Aplikasi Pembelajaran Pengenalan Kriptografi Algoritma Affine Cipher Dan Vigenere Cipher Menggunakan Metode Computer Assisted Instruction

[1)]Batara Silaban
STMIK Budi Darma Medan, Jl. Sisingamangaraja No. 338 Simpang Limun Medan
http://www.stmik-budidarma.ac.id // Email : batarasilaban@gmail.com

[2)]Tonni Limbong
Universitas Katolik Santo Thomas, Jl. Setiabudi No. 479 F Tanjungsari Medan
http://www.ust.ac.id // Email : tonni.budidarma@gmail.com

ABSTRAK
In a special room for smokers, Exhoust Fan is installed to clean the air and keep the room air fresh. Most Exhoust Fan works manually, not set automatically so that it has a constant rotational speed, so the function of the exhaust fan as an air purifier is not optimal. This study aims to apply a fuzzy method as well as to control the speed of the Exhoust Fan. Fuzzy logic will process the carbon monoxide gas which is detected by the MQ-3 sensor then the output decision maker is in the form of the Exhoust Fan rotation speed level which is exactly in accordance with the amount of carbon monoxide read by the MQ3 sensor. fuzzysugeno method can regulate the speed of putan fan based on the amount of carbon monoxide read by the MQ-3 sensor.

Kata Kunci : Computer Assisted Instruction, Pembelajaran, Kriptografi, Affine Cipher, Vigenere Cipher.

PENDAHULUAN

1.1 Latar Belakang Masalah

Aplikasi adalah komponen yang berguna melakukan pengolahan data maupun kegiatan-kegiatan seperti pembuatan data dan pengolahan data. Aplikasi merupakan penggunaan dalam suatu komputer, instruksi atau pernyataan yang disusun sedemikian rupa sehingga komputer dapat memproses *input* menjadi *output*.

Pembelajaran adalah proses interaksi peserta didik dengan pendidik dan sumber belajar pada suatu lingkungan belajar. Pembelajaran menggunakan media sebagai alat penyalur merupakan sebuah media yang mampu memberikan pembelajaran baik dalam gambar mati, audio maupun visualisasi bagi setiap *user*. Sehingga pembelajaran lebih menarik dan tidak membosankan karena di dalam pembelajaran ini akan diberikