



Plagiarism Checker X Originality Report

Similarity Found: 10%

Date: Tuesday, March 26, 2019

Statistics: 159 words Plagiarized / 1661 Total words

Remarks: Low Plagiarism Detected - Your Document needs Optional Improvement.

APLIKASI PEMBELAJARAN KRIPTOGRAPHY BERBASIS MOBILE MENGGUNAKAN COMPUTER ASSISTED INSTRUCTION Harvei Desmon Hutahaeen1) Paska Marto Hasugian2) Teknik Informatika STMIK Pelita Nusantara Medan Jln. Iskandar Muda No. 1, 20154, Indonesia harvei.hutahaeen@gmail.com, paskamarto86@gmail.com Abstrak Sumber keilmuan sampai saat ini masih didominasi oleh buku, meskipun dengan adanya internet siswa mendapatkan informasi dengan bidang keilmuan yang beragam, tetapi sesungguhnya informasi tersebut bersumber dari bahan materi pada buku.

Untuk dapat menguasai suatu bahan materi dari buku, terlebih dahulu mahasiswa harus dapat membaca dan memahami dengan baik. 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 oleh** para mahasiswa, agar dapat dapat menarik minat belajar mahasiswa, sehingga secara otomatis dapat meningkatkan proses belajar menjadi lebih aktif dan efektif. Sebenarnya metode ini telah banyak digunakan dan mempunyai manfaat yang baik dalam pembelajaran.

Adapun yang menjadi capaian dari penelitian ini untuk membantu para mahasiswa dalam mempelajari dan memahami pembelajaran teknik pengamanan data, hal ini adalah solusi dalam beberapa masalah pembelajaran yaitu penjelasan yang terlalu cepat, suasana yang kondusif, waktu, media pembelajaran dan minat peserta didik. Kata Kunci : Keamanan, Data, Pembelajaran, CAI, Mobile

PENDAHULUAN Latar Belakang 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 salah satu sumber belajar atau sumber informasi, peran dosen juga sangat dibutuhkan sebagai motivator sekaligus fasilitator dalam proses belajar mengajar. 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 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.

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. Masalah proses belajar serta mengajar sangat penting diperhatikan dalam dunia pendidikan terutama dalam Perguruan Tinggi. 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 plaintext dan dekripsi ciphertext. Tujuan Penelitian **Dari uraian di atas dapat** dijabarkan beberapa **yang menjadi tujuan dari** penelitian yaitu: Menampilkan dan menyajikan teori-teori pengamanan data khususnya algoritma RC5. Menerapkan model CAI pada aplikasi pembelajaran matakuliah keamanan komputer.

Mengembangkan software media pembelajaran pengamanan data dengan menggunakan aplikasi android. LANDASAN TEORI 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 komputer sebagai alat pembelajaran individu, yang berarti **siswa dapat berinteraksi dengan** komputer. Alat bantu pembelajaran merupakan gambaran dari media pembelajaran. **Interaksi langsung antara siswa** dengan komputer merupakan konsep media yang interaktif. B. Kriptografi Kriptografi adalah seni atau ilmu yang mempelajari cara mengkodekan atau menyandikan pesan agar tetap aman dari gangguan.

Menurut beberapa pakar bahwa kriptografi adalah cabang dari ilmu matematika yang memiliki banyak fungsi dalam pengamanan data. Kriptografi adalah proses mengambil pesan/message dan menggunakan beberapa fungsi untuk menggenerasi materi kriptografis (sebuah digest atau message terenkripsi). Rivest Cipher 5 Algoritma RC5 merupakan algoritma kriptografi dengan konsep block cipher. 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. Algoritma RC5 merupakan algoritma simetrik yang diproses dalam bentuk block cipher. 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 digunakan untuk key pada proses enkripsi dan

dekripsi. PEMBAHASAN Penerapan Metode CAI Penerapan Metode CAI pada Algoritma RC5 yaitu : 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 sebesar w bit. Dalam prose enkripsi diperlukan sebuah tabel key $S[0..t - 1]$ $A = A + S [0]$ $B = B + S [1]$ For $i = 1$ to r do $A = ((A \oplus B) \lll B) + S [2i]$ $B = ((B \oplus A) \lll A) + S [2i + 1]$ 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) Kemudian plaintext yang dikirim diubah menjadi ciphertext pada sistem komputer diubah ke (int) menjadi -1094006915, 1055364136 lalu diubah menjadi plaintext * Simulation (simulasi) Simulasi dari cara penyelesaian serta langkah – langkah dari mulai enkripsi hingga dekripsi.

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. seterusnya operasi EX-OR proses pergeseran ke bagian kiri (shift left) sejauh y terhadap x word ($x \lll y$). y adalah hasil modulo w atau jumlah word w dibagi 2.

Bagian akhir dari proses dengan melakukan penggabungan dimana tujuannya yaitu untuk mendapatkan data enkripsi. Untuk proses dekripsi dilakukan dengan cara berikut : Data ciphertext yang sudah dibagi dua disimpan di pada register A dan register B. Setelah itu rotasi ke sebelah kanan dengan jumlah r .

