CORE
Metadata, citation and similar papers at core.ac.uk
Provided by Jurnal Online Universitas Islam Sumatera Utara

Sistem Pembelajaran dan Pemahaman Algoritma *Electronic Code Book (*ECB*)* Menggunakan Metode *Computer Assisted Instruction* (CAI)

Helma Widya
Dosen Teknik Informatika – Institut Teknologi Medan
helmawidya@itm.ac.id

Abstrak

Algoritma Electronic Code Book (ECB) merupakan salah satu teknik dalam kriptografi modern. Algoritma Electronic Code Book (ECB) beroperasi pada mode block cipher yaitu membagi blok-blok bit plainteks. Pada algoritma Electronic Code Book (ECB) setiap blok plainteks dienkripsi secara individual dan independen menjadi blok cipherteks. Hal ini berkaitan dengan isi dari mata kuliah tersebut yang tidak hanya membahas tentang teori, namun dibutuhkan pengalaman untuk prakteknya. Maka akan lebih mudah jika dapat merancang dan membangun sebuah sistem dimana dapat mencakupi materi yang ada secara utuh, tertata rapi namun tetap dapat dirasakan menarik oleh mahasiswa yang mengikuti proses pembelajaran. MetodeComputer Assisted Instruction (CAI) adalah suatu pembelajaran menggunakan program pendidikan yang dirancang khusus untuk bertindak sebagai perangkat ajar yang dalam pembelajarannya terdapat tutorial, latihan, simulasi dan games. CAI merupakan suatu cara penggunaan komputer secara langsung dalam proses pembelajaran sebagaimana pengganti buku dan pengajar (guru). Dengan menggunakan CAI, diharapkan cara belajar pengguna dapat diubah menjadi cara belajar yang lebih aktif, interaktif dan menarik. Dengan menganalisa masalah yang ada dan merancangan sebuah sistem pembelajaran algoritma Electronic Code Book (ECB) menggunakan metode yang telah diterapkan, maka menghasilkan sebuah aplikasi pembelajaran yang akan membantu mahasiswa dalam memahami materi Electronic Code Book (ECB).

Kata Kunci : Pembelajaran, *Computer Assisted Instruction, Electronic Code Book*

I. PENDAHULUAN

Media pembelajaran banyak jenis dan macamnya, dari yang paling sederhana dan murah hingga yang canggih dan mahal.Ada yang sudah tersedia untuk langsung dimanfaatkan dan ada yang sengaja dirancang. Saat ini teknologi komputer telah menawarkan peluang-peluang baru dalam proses pembelajaran baik di ruang kelas, belajar jarak jauh maupun belajar mandiri. Komputer memiliki fungsi yang sangat banyak dalam dunia pendidikan.

Pada era globalisasi seperti sekarang, proses pembelajaran khususnya pada pembelajaran di perguruan tinggi, proses pembelajaran harus dapat mengikuti perkembangan zaman, namun harus tetap sesuai dengan standarisasi yang ada dimana proses pembelajaran diharapkan dilakukan secara timbal balik atau mahasiswa tidak hanya mampu menangkap hal yang dijelaskan, namun dapat memberikan feedback yang baik atas materi yang sedang dipelajari.

