalikan dari enkripsi upaya pengolahan data menjadi sesuatu yang dapat diutarakan secara jelas dan tepat dengan tujuan agar dapat dimengerti oleh orang yang tidak langsung mengalami sendiri.

e. *Plaintext*
Pesan atau data dalam bentuk aslinya yang dapat terbaca. *Plaintext* adalah masukan bagi algoritma enkripsi. Untuk selanjutnya digunakan istilah teks asli sebagai padanan kata *plaintext.*

f. *Ciphertext*
Ciphertext adalah keluaran algoritma enkripsi. *Ciphertext* dapat dianggap sebagai pesan dalam bentuk tersembunyi. Algoritma enkripsi yang baik akan menghasilkan *ciphertext* yang terlihat acak. Untuk selanjutnya digunakan istilah texs sandi sebagai padanan kata *ciphertext*.

2. Praktik atau Latihan
Seperti yang telah di uraikan sebelumnya bahwa setelah peserta mempelajari setiap materi, maka akan dilakukan pengujian (*test*). Latihan dalam aplikasi pembelajaran ini disajikan dalam bentuk latihan pilihan berganda dengan jumlah soal 5 . setiap jawaban mahasiswa yang benar akan disajikan *feedback* secara otomatis oleh aplikasi apakah jawaban benar atau tidak.

Berikut uraian contoh soal yang akan ada dalam aplikasi pada setiap materi pelajaran.

1. Layanan yang ditunjukan untuk menjaga agar pesan tidak dapat dibaca pleh pihak-pihak yang tidak berhak. Berikut ini merupakan pengertian dari..
   a. Kerahasiaan
   b. Integritas data
   c. Otentikasi
   d. Ningpenyangkalan
2. Dibawah ini yang merupakan istilah-istilah pada kriptografi adalah…..
   a. Plainteks, Ciphertext, Enkripsi, Deskripsi, Cipher.
   b. Secrecy, Key Message,Digest, Hash
   c. Kerahasiaan, Integritas data, Otentikasi, Nirpenyangkalan
   d. Semuanya Benar.
3. Dibawah ini yang merupakan pengertian Enkripsi adalah….
   a. Proses pengubahan dari plaintext ke ciphertext, dengan algoritma kriptografi tertentu
   b. Semua data yang belum diproses melalui suatu algoritma kriptografi, plaintext dapat berupa text, image atau bentuk lain.
   c. Informasi hanya dapat diakses oleh yang berhak
   d. Layanan yang menjaminbahwa pesan masih asli\utuh atau belum tentu pernah memanipulasi selama pengiriman.
4. Proses pengubahan dari plaintext ke ciphertext, dengan algoritma kriptografi tertentu. Pernyataan diatas merupakan pengertian dari….
   a. Secrecy
   b. Integrity
   c. Enkripsi
   d. Message Digest
5. Dibawah ini yang merupakan tujuan kriptografi adalah….
   a. Informasi dengan aman
   b. Informasi tidak rusak
   c. Informasi yang hanya diakses oleh yang berhak
   d. Semuanya benar

Keterangan untuk setiap soal yang dijawab :

1. Latihan pada materi pembelajaran kriptografi. Ruang lingkup soal mengenai defenisi dan fungsi kriptografi
   Jumlah soal = 5 soal
   Jenis soal = pilhan ganda
   Skor setiap soal= (apbila benar), apabila salah maka skor = 0
   Standar nilai kemampuan >= 60
3. Games
   Pemanfaatan game dalam pembelajran merupakan salah satu unsur penting untuk menghilangkan kejenuhan atau kebosanan mahasiswa dalam belajar permainan (*game)* dapat meningkatkan minat peserta untuk tetap meminati pelajaran yang sedang dipelajari.
4. Simulasi
   Model simulasi pada dasarnya menampilkan dan memadukan unsure teks, gambar audio dan gerak dan panduan warna yang serasi, dengan demikian mahasiswa bisa lebih mengerti konsep tentang kriptografi.

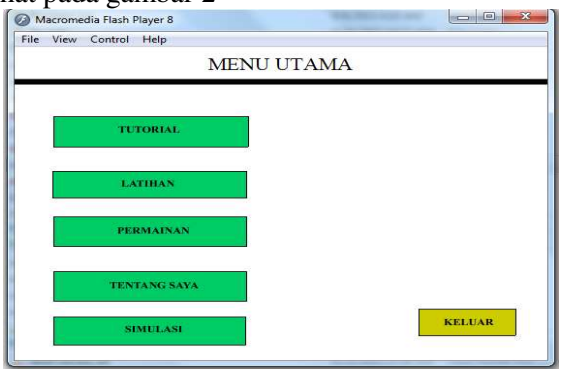
Pembelajaran kriptografi pada algoritma fungsi *hash* yang telah dirancang menggunakan bahasa pemrograman macromedia flash 8, dimana untuk mengetik *listing program* dilakukan pada *action script* yang merupakan perintah *script*.

