# Aplikasi Pembelajaran Kriftografi Vigenere Cipher Menggunakan Metode Computer Assisted Instruction

**Yuli Safitri**
STMIK Budi Darma Medan, Jl. Sisingamangaraja No. 338 Simpang Limun Medan
Email : yulisjava@gmail.com

**Abstrak**

Kriptografi Vigenere Cipher merupakan salah satu kriptografi klasik yang cukup amakan digunakan untuk pesan, penggunaan kriptografi pada sebagian mahasiswa mungkin terasa rumit dikarenakan banyak proses dan langkah yang harus digunakan, pembelajaran merupakan sala satu solusi yang bisa digunakan untuk menampilkan materi mengenai kriptografi vigenere cipher, pembelajaran yang dirancang akan menerapakn metode computer assisted instruction. Model Pembelajaran diperlukan untuk membantu mahasiswa dalam memahami pembelajaran dengan cepat dan membuat mahasiswa antusias. Ini adalah model pembelajaran berbasis computer yang disertai dengan metode CAI ( Computer Assisted Instruction ). Tutorial dan latihan ini menggunakan metode pembelajaran strategis dengan memberikan materi, latihan, simulasi, game. Tujuannya adalah untuk membuat mahasiswa memahami materi. Dalam proses pembelajaran ini diimplementasikan dengan Adobe Flash CS6 untuk menghasilkan pembelajaran yang mudah untuk digunakan mahasiswa agar lebih memahami materi tersebut.

**Kata Kunci: Animasi, Visualisasi Kriptografi, Metode Computer Asissted Instruction**

***Abstract***

*Vigenere Cipher cryptography is one of the classic cryptography which is quite easy to use for messages, the use of cryptography on some students may feel complicated because of the many processes and steps that must be used, learning is one solution that can be used to present material about cryptography vigenere ciphers, designed to apply the computer assisted instruction method. Learning models are needed to help students understand learning quickly and make students enthusiastic. This is a computer-based learning model which is accompanied by the CAI (Computer Assisted Instruction) method. These tutorials and exercises use strategic learning methods by providing materials, exercises, simulations, games. The aim is to make students understand the material. In this learning process it is implemented with Adobe Flash CS6 to produce learning that is easy for students to use to better understand the material.*

***Keywords: Animation, Cryptographic Visualization, Computer Assisted Instruction Method***

## 1. PENDAHULUAN

Perkembangan teknologi membawa banyak perubahan pada sebuah program aplikasi dan seharusnya didesain dalam upaya menjadikan teknologi ini mampu memanipulasi keadaan sesungguhnya. Penekanannya terletak pada upaya yang berkesinambungan untuk memaksimalkan aktifitas belajar mengajar sebagai interaksi kognitif antar mahasiswa, materi subjek, dan instruksi (dalam hal ini komputer yang diprogramkan). Dengan Adanya perkembangan ilmu pengetahuan dan teknologi maka seseorang dapat mempelajari sesuatu menjadi lebih mudah, cepat serta memungkinkan seseorang dapat mempelajari sesuatu dengan bersifat otodidak atau belajar sendiri [1].

Salah satu mata kuliah yang diajarkan dalam dunia pendidikan yaitu mata kuliah *kriptografi*. Dalam proses belajar mengajar dikelas terdapat keterkaitan yang erat antara dosen, mahasiswa, sarana dan prasarana. Dosen mempunyai tugas untuk memilih model pembelajaran yang tepat dan sesuai dengan materi yang disampaikan demi tercapainya tujuan pendidikan[2], [3]. Berbagai kendala dalam pembelajaran *kriptografi* terutama pada mahasiswa semester 8 yang sering tidak mengikuti pelajaran atau tidak masuk maka mahasiswa tersebut ketinggalan pelajaran dan pelajaran sebelumnya tidak akan dibahas ulang. Jadi untuk menyelesaikan permasalahan diatas serta untuk mengoptimalisasi proses pembelajaran khususnya pembelajaran *kriptografi* dibutuhkan suatu aplikasi yang dapat membantu memenuhi proses belajar mengajar.