Dalam perguruan tinggi khususnya jurusan teknik informatika terdapat berbagai mata kuliah komputer. Salah satunya adalah mata kuliah kriptografi.Pada mata kuliah ini tedapat materi yang membahas tentang *block cipher* yang dalam algoritma ini sering mengalami permasalahan dalam pemahamannya.Salah satu mode yang ada dalam *block cipher* adalah mode *Electronic Code Book (ECB).* Algoritma *Electronic Code Book (ECB)* merupakan salah satu teknik dalam kriptografi modern. Algoritma *Electronic Code Book (ECB)* beroperasi pada mode *blockcipher* yaitu membagi blok-blok bit plainteks. Pada algoritma *Electronic Code Book (ECB)* setiap blok plainteks dienkripsi secara individual dan independen menjadi blok cipherteks. Hal ini berkaitan dengan isi dari mata kuliah tersebut yang tidak hanya membahas tentang teori, namun dibutuhkan pengalaman untuk prakteknya. Maka jalan keluar untuk permasalahan tersebut adalah dengan merancang dan membangun sebuah sistem dimana dapat mencakupi materi yang ada secara utuh, tertata rapi namun tetap dapat dirasakan menarik oleh mahasiswa yang mengikuti proses pembelajaran. Pemenuhan kebutuhan kata yang menarik bagi mahasiswa inilah yang sebenarnya menjadi inti latar belakang, sehingga dalam merancang sistem yang menarik diperlukan penggabungan antara berbagai variabel, seperti variabel visualisasi, audio, dan gerakan animasi. Perancangan ini sendiri dibutuhkan ketelitian antara pembagian porsi bagi masing-masing variabel tersebut, sehingga sistem yang dihasilkan dapat menjadi suatu sistem yang menjadikan mahasiswa yang memakainya mengerti serta memahami materi yang ada dan dijelaskan, dan pada akhirnya mahasiswa dapat memberikan sebuah feedback terkait pembelajaran tersebut, walau pada hakekatnya tidak ada sistem yang 100% benar-benar sempurna, sehingga diharapkan jika mendapat kendala lain, mahasiswa dapat mandiri dengan mencari jalan keluar atas permasalahan

yang dihadapi diluar, seperti mencari dengan media internet, bertanya kepada dosen, dan lain sebagainya.

Salah satu metode pembelajaran yang berbantuan komputer yaitu *Computer Assisted Instruction* (CAI). Metode*Computer Assisted Instruction* (CAI) adalah suatu pembelajaran menggunakan program pendidikan yang dirancang khusus untuk bertindak sebagai perangkat ajar yang digunakan sebagai tutorial, latihan pembahasan dan untuk menyajikan topik pelajaran. CAI merupakan suatu cara penggunaan komputer secara langsung dalam proses pembelajaran sebagaimana pengganti buku dan pengajar (guru). Dengan menggunakan CAI, diharapkan cara belajar pengguna dapat diubah menjadi cara belajar yang lebih aktif, interaktif dan menarik.

II. LANDASAN TEORI

2.1 Perancangan

Menurut kenyataan Joseph Mansueto, perancangan adalah satu proses untuk membuat keputusan tentang apa yang perlu dilakukan oleh organisasi. (Ahmad SMN, dkk, Pengurusan Teknologi, 2005: 5)

Menurut Syifaun Nafisah, perancangan adalah penggambaran, perencanaan dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah ke dalam satu kesatuan yang utuh dan berfungsi Perancangan sistem dapat dirancang dalam bentuk bagan alir sistem (*system flowchart*), yang merupakan alat bentuk grafik yang dapat digunakan untuk menunjukan urutan-urutan proses dari sistem. (Muhammad Fadlan, *Perancangan Aplikasi Pembelajaran Sejarah Nabi Muhammad Saw Berbasis Multimedia Dengan Metode Computer Based Instruction (CBI)*, Vol. IV, No. 3, 2014).

Berdasarkan dari definisi diatas, dapat disimpulkan bahwa perancangan adalah suatu konsep mendesain atau mengubah hasil rancangan ke dalam struktur konsep yang baru.

2.2 Aplikasi

Aplikasi adalah penggunaan atau penerapan suatu konsep yang menjadi pokok pembahasan. Aplikasi dapat diartikan juga sebagai program komputer yang dibuat untuk menolong manusia dalam melaksanakan tugas tertentu. Aplikasi software yang dirancang untuk penggunaan praktisi khusus, klasifikasi luas ini dapat dibagi menjadi 2 (dua) yaitu:

1. Aplikasi *software spesialis*, program dengan dokumentasi tergabung yang dirancang untuk menjalankan tugas tertentu.
2. Aplikasi paket, suatu program dengan dokumentasi tergabung yang dirancang untuk jenis masalah tertentu.