Pembelajaran kriptografi pada algoritma fungsi hash yang dirancang menggunakan metode *computer based learning* (CBL), dimana pada metode ini berguna agar peserta didik yang mengguanakan aplikasi pembelajaran ini dapat melakukan simulasi dari program materi yang telah diberikan. Berikut hasil dari implementasi program keseluruhan yang telah dirancang :

1. Menu utama
   Menu utama ini ini menampilkan pilihan menu yang ingin dijalankan atau dipergunakan. Pada menu utama tersedia empat pilihan menu yaitu :

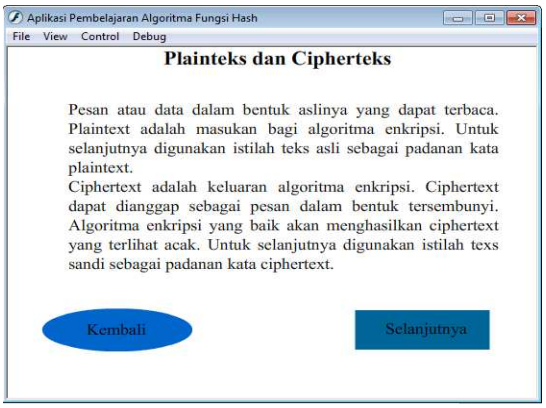
a. Tutorial
b. Latihan
c. Permainan
d. Tentang saya
e. Simulasi

Menu tersebut dapat dilihat pada gambar 2



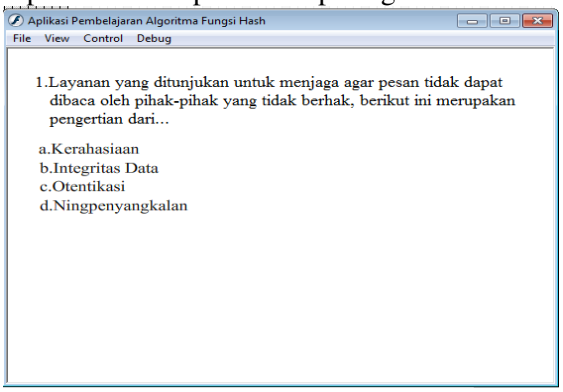
Gambar 2. Tampilan Menu Utama

Pada menu tutorial ini terdapat materi-materi yang membahas mengenai pemebelajaran kriptografi. Menu tutorial dapat dilihat pada gambar 3

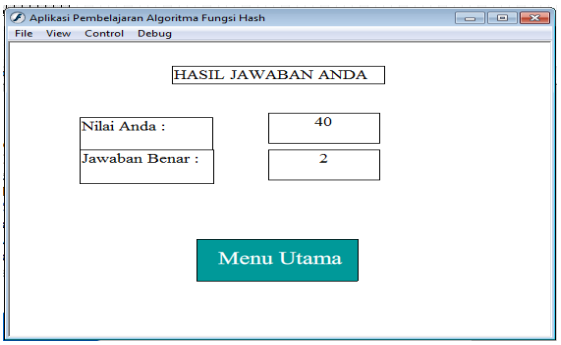


Gambar 3. Tampilan Menu Tutorial

Pada menu ini menampilakn butiran-butiran soal yang membahas tentang kriptografi dan algoritma fungsi hash, tampilan menu dapat dilihat pada gambar dibawah ini

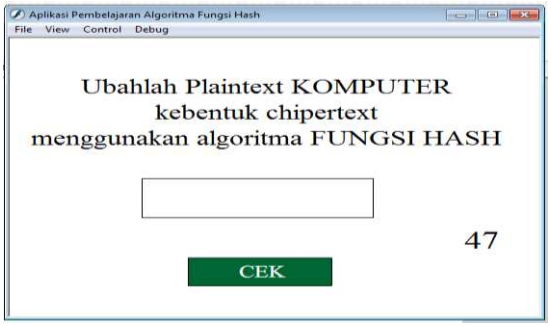


Gambar 4. Tampilan Menu Latihan

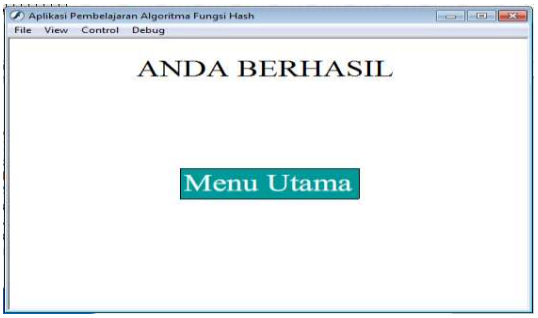


Gambar 5. Tampilan Hasil Menu Latihan

Pada menu ini hanya terdapat soal-soal latihan mengubah plainteks ke bentuk chiperteks yang dalam penyelesaiannya diberikan waktu batas waktu.

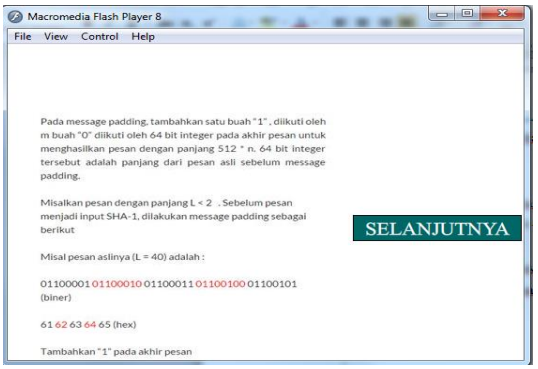


Gambar 6. Tampilan Menu Permainan

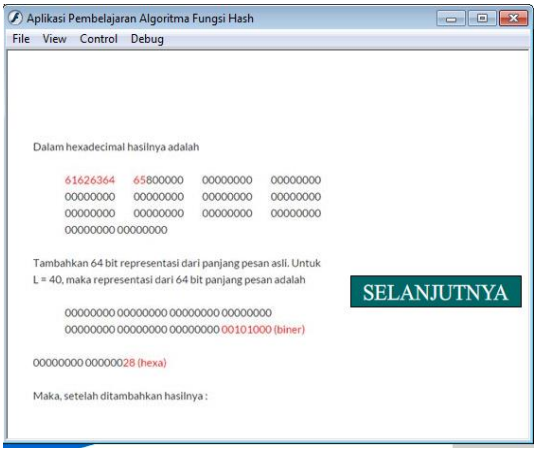


Gambar 7. Tampilan Menu Permainan Jawaban Tepat

Pada menu ini menampilkan cara pengerjaan algortima fungsi hash, gambar dapat dilihat pada gambar 18



Gambar 8. Tampilan Menu Simulasi



Gambar 9. Tampilan Menu Simulasi

4. KESIMPULAN

Dari pembahasan sebelumnya, maka penulis menarik kesimpulan sebagai berikut :

1. Aplikasi ini dibuat untuk pembelajaran kriptografi.
2. Perancangan aplikasi pembelajaran kriptografi yang menggunakan metode *Computer Based learning* (CBL) dibuat untuk memudahkan pengguna secara umum dapat mengetahui dan mempelajari tentang kriptografi.
3. Perancangan aplikasi pembelajaran kriptografi dirancang menggunakan *Macromedia Flash 8*, sehingga pengguna secara umum dapat mudah mengetahui sekilas tentang kriptografi.

DAFTAR PUSTAKA

[1] Bin Ladjamudin, Al-Bahra, 2005, *Analisis dan Desain Sistem Informasi*, Graha Ilmu, Yogyakarta
[2] Jogiyanto, H.M, 2005, *Analisis dan Desain Sistem*, Andi Offiset, Yogyakarta
[3] M, Scott pada Buku Principle of Management Information System, Perancangan, 1977
[4] Sagala Syaiful, 2011, *Suvervisi Pembelajaran*, Penerbit Andi, Yogyakarta
[5] Sadikin Rifki, 2012, *Kriptografi Untuk Keamanan Jaringan*, Penerbit Andi, Yogyakarta
[6] T Limbong, P.D Silitonga, *Local Development Application Of Learning Content-Based Multimedia Batak Toba Scripts*, AISTELL, UNIMED Press, 2016
[7] Zeembry, 2001, *Animasi Macromedia Flash 5*, PT Elex Media Komputindo, Jakarta
[8] http://pelita–Informatika.com/berkas/jurnal/4312.pdf