Aplikasi Pembelajaran Kriptograpi berbasis Mobile menggunakan Computer Assisted Instruction

[1)] **Harvei Desmon Hutahaean**
STMIK Pelita Nusantara Medan Jln. Iskandar Muda No. 1, 20154, Indonesia
E-Mail : harvei.hutahaean@gmail.com

[2)] **Paska Marto Hasugian**
STMIK Pelita Nusantara Medan Jln. Iskandar Muda No. 1, 20154, Indonesia
E-Mail : paskamarto86@gmail.com

ABSTRACT
The source of science is still dominated by books, although with the internet students get information with diverse scientific fields, but actually the information comes from material in the book. To be able to master a material from a book, students must first be able to read and understand well. Nowadays software is growing very rapidly. The world of education has also used software to create interactive learning application methods with multimedia concepts. This can help overcome, the level of difficulty experienced by students, in order to be able to attract student learning interest, so that it can automatically improve the learning process to be more active and effective. Actually this method has been widely used and has good benefits in learning. As for the achievements of this study to assist students in learning and understanding the learning of data security techniques, this is a solution in several learning problems, namely an explanation that is too fast, a conducive atmosphere, time, learning media and student interest.

Keywords: Security, Data, Learning, CAI, Mobile

PENDAHULUAN

Kegunaan teknologi informasi pada abad masa sekarang sangat diperlukan. Sehingga perkembangannya harus di ikuti agar tidak tertinggal. Seseorang yang dapat menumbuhkan sikap kreativitas membutuhkan referensi seperti buku. Berbagai karya yang dibuat oleh siapapun juga tidak akan lepas dari referensi buku. Jadi, buku itu sesuatu yang wajib dibaca oleh siapapun.

Keberhasilan kegiatan belajar mengajar di Perguruan Tinggi baik swasta maupun negeri, bukan hanya ditentukan oleh pengajar/dosen, tentu di pengaruhi juga oleh keaktifan dan kreatifitas mahasiswa. Proses pembelajaran didukung oleh fasilitas yang memadai agar para peserta belajar mampu memahami setiap pelajaran, dan tentu juga dosen maupun pengajar merupakan salaha satu sumber belajar atau sumber informasi, peran dosen juga sangat dibutuhkan sebagai motivator sekaligus fasilitator dalam proses belajar mengajar[1].

Saat ini *software* berkembang sangat pesat. Dunia pendidikan juga telah memanfaatkan *software* untuk membuat metode aplikasi pembelajaran interaktif dengan konsep multimedia. Hal ini dapat membantu mengatasi, tingkat kesulitan yang dialami para mahasiswa, agar dapat dapat menarik minat belajar mahasiswa, sehingga secara otomatis dapat meningkatkan proses belajar menjadi lebih praktis dan efektif. Sebenarnya metode ini telah banyak digunakan dan mempunyai manfaat yang besar dalam proses belajar [2].

Kurikulum yang sekarang ini menuntut adanya fasilitas yang menunjang keberhasilan sebuah proses pendidikan di dalam perkuliahan, termasuk kemampuan pengajar dalam menguasai materi. Model pembelajaran komputer yang tepat perlu dikembangkan sehingga tidak menimbulkan kebosanan dan kejenuhan dari mahasiswa. Terdapat tiga komponen utama pembelajaran, terdiri dari mahasiswa, kompetensi dosen, dan fasilitas pembelajaran.

Perkembangan Teknologi saat ini, telah menyebabkan banyak perubahan termasuk dalam Perguruan Tinggi yang melahirkan konsep *e-learning*, sebagai salah satu media pembelajaran elektronik yang memungkinkan peserta didik lebih cepat menerima pelajaran yang disampaikan. Teknologi pembelajaran berbasis komputer seperti *Computer Assisted Instruction* (CAI) yaitu metode yang digunakan dalam pengembangan pembelajaran dengan konsep multimedia. Model belajar berbasis komputer seperti *Computer Assisted Instruction* (CAI) disebut konsep *e-learning* [3].

Masalah proses belajar serta mengajar sangat penting diperhatikan dalam dunia pendidikan terutama dalam Perguruan Tingi. Dalam proses belajar sehari-hari yaitu dengan proses konvensional kurang mampu meningkatkan kreatifitas proses belajar para anak didik. Dalam aplikasi pembelajaran yang akan dikembangkan dengan memuat materi kriptografi yaitu algoritma RC5 dimana di dalamnya terdapat proses enkripsi plainteks dan dekripsi chiperteks [4][5].

Dari uraian di atas dapat dijabarkan beberapa yang menjadi tujuan dari penelitian yaitu:

1. Menampilkan dan menyajikan teori-teori pengaman data khususnya algoritma RC5.
2. Menerapkan model CAI pada aplikasi pembelajaran matakuliah keamanan komputer.
3. Mengembangkan software media pembelajaran pengamanan data dengan menggunakan aplikasi android.

LANDASAN TEORI

2.1. CAI

Komputer sebagai media yang membantu pekerjaan manusia sangat diperlukan terutama dalam pengembangan aplikasi pembelajaran berbasis multimedia. *Computer Assisted Instruction* menggunakan media komputer menjadi suatu sistem pembelajaran. CAI memberikan dampak terhadap pendidikan. CAI menempatkan perangkat computer sebagai alat pembelajaran individu, yang berarti siswa dapat berinteraksi dengan komputer[6].

Alat bantu pembelajaran merupakan gambaran dari media pembelajaran. Interaksi langsung antara siswa dengan komputer merupakan konsep media yang interaktif.

2.2. Kriptografi

Kriptografi adalah seni atau ilmu yang mempelajari cara mengkodekan atau menyandikan pesan agar tetap aman dari pengganggu [7]. Menurut beberapa pakar bahwa kriptografi adalah cabang dari ilmu matematika yang memiliki banyak fungsi dalam pengamanan data [8]. Kriptografi adalah proses mengambil pesan/message dan menggunakan
beberapa fungsi untuk menggenerasi materi kriptografis (sebuah digest atau message terenkripsi).

2.3. Rivest Cipher 5

Algoritma RC5 merupakan algoritma kriptografi dengan konsep block chiper. RC5 Memberikan tingkat akses keamanan yang akurat. Algoritma RC5 secara ringkas adalah melakukan proses penjumlahan modulus 2 w, kemudian operasi X-OR dan pergeseran x ke kiri sejumlah y [9].

Algoritma RC5 merupakan algoritma simetrik yang diproses dalam bentuk block chiper . Proses yang harus ada pada algoritma RC5 : r (iterasi) untuk rotasi dengan nilai 1,2,3,….255. word dalam satuan bit dibuat dalam w. untuk bit yang support yaitu 16,32 dan 64 bit. Sedangkan kunci (b) range 0,1,2,3…255, key word diubah menjadi array S dugunakan untuk key pada proses enkripsi dan dekripsi [10].

PEMBAHASAN

3.1. Penerapan Metode *CAI*

Penerapan Metode *CAI* pada Algoritma RC5 yaitu :

1. **Tutorial**
   Enkripsi data adalah materi yang akan disajikan dalam pembelajaran ini. Langkah – langkah penyelesaiannya sebagai berikut:
   Fungsi Enkripsi Algoritma RC5 menerima masukan 1 blok yaitu A dan B sebesara w bit [9]. Dalam prose enkripsi diperlukan sebuah tabel key S[O..t - 1].
   A = A + S [0]
   B = B + S [1]
   For i = 1 to r do
   A = ((A⊕ B) <<< B) + S [2i]
   B = ((B⊕ A) <<< A) + S [2i + 1]

2. ***Drill and Practice*** **(Latihan dan Praktek)**
   Menyajikan materi pelajaran untuk dipelajari dan dibuat berupa latihan.
   Proses di komputer yaitu plaintext nya ^ *
   Kemudian melakukan proses enkripsi dan menghasilkan ciphertext (int)
   -10094006915 dan 1055364136
   Kemudian data diubah dari int menjadi string dengan ciphertext (string) [9]. Kemudian plaintext yang dikirim diubah menjadi ciphertext pada sistem komputer diubah ke (int) menjadi -1094006915, 1055364136 lalu diubah menjadi plaintext ^*

3. ***Simulation*** **(simulasi)**
   Simulasi dari cara penyelesaian serta langkah-langkah dari mulai enkripsi hingga deskripsi.
   a. Menampilkan proses enkripsi yang sudah terbagi dua yaitu kiri dan kanan dan setelah itu proses penambahan dengan kunci word yang sebelumnya sudah dilakukan ekspansi. Notasi untuk penjumlahan disimbolkan dengan “+“, dan notasi tersebut disimpan pada reg A dan reg B.

b. seterusnya operasi EX-OR
c. proses pergeseran ke bagian kiri (shift left) sejauh y terhadap x word (x<<< y). y adalah hasil modulo w atau jumlah word w dibagi 2.
d. Bagian akhir dari proses dengan melakukan penggabungan dimana tujuannya yaitu untuk mendapatkan data enkripsi.
e. Untuk prosess dekripsi dilakukan dengan cara berikut :
   1. Data chiperteks yang sudah dibagi dua disimpan di pada register A dan register B.
   2. Setelah itu rotasi ke sebelah kanan dengan jumlah r .
   3. Selanjutnya dilakukan proses EX-OR
   4. Phase akhir yaitu proses pengurangan kepada setiap register dengan key word yang ditunjukan dengan tanda "-", untuk mendapatkan plaintext.