(Muhammad Fadlan, *Perancangan AplikasiPembelajaran Sejarah Nabi Muhammad Saw Berbasis Multimedia Dengan Metode Computer Based Instruction (CBI)*, Vol. IV, No. 3, 2014).

Dari uraian di atas dapat disimpulkan bahwa perancangan aplikasi adalah persiapan, atau rencana untuk merancang dan menyusun langkah-langkah perancangan dan mengimplementasikan suatu program yang ditulis atau dirancang untuk menangani masalah tertentu.

2.3 Multimedia

Multimediaadalah penggunaan komputer untuk menyajikan dan menggabungkan teks, suara, gambar, animasi dan video dengan alat bantu (*tool*) dan koneksi (*link*) sehingga pengguna dapat bernavigasi, berinteraksi, berkarya dan berkomunikasi.

Multimedia sering digunakan dalam dunia hiburan. Selain dari dunia hiburan, Multimedia juga diadopsi oleh dunia Game.**Multimedia** juga dapat diartikan sebagai penggunaan beberapa media yang berbeda dalam menyampaikan informasi berbentuk text, audio, grafik, animasi, dan video.

Multimedia dimanfaatkan juga dalam dunia pendidikan dan bisnis.Di dunia pendidikan, multimedia digunakan sebagai media peengajaran, baik dalam kelas maupun secara sendiri-sendiri atau otodidak.Di dunia bisnis, multimedia digunakan sebagai media profil perusahaan, profil produk, bahkan sebagai media kios informasi dan pelatihan dalam sistem *e-learning*.

2.4 Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: "*cryptos*" artinya "*secret*" (rahasia), sedangkan "*graphein*" artinya "*writing*" (tulisan), Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia). Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentifikasi (Rinaldi Munir, 2006; 11).

Definisi yang digunakan di dalam buku menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Definisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata . Namun saat ini kriptografi lebih dari sekadar *privacy*, tetapi juga untuk tujuan *data integrity*, *authentication,* dan *non-repudation*.

2.5 Algoritma

*Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematis dan logis.*Kata *logis* merupakan kata kuncidalam algoritma. Langkah-langkah dalam algoritma harus logis dan harusdapat ditentukan bernilai salah atau benar.Dalam beberapa konteks, algoritma adalah spesifikasi urutan langkah untukmelakukan pekerjaan tertentu. Pertimbangan dalam pemilihan algoritmaadalah Algoritma haruslah benar artinya algoritma akan

memberikankeluaran yang dikehendaki dari sejumlah masukan yang diberikan, tidakpeduli sebagus apapun algoritma, kalau memberikan keluaran yang salah pastilah algoritma tersebut bukanlah algoritma yang baik.Pertimbangan kedua yang harus diperhatikan adalah kita harus mengetahui seberapa baik hasil yang dicapai oleh algoritma tersebut. Hal ini penting terutama pada algoritma untuk menyelesaikan masalah yang memerlukan aproksimasi hasil (hasil yang hanya berupa pendekatan). Algoritma yang baik harus mampu memberikan hasil yang sedekat mungkin dengan nilai yang sebenarnya. Efisiensi algoritma yaitu efisiensi algoritma dapat ditinjau dari dua hal yaitu efisiensi waktu dan memori. Meskipun algoritma memberikan keluaran yang benar (paling mendekati), tetapi jika kita harus menunggu berjam-jam untuk mendapatkan keluarannya, algoritma tersebut biasanya tidak akan dipakai, setiap orang menginginkan keluaran yang cepat. Begitu juga dengan memori, semakin besar memori yang terpakai maka semakin buruklah algoritma tersebut. Dalam kenyataannya, setiap orang bisa membuat algoritma yang berbeda untuk menyelesaikan suatu permasalahan, walaupun terjadi perbedaan dalam menyusun algoritma, tentunya kita mengharapkan keluaran yang sama. Jika terjadi demikian, carilah algoritma yang paling efisien dan cepat (Rinaldi Munir, 2006; 10).