Salah satu bentuk bahan ajar berbantuan komputer yang dapat digunakan adalah CAI (*Computer Assisted Instruction*). *The Associationt for Education Communication and Technology* (1977) mendefenisikan CAI sebagai suatu metode instruksi yang menggunakan komputer untuk mengins-truksikan kepada mahasiswa dan meliputi instruksi-instruksi yang didesain untuk mengajari, mengarahkan, dan menguji mahasiswa sampai pada tingkat kecapaian tertentu yang ingin dicapai.[4], [5]

Dengan menggunakan CAI, pembelajaran tidak hanya terbatas pada satu waktu tertentu saja, seorang mahasiswa dapat menggunakan perangkat lunak tersebut selama dia membutuhkan. Pemanfaatan CAI juga dapat memperbaiki tingkat belajar mahasiswa karena meliputi unsur aktifitas latihan, pembelajaran secara bertahap yang dikendalikan oleh mahasiswa, informasi personal dan animasi.

Adapun rumusan masalah yang dibahas dalam penelitian ini adalah sebagai berikut[6]:

1. Bagaimana proses pembelajaran *kriptografi vigenere cipher* menggunakan metode *Computer Assisted Assisted ?*
2. Bagaimana menerapkan metode *Computer Assisted Instruction (CAI)* pada pembelajaran *kriptografi vigenere cipher* ?
3. Bagaimana merancang aplikasi untuk pembelajaran *kriptografi vigenere cipher* dengan menggunakan metode *Computer Assisted Instruction* ?

## 2. LANDASAN TEORI

### 2.1 Pembelajaran

Pembelajaran ( *instructiont )* merupakan akumulasi dari konsep belajar *(learning),* konsep tersebut dapat dipandang sebagai suatu sistem, sehingga dalam sistem belajar ini terdapat komponen - komponen siswa atau peserta didik, tujuan, materi untuk mencapai tujuan, fasilitas dan prosedur serta alat atau media yang harus dipersiapkan[7], [8]. Pembelajaran dapat diartikan sebagai setiap upaya yang sistematik dan sengaja untuk menciptakan agar terjadi kegiatan interaksi *edukatif* antara dua pihak, yaitu antara peserta didik (warga belajar) dan pendidik (sumber belajar) yang melakukan kegiatan membelajarkan[9].

### 2.2 Kriptografi

Kriptografi *(cryptography)* berasal dari bahasa yunani yaitu *cryptos* yang artinya *secret* (rahasia), sedangkan *graphein* artinya *writing* (tulisan). Jadi, kriptografi berarti *secret writing* (tulisan rahasia). Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat lainnya, isi pesan tersebut mungkin dapat disadap oleh pihak lainnya yang tidak berhak untuk mengetahui isi pesan tersebut [10], [11]. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain.

### 2.3 Vigenere cipher

Vigenere Cipher adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan BattistaBellaso. Beliau menuliskan metodenya tersebut pada bukunya yang berjudul La Cifra del. Sig. Giovan Battista Bellaso pada tahun 1553. Nama vigenere sendiri diambil dari seorang yang bernama Blaisede Vigenere. Nama vigenere diambil sebagai nama algoritma ini karena beliau menemukan kunci yang lebih kuat lagi untuk algoritma ini dengan metode autokey cipher meskipun algoritma dasarnyatelah ditemukan lebih dahulu oleh Giovan Battista Bellaso[12].

Algoritma ini menjadi terkenal karena cukup sulit dipecahkan. Matematikawan Charles Lutwidge Dodgson menyatakan bahwa algoritma ini tidak terpecahkan. Pada tahun 1917, ilmuwan Amerika menyebutkan bahwa Vigenere cipher adalah sesuatu yang tidak mungkin untuk ditranslasikan. Namun hal ini terbantahkan sejak Kasiski berhasil memecahkan algoritma pada abad ke-19. Pada dasarnya Vigenere Cipher serupa dengan Caesar Cipher, perbedaannya adalah pada Vigenere Cipher setiap huruf pesan aslinya digeser sebanyak satu huruf pada kuncinya sedangkan pada Caesar Cipher setiap huruf pesannya digeser sebanyak 1 huruf yang sama.

Enkripsi : Ci= (Pi+Ki) mod 26

Depenelitian : Pi= (Ci+Ki) mod 26

### 2.4 Computer Assisted Instruction (CAI)

Menurut Herman D Surjono (1999), istilah CAI (Computer-Assisted Instruction) umumnya menunjuk pada semua software pendidikan yang diakses melalui computer di mana anak didik dapat berinteraksi dengannya. Sistem komputer menyajikan serangkaian program pengajaran kepada anak didik baik berupa informasi maupun latihan soal-soal untuk mencapai tujuan pengajaran tertentu dan peserta belajar melakukan aktivitas belajar dengan cara berinteraksi dengan sistem komputer[6]. *Computer Assisted Instructiont* (CAI) memiliki beberapa model yaitu : model *tutorial*, model *drill and practice*, model simulasi dan model *instructional game*.