3.2. Game (Permainan)

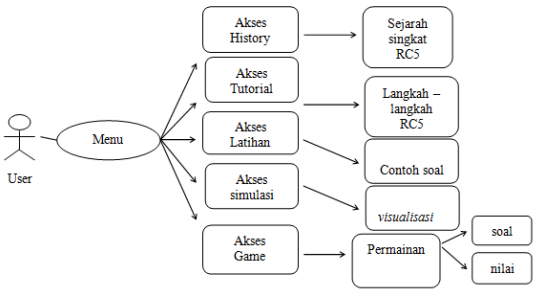
Permainan (*game*) yang disediakan berupa permainan pilihan berganda. Dimana para pengguna harus menebak pilihan (a, b, c atau d) yang sesuai dengan pertanyaan. Jika jawaban benar maka akan mendapatkan skor dari setiap pertanyaan yang disajikan, namun jika jawaban tidak benar maka skor akan tetap atau tidak bertambah. Game ini juga diberikan waktu pada setiap pertanyaan, yang membuat pengguna harus berpikir cepat. Pemberian batasan waktu terhadap game tersebut, pengguna menjadi sangat tertarik untuk menyelesaikannya. Berikut ini adalah contoh *games* pada aplikasi pembelajaran :

1. Algoritma RC5 adalah algoritma block cipher yang dirancang oleh….
   a. Ronald Griya c. Profesor Ronald L. Rivest
   b. Alfouns Romero d. Ligaya

3.3. Perancangan Aplikasi

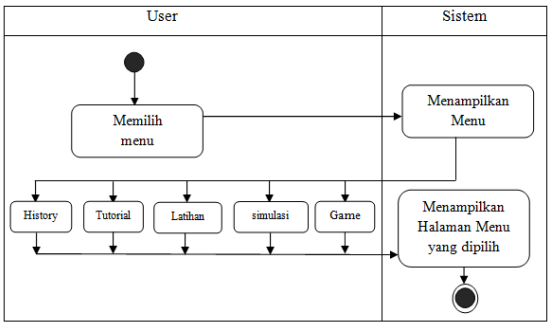
Perancangan sistem dilakukan agar aplikasi yang dibuat dapat berjalan dengan baik dan sesuai dengan yang diharapkan dan terstruktur sehingga mampu memberikan informasi tentang Algoritma RC5. Dalam perancangan ada beberapa tahapan yang harus dilakukan. Adapun fase atau tahapan yang akan dilakukan yaitu membuat *Use Case Diagram, Activity Diagram* dan merancang *output* perangkat lunak pembelajaran.

Gambar 1 menjelaskan *use case* Aplikasi Pembelajaran Algoritma RC5 Dengan Metode berbasis komputer *CAI*.



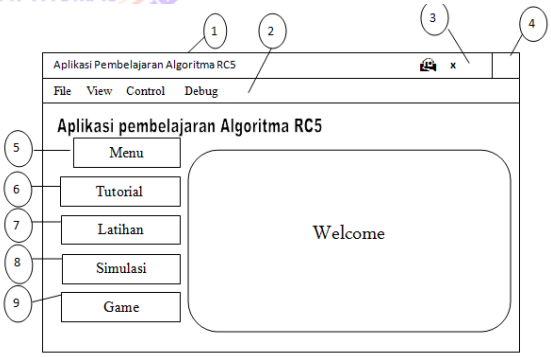
Gambar 1 : Diagram Pembelajaran

Activity Diagram menunjukkan langkah demi langkah untuk melakukan komputasi. Gambar 2 menggambarkan langkah mana yang harus dijalankan secara berurutan dan langkah mana yang dijalankan secara bersamaan.



Gambar 2 : Activity Diagram Pembelajaran

Bagian main menu terdapat empat buah tombol pilihan yaitu History, Tutorial, Latihan dan juga *Game* yang dapat dilihat pada gambar berikut:



Gambar 3 : Rancangan Form Pembelajaran

HASIL

Aplikasi hasil pengembangan yaitu :

1. Tampilan Menu Tutorial

Menu tutorial berisikan penjelasan materi dimana *user* dapat memahami agar dapat mengerjakan soal Latihan.