Selanjutnya dilakukan proses EX-OR Phase akhir yaitu proses pengurangan kepada setiap register dengan key word yang ditunjukkan dengan tanda "-", untuk mendapatkan plaintext. 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 : Algoritma RC5 adalah algoritma block cipher yang dirancang oleh... Ronald Griya c. Profesor Ronald L. Rivest b. Alfouns Romero d. Ligaya 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. Use-case Diagram Gambar 1 menjelaskan use case Aplikasi Pembelajaran Algoritma RC5 Dengan Metode berbasis komputer CAI. / Gambar 1 : Diagram Pembelajaran Activity Diagram 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 Perancangan Form Menu Utama 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 : Tampilan Menu Tutorial Menu tutorial berisikan penjelasan materi dimana user dapat memahami agar dapat mengerjakan soal Latihan.

/ Gambar 4 : Menu Tutorial 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 Tampilan Menu Simulasi Menu Simulasi berisikan visualisasi / adegan proses algoritma RC5 / Gambar 6 : Menu Simulasi 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 V KESIMPULAN Dari penjelasan sebelumnya maka ditentukan kesimpulan dari aplikasi pembelajaran kriptografi ini antara lain : Dari masalah yang ada sistem yang ingin dibangun yaitu dari pembuatan pembelajaran kriptografi dari matakuliah keamanan komputer dimana materinya tentang RC5. Dengan menerapkan metode CAI pada aplikasi pembelajaran algoritma RC 5, dapat membantu pengguna untuk belajar dan memahami kriptografi khususnya RC5.

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. REFERENSI Ariyus Dony, 2008, Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi, Yogyakarta, Andi Offset.

Ariyus Dony, 2006, Computer Security, Yogyakarta, Andi Offset.

http://staff.uny.ac.id/sites/default/files/1315683_00/ pembelajaran berbantuan komputer Mahyudin, Rezza. 2009. Studi dan Perbandingan Algoritma ADFGVX Cipher dengan Algoritma Playfair Cipher pada Perang Dunia I. Makalah. Bandung: Institut Teknologi Bandung. Ivan Wibowo, Budi Susanto, Junius Karnel T, Penerapan Algoritma Kriptografi Asimetris RSA Untuk Keamanan Data Di Oracle.

Fakultas Teknik, Universitas Kristen Duta Wacana. Sadikin, Rifki. 2012. Kriptografi untuk Keamanan Jaringan. Yogyakarta: ANDI. Rhe, Man Young. 1994. Cryptography and Secure Communication. Singapore : McGraw-Hill Book Co.

INTERNET SOURCES:

1% - <http://e-jurnal.pelitanusantara.ac.id/index.php/JIPN/article/download/365/240>

<1% -

<http://contoh-contohskripsi.blogspot.com/2010/02/analisis-kesulitan-belajar-bahasa-ara-b.html>

<1% - <http://arikmetafora.blogspot.com/2013/08/>

<1% - https://www.academia.edu/4506455/INTERNET_SEBAGAI_SUMBER_BELAJAR

<1% -

https://bekompas.blogspot.com/2012/04/contoh-ptk-penggunaan-media-gambar-guna_5706.html

<1% - <http://eprints.binadarma.ac.id/2021/1/JurnalBaru.pdf>

<1% -

<https://bimanursyahputra11.blogspot.com/2013/10/perkembangan-teknologi-informasi-dan.html>

<1% -

https://www.academia.edu/5690668/Pengembangan_Multimedia_Pembelajaran_Interaktif

<1% -

<https://gifalytwinsa.wordpress.com/2010/01/07/model-pembelajaran-cai-dan-penerapannya-di-sd/>

<1% - <https://sandimulyana.blogspot.com/feeds/posts/default>

<1% -

<https://must-august.blogspot.com/2014/04/penggunaan-metode-eksperimen-untuk.html>

<1% - <http://lib.unnes.ac.id/27711/1/5202412062.pdf>
<1% -
<http://staff.uny.ac.id/sites/default/files/17b%20herman%20dwi%20surjono%20Pengembangan%20CAI%20Authoring%201996.pdf>
<1% - <https://sartikahinata.wordpress.com/2013/02/15/alatmedia-pendidikan-islam/>
<1% - <https://lekkomputer.wordpress.com/category/kriptografi/>
1% - <https://kriptologi.wordpress.com/category/kriptografi/block-cipher/>
<1% - <https://bincangandroid.blogspot.com/2018/05/>
<1% -
http://repository.uksw.edu/bitstream/123456789/13709/1/T1_672013226_Full%20text.pdf
<1% - https://www.academia.edu/26300023/MAKALAH_PROTOTYPE
<1% -
<https://pelajarbisu.blogspot.com/2015/03/PERANCANGAN-GAME-EDUKASI-BERBASIS-ANDROID.html>
<1% - <http://zonaskripsi.blogspot.com/2012/03/skripsi-komputer-3.html>
<1% - <https://jurnal.umj.ac.id/index.php/fbc/article/download/2109/2018>
<1% -
<http://sekolahonlineprogrammer.blogspot.com/2012/11/pengembangan-media-pembelajaran.html>
<1% -
<http://seminar.uny.ac.id/semnasmatematika/sites/seminar.uny.ac.id/semnasmatematika/files/A-5.pdf>
1% - <http://digilib.unila.ac.id/886/13/DAFTAR%20PUSTAKA.pdf>
1% -
<http://repository.usu.ac.id/bitstream/handle/123456789/52303/Reference.pdf?sequence=2&isAllowed=y>