2.7 *Macromedia Flash*

Menurut Yudhiantoro, *Macromedia Flash* adalah sebuah program yang ditujukan kepada para desaigner maupun programer yang bermaksud merancang animasi untuk pembuatan halaman web, presentasi untuk tujuan bisnis maupun proses pembelajaran hingga pembuatan game interaktif serta tujuan-tujuan lain yang lebih spesifik.

Menurut Riski Rahman J, *Macromedia Flash* adalah *software* yang banyak dipakai oleh para profesional *web* karena kemampuannya yang mengagumkan dalam menampilkan multimedia, menggabungkan unsur teks, grafis, animasi, suara dan serta interaktivitas bagi pengguna program animasi internet. Menurut Astuti Salim, *Macromedia Flash* adalah salah satu *Future Splash Animator* yang memudahkan pembuatan animasi pada layar komputer dalam menampilkan gambar secara audiovisual dan lebih menarik.

III. ANALISA DAN PERANCANGAN

3.1 Analisa

Masalah yang dihadapi adalah bagaimana menyajikan sebuah materi pembelajaran yang lengkap dan menarik sehingga dapat mempermudah mahasiswa dalam memahami pelajaran, dalam hal ini belajar tentang mode *Electronic Code Book (ECB)* pada algoritma*cipher block*.Dimana materi yang akan disajikan adalah materi yang membahas tentang proses enkripsi dan dekripsi pada mode *Electronic Code Book (ECB).*Materi yang di ambil berdasarkan buku-buku, jurnal dan internet. Agar penyajian materi dapat terstruktur dan menarik maka dibutuhkan suatu cara yaitu dengan menggunakan metode *Computer Assisted Instruction* (CAI) atau mengajar dengan menggunakan bantuan komputer, dimana komputer sebagai sarana utama atau alat bantu yang menampilkan objek yang di ajarkan, yang di sertakan dengan video dan audio sehingga mahasiwa dapat lebih memahami dan menguasai materi pembelajaran.

Penyajian materi akan disajikan melalui tutorial terlebih dahulu, adapun isi dari tutorial tersebut yaitu:

1. Pengenalan
2. Penyajian materi
3. Contoh soal
4. Pertanyaan dan respons

3.2 Penerapan Metode *Computer Assisted Instruction* (CAI)

Metode CAI yang diterapkan dalam pembelajaran ini yaitu : model tutorial, model latihan, model simulasi, dan model permainan.

3.3 Perancangan

Perancangan sistem merupakan rancangan awal sebelum dilakukan penyelesaian suatu masalah yang ada. Pencapaian tujuan atau hasil yang diinginkan sesuai dengan kebutuhan dari permasalahan yang ada, maka suatu rancangan sistem diperlukan untuk mendapatkan gambaran secara garis besar seluruh masalah yang akan di komputerisasi. *UML* sebagai bahasa pemodelan untuk merancang sistem pada aplikasi yang akan di bangun.

Flowchart

Flowchart digunakan untuk penyajian yang sistematis tentang proses dan logika dari kegiatan, penanganan informasi atau penggambaran secara grafik dari langkah-langkah dan urut-urutan prosedur dari suatu program.

Flowchart membantu analis dan programmer untuk memecahkan masalah kedalam segmen-segmen yang lebih kecil dan menolong dalam menganalisis alternatif-alternatif lain dalam pengoperasian.

Flowchart diasumsikan sebagai salah satu cara penyajian dari suatu algoritma.