Gambar 4 : Menu Tutorial

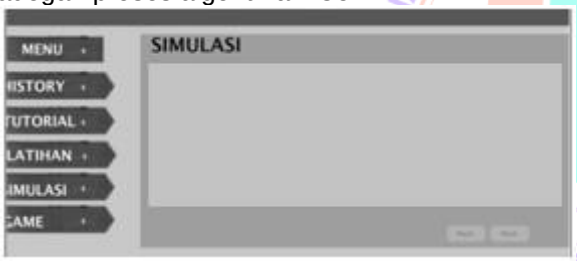
2. Tampilan Menu Latihan

Menu latihan disajikan dengan *user* untuk lebih menembah wawasan tentang algoritma RC 5 terlebih dahulu sebelum masuk kedalam permainan.

Gambar 5 : Menu Latihan

3. Tampilan Menu Simulasi

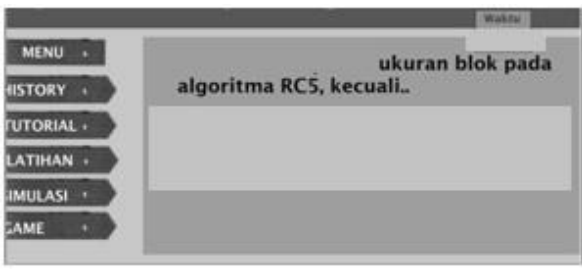
Menu Simulasi berisikan visualisasi / adegan proses algoritma RC5



Gambar 6 : Menu Simulasi

4. Tampilan Menu Game

Menu *Game* disajikan dengan *user* untuk lebih menambah wawasan dan mengasah ingatan pengguna / *user* tentang algoritma RC5 dengan tambahan waktu sebagai acuan dan juga skor sebagai penilaian akhir.



Gambar 7 : Menu Game

KESIMPULAN

Dari penjelasan sebelumnya maka ditentukan kesimpulan dari aplikasi pembelajaran kriptografi ini antara lain :

1. Dari masalah yang ada sistem yang ingin dibangun yaitu dari pembuatan pembelajaran kriptografi dari matakuliah keamanan komputer dimana materinya tentang RC5.
2. Dengan menerapkan metode *CAI* pada aplikasi pembelajaran algoritma RC 5, dapat membantu pengguna untuk belajar dan memahami kriptografi khususnya RC5.
3. Aplikasi komputer pembelajaran ini merupakan media pendukung yang tepat untuk sistem pembelajaran pada kampus, dengan adanya aplikasi ini nantinya dapat memudahkan para mahasiswa dalam memahami materi pembelajaran khususnya mata kuliah kriptografi.

DAFTAR PUSTAKA

[1] I. K. Sudarsana *et al.*, “Paradigma Pedidikan Bermutu Berbasis Teknologi Pendidikan,” *Jayapangus Press Books*, vol. 0, no. 0, Mar. 2018.

[2] P. Berbasis, K. Pbk, and S. Sunarto, “Pembelajaran berbasis komputer (pbk),” pp. 1–11, 1990.

[3] T. Limbong, E. Napitupulu, and P. Simangunsong, Barita,Nauli, “Learning Application Soft Skill for Facial with Computer Assisted Instruction Model,” vol. 1, no. 4, pp. 561–570, 2018.

[4] M. Y. Rhee, *Internet Security : Cryptographic Principles, Algorithms and Protocols*. Seoul National University, Republic of Korea, 2003.

[5] R. Munir, “Kriptografi,” *Inform. Bandung*, 2006.

[6] T. Limbong, P. Manullang, and E. Napitupulu, “Dikte Test Applications (IMLA) Using Computer Assisted Instruction (CAI) Model,” *Int. J. Eng. Res. Technol.*, vol. 6, no. 10, pp. 384–388, 2017.

[7] D. Ariyus, “PENGANTAR ILMU KRIPTOGRAFI Teori Analisis Dan Informasi, FI,” *Yogyakarta CV ANDI OFFSET*, 2008.

[8] D. Ariyus, “Kriptografi keamanan data dan komunikasi,” *Yogyakarta Graha Ilmu*, 2006.

[9] I. Wibowo, B. Susanto, and J. Karel T, “Penerapan algoritma Kriptografi Asimetris RSA untuk keamanan data di Oracle,” *J. Inform.*, vol. 5, no. 1, 2009.

[10] “Kriptografi untuk keamanan jaringan dan implementasinya dalam bahasa Jawa / Rifki Sadikin,” p. 2012, 2012.