## 3. PEMBAHASAN

### 3.1 Analisa Masalah

Kriptografi merupakan salah satu bidang ilmu yang berkaitan dengan keamanan komputer, kriptografi bagi sebagian mahasiswa merupakan materi yang susah selain berhubungan dengan perhitungan XOR, komputasi numeric, biner dan sebagainya.

Vigenere cipher merupakan salah satu jenis kriptografi klasik yang bisa digunakan untuk mengamankan pesan teks, vigenere cipher memiliki cara kerja enkripsi substitusional cipher artinya satu huruf diganti dengan huruf lainnya[13]. Permasalahan yang biasa terjadi dalam pembelajaran kriptografi adalah bagaimana menjelaskan dan menyelesaikan cara kerja algoritma khususnya algorima Vigenere Cipher. Pembelajaran yang dirancang dijadikan sebuah solusi dimana pembelajaran digunakan untuk menjelaskan cara algoritma vigenere cipher disamping pengajar memberikan penjelasan tambahan mengenai algoritma vigenere cipher.

**a. Analsisa Penerapan Metode Computer Assisted Instruction**

Pembahasan yang dilakukan pada penelitian ini terdiri dari beberapa bahagian yang sesuai dengan penerapan metode computer assisted instruction, berikut adalah pembahasannya.

1. Pengertian Kriptografi
   Pada bagian ini ditampilkan mengenai pengertian kriptografi yang dimasukkan dalam animasi.
2. Materi
   Pada bagian ini ditampilkan mengenai kriptografi yang dibahas pada penelitian ini yaitu algoritma kriptografi Vigenere Cipher.
3. Model Drill And Practice
   Pada model ini terdapat 2 drill and practice yaitu di setiap topik pembahasan mengenai algoritma vigenere cipher, berikut adalah beberapa contoh soal dari aplikasi yang penulis rancang
   1. Yang manakah termasuk algoritma kriptografi?
      a. Vigenere Cipher
      b. Huffman
      c. LZW
      d. Burrows Wheeler
      e. Deflate
4. Model Simulasi
   Vigenere chiper merupakan salah satu algoritma kriptografi klasik untuk menyandikan suatu plaintext dengan menggunakan teknik substitusi. Vigenere cipher pada dasarnya cukup rumit untuk dipecahkan. Meskipun begitu, Vigenere cipher tetap memiliki kelemahan. Salah satunya adalah dapat diketahui panjang kuncinya dengan menggunakan metode kasiski. Hal ini disebabkan karena umumnya terdapat frasa yang berulang-ulang pada ciphertext yang dihasilkan, sebagai catatan bahwa proses kriptografi klasik berhubungan dengan tabel nilai dibawah ini

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Contoh :
Plainteks = BUDIDARMA
Kunci = YULI
Dikarenakan kunci > Plainteks maka panjang kunci disesuaikan dengan panjang plainteks, maka hasilnya adalah

Plainteks = BUDIDARMA
Kunci = YULIYULIY
Berikut adalah proses enkripsi nya

| Plainteks | B | U | D | I |
|---|---|---|---|---|
| Plainteks ASCII | 1 | 20 | 3 | 8 |
| Kunci | Y | U | L | I |
| Kunci ASCII | 24 | 20 | 11 | 8 |
| Hasil Ciphertext | 25 | 15 | 14 | 16 |
| | Z | P | O | Q |

| Plainteks | D | A | R | M | A |
|---|---|---|---|---|---|
| Plainteks ASCII | 3 | 0 | 17 | 12 | 0 |
| Kunci | Y | U | L | I | Y |
| Kunci ASCII | 24 | 20 | 11 | 8 | 24 |
| Hasil Ciphertext | 2 | 20 | 3 | 20 | 24 |
| | B | U | D | U | Y |

Plainteks = BUDIDARMA
Kunci = YULIYULIY
Cipherteks = ZPOQBUDUY
Pada proses enkripsi jika nilai lebih dari 25 semisal 40, maka nilainya dikurangi 25 sesuai dengan tabel nilai, maka 40 - 25 = 15 maka 15 = P.

## 4. ALGORITMA DAN PEMBAHASAN

Algoritma merupakan suatu susunan logis berupa langkah-langkah atau cara yang sistematis untuk memecahkan suatu masalah atau untuk mencapai suatu tujuan tertentu. Nilai kebenarannya harus dapat ditentukan benar atau salahnya.

1. Algoritma Materi
   Input : Materi
   Proses :
   Tampilan menu pilihan materi, latihan, simulasi, games
   If pilihan = materi then
   Tampilkan halaman materi
   End if
   Output : Materi
2. Algoritma Latihan
   Input : Latihan
   Proses :
   Tampilan menu pilihan materi, latihan, simulasi, games
   If pilihan = latihan then
   Tampilkan halaman latihan
   End if
   Output : Latihan
3. Algoritma Simulasi
   Input : Simulasi
   Proses :
   Tampilan menu pilihan materi, latihan, simulasi, games
   If pilihan = simulasi then
   Tampilkan halaman simulasi
   End if
   Output : simulasi

4. Algoritma Simulasi
   Input : Simulasi
   Proses :
   Tampilan menu pilihan materi, latihan, simulasi, games
   If pilihan = games then
      Tampilkan halaman games
   End if
   Output : Games

## 5 KESIMPULAN

Berdasarkan keterangan di atas penulis dapat menarik kesimpulan sebagai berikut ;

1. Proses pembelajaran kriptografi vigenere cipher, khususnya tentang enkripsi dan dekripsi dapat diterapkan dalam suatu aplikasi pembelajaran.
2. Metode *Computer Assisted Instruction( CAI )* yang diterapkan dalam aplikasi ini untuk mempermudah mahasiswa dalam memahami materi ataupun menyelesaikan soal-soal latihan dari *kriptografi vigenere cipher.*
3. Aplikasi pembelajaran multimedia berhasil dibuat dengan tampilan yang menarik serta visualisasi animasi yang menampilkan contoh visualisasi kriptografi vigenere cipher
4. Terdapatnya soal menjadi nilai tambah tersendiri sehingga pengguna bisa mengasah pengetahuan pengguna

## DAFTAR PUSTAKA

[1] I. K. Sudarsana *et al.*, "Paradigma Pedidikan Bermutu Berbasis Teknologi Pendidikan," *Jayapangus Press Books*, vol. 0, no. 0, Mar. 2018, Accessed: Sep. 12, 2018. [Online]. Available: http://books.jayapanguspress.org/index.php/publisher/article/view/19.

[2] Munir, *Multimedia Konsep & Aplikasi Dalam Pendidikan*, vol. 58, no. 12. Bandung: Penerbit Alfabeta, Bandung, 2012.

[3] R. W. Dahar, "Teori-Teori Belajar," 1989. Accessed: Dec. 12, 2019. [Online]. Available: www.tcpdf.org.

[4] 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.

[5] H. D. Hutahaean and P. M. Hasugian, "Aplikasi Pembelajaran Kriptograpi berbasis Mobile menggunakan Computer Assisted Instruction," vol. 4, no. 1, pp. 2–5, 2019.

[6] R. Wondal, "PENGARUH MEDIA PEMBELAJARAN COMPUTER ASSISTED INSTRUCTION (CAI) TERHADAP HASIL BELAJAR SISWA," 2015.

[7] C. Watkins, E. Carnell, and C. Lodge, *Effective Learning in Classrooms*. 2007.

[8] M. A. Carter and D. Goldie, "Educational media: Potential impacts on tertiary students' mental health," *Int. J. Innov. Creat. Chang.*, vol. 3, no. 3, pp. 61–88, 2017.

[9] R. E. Mayer and R. Moreno, "A Cognitive Theory of Multimedia Learning," *Multimed. Learn.*, no. January 2005, pp. 41–62, 2012, doi: 10.1017/cbo9781139164603.004.

[10] D. Ariyus, "Kriptografi keamanan data dan komunikasi," *Yogyakarta Graha Ilmu*, 2006.

[11] T. Limbong, "Pengujian Kriptografi Klasik Caesar Chipper Menggunakan Matlab," *no. Sept.*, vol. 2017, 2015.

[12] H. Sahara, "Implementasi Pengamanan Pesan Chatting menggunakan Metode Vigenere Cipher dan Cipher Block Chainning," *MEANS (Media Inf. Anal. dan Sist.*, vol. 3, no. 2, pp. 173–178, 2018.

[13] B. Silaban and T. Limbong, "Aplikasi Pembelajaran Pengenalan Kriptografi Algoritma Affine Cipher Dan Vigenere Cipher Menggunakan Metode Computer Assisted Instruction," *Media Inf. Anal. dan Sist.*, vol. 2, no. 2, pp. 14–20, 2017.