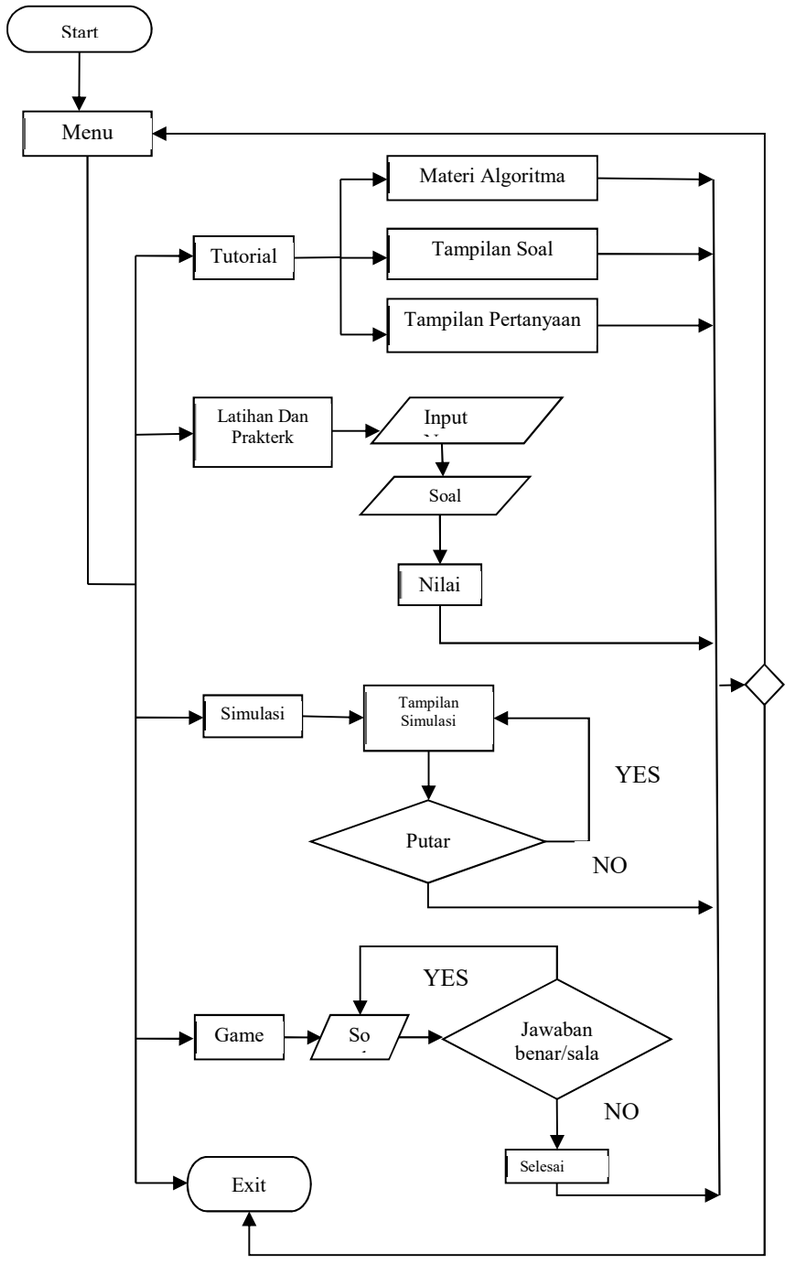
IV. ALGORITMA DAN IMPLEMENTASI

4.1 Algoritma

Algoritma merupakan urutan langkah-langkah logis dalam penyelesaian masalah yang disusun secara sistematis. Langkah-langkah yang tidak benar dapat memberikan hasil yang salah. Pada algoritma pembelajaran ini akan melakukan tahapan-tahapan dalam perancangan aplikasi pembelajaran kriptografi algoritma *Electronic Code*

Book (ECB). Adapun algoritma pembelajaran ini adalah:

1. Algoritma penyajian materi
2. Algoritma latihan dan praktek
3. Algoritma penyajian simulasi
4. Algoritma penyajian *games*



Gambar 1. Flowchart

4.1.1 Algoritma Penyajian Materi

Berikut ini merupakan algoritma dari penyajian materi aplikasi pembelajaran algoritma *electronic code book*

Input : M←Materi *ECB*; C←contoh soal; P←pertanyaan dan respon

Output :

View pembahasan materi yang akan ditampilkan

Proses :

If (M←"materi *ECB*") *then*

View halaman materi *Electronic Code Book*

Else if (C←"contoh soal") *then*

View halaman contoh soal *Electronic Code Book*
Else if (P←"pertanyaan dan respon") *then*
View halaman pertanyaan dan respon
End if

4.1.2 Algoritma Latihan dan Praktek

Berikut ini merupakan algoritma dari latihan dan praktek aplikasi pembelajaran algoritma *electronic code book*

Input:n ←nama; j ←jawaban;
Output: s←nilai;
Proses **:**
Deklarasi n, s : integer j: boolean
n ← inputkan nama
If(nama←"kosong") then
Tampilkan input nama kosong
Else
While(soal latihan) do
Tampil halaman soal latihan
j ← inputkan jawaban
if(jawaban←"benar")th
en
nilai = n+30
else
nilai = n+0
end if
end while

4.1.3 Algoritma Penyajian Simulasi

Berikut ini merupakan algoritma dari simulasi aplikasi pembelajaran algoritma *Electronic Code Book.*

Input : v←video;
Output :
View simulasi proses kerja algoritma;
Proses :
If (v← "jalankan video simulasi" *then*
View jalankan simulasi
End if

4.1.4 Algoritma Penyajian *Games*

Berikut ini merupakan algoritma dari *games* aplikasi pembelajaran algoritma *electronic code book*

Input **:** j ←jawaban
Output **:** boolean (b←halaman benar/s← halaman salah)
Proses **:**
Deklarasi : j ← integer
While(soal game) do
Tampil halaman soal game
j ← inputkan jawaban
if(
j←jawaban"benar")then
View halaman
Anda Benar
else
View halaman
Maaf Jawaban
Anda Masih Salah
end if
end while

4.2 Spesifikasi Perangkat Keras dan Perangkat Lunak

Peralatan yang digunakan untuk proses pembuatan aplikasi *Text Editor* adalah menggunakan perangkat keras (*hardware*) dan perangkat lunak (*software*). Berikut ini merupakan spesifikasi dari perangkat keras yang digunakan penulis untuk menjalankan aplikasi :

1. Prosesor AMD A10 Radeon R6, 2.50 GHZ.
2. Memory 4 GB.
3. Hard Disk 1000 GB.
4. AMD radeon R6 Graphics.
5. Monitor dengan resolusi 1366 x 768 pixel.
6. Mouse
7. Keyboard

Adapun perangkat lunak (*software*) yang digunakan untuk menjalankan aplikasi ini adalah lingkungan sistem operasi MS-Windows 7 Ultimate.

4.3 Implementasi

Aplikasi pembelajar dibangun menggunakan *software macromadia flash 8*. Berikut hasil dari implementasi aplikasi keseluruhan :

1. Halaman utama aplikasi pembelajaran

Gambar 2. Halaman Utama

Halaman utama merupakan halaman perbuka dari aplikasi yang dirancang adapun menu dari aplikasi pembelajaran yang dirancang antara lain :

a. Menu tutorial yang berisi halaman materi algoritma *Electronic Code Book* dari aplikasi.
b. Latihan yang berisi pertanyaan pertanyaan dari pembelajaran algoritma *Electronic Code Book*.
c. Simulasi yang merupakan tampilan slide animasi dari aplikasi pembelajaran.
d. *Games* merupakan menu halaman permainan permainan.
e. *Exit* keluar dari aplikasi pembelajaran.

Jika pengguna menekan tombol tabel ASCII maka akan muncul tampilan seperti Gambar 3.

Gambar 3. Halaman Tabel ASCII

2. Halaman materi aplikasi pembelajaran.
   Form materi menyajikan materi-materi yang akan dipelajari oleh peserta didik. Adapun tampilan dari form materi adalah sebagai berikut

Gambar 4. Tampilan Halaman Materi

3. Halaman contoh soal aplikasi pembelajaran
   halaman contoh soal merupakan halaman yang menyajikan beberapa contoh soal agar peserta didik lebih memahami mengenai algoritma *Electronik Code Book* terutama enkripsi dan dekripsi.

Gambar 5. Tampilan Halaman Contoh Soal

4. Halaman pertanyaan dan respon
   Halaman pertanyaan dan respon merupakan halaman pemahaman agar peserta didik lebih memahami meteri yang telah diajarkan.

Gambar 6. Halaman Pembuka Pertannyaan

Gambar 7 di bawah merupakan halaman dari pertanyaan yang akan disajikan

Gambar 7. Pertannyaan Dan Respon

Setelah seluruh pertanyaan terjawab maka aplikasi akan memberikan penilaian dari jawaban-jawaban yang di inputkan peserta didik.

Gambar 8. Halaman Penilaian

5. Halaman latihan dan praktek
   Halaman latihan dan praktek merupakan halaman untuk mengevaluasi pemahaman peserta didik tentang meteri yang telah diajarkan. Gambar 9 merupakan halaman latihan dan praktek yang akan disajikan.

Gambar 9. Halaman Pembuka Latihan Dan Praktek

Gambar 10, merupakan tampilan dari soal yang akan disajikan

Gambar 10. Halaman Soal Latihan Dan Praktek

Gambar 11, merupakan tampilan penilaian dari soal yang disajikan

Gambar 11. Halaman Hasil Evaluasi

V. KESIMPULAN

Setelah menyelesaikan perancangan aplikasi pembelajaran algoritma *Electronic Code Book (ECB)* ini, maka penulis dapat menarik kesimpulan sebagai berikut :

1. Penyajian Materi pada pembelajaran algoritma *Electronic Code Book (ECB)* disajikan dalam bentuk tutorial yang di dalamnya terdapat materi tentang pengenalan kriptografi, enkripsi dan dekripsi, serta penjelasan algoritma *Electronic Code Book (ECB)* secara keseluruhan beserta contoh-contoh soalnya.
2. Metode *Computer Assisted Instruction* (CAI) yang diterapkan dalam pembelajaran algoritma *Electronic Code Book (ECB)* ini meliputi beberapa tipe yaitu, tipe tutorial, latihan dan praktek, simulasi, dan *games.*
3. Aplikasi pembelajaran algoritma *Electronic Code Book (ECB)*yang telah dirancang dapat mencakup materi secara utuh, tertata rapi namun tetap dapat dirasakan menarik oleh mahasiswa yang mengikuti proses pembelajaran.

DAFTAR PUSTAKA

[1] Adi Nugroho,, 2010, *Rekayasa Perangkat Lunak Berorientasi Objek***.** PenerbitAndi, Yogyakarta,.

[2] H. Martinis Yamin, 2013, *Strategi & Metode Dalam Pembelajaran,* GP Press Group, Jakarta.

[2] Muhammad Fadlan, 2014, *Perancangan Aplikasi Pembelajaran Sejarah Nabi Muhammad Saw Berb asis Multimedia DenganMetode Computer Based Instruction (CBI)***,** Vol. IV, No. 3.

[3] Mardi Iwan Gunawan Saragih, 2014, *Perancangan Aplikasi Pembelajaran Bangun Ruang Pada Tingkat SD Berbasis Flash Dengan Metode Computer Assisted Instruction*, Vol. VII, No. 02.

[5] Rusman, Deni Kurniawan, Cepi Riyana, 2012, *Pembelajatan Berbasis Teknologi dan Komputer*, Penerbit Rajawali Pers, Jakarta.

[6] Rusman, Deniurniawan, CepiRiyana, 2012, *Pembelajatan Berbasis Teknologi dan Komputer*, Penerbit Rajawali Pers, Jakarta.

[7] Rinaldi Munir, 2006, *Kriptografi*, Penerbit Informatika Bandung, Bandung, Edisi 1.

[8] Widi Hardiyanto, 2012, *Pemanfaatan Media Pembelajaran Fisika Berbasis Macromedia Flash 8 Guna Meningkatkan Motivasi Belajar Siswa Pada Pokok Bahasan Sifat Mekanik Bahan Kelas X TKJ 2 SMK Batik Perbaik Tahun Pelajaran 2011/2012*, Vol. 01, No. 1,

[9] Yurika Permanasari, Erwin Harahap**,** *2006, Algoritma Data Encryption Standard (Des) Pada Electronic Code Book (ECB)*, Vol.6, No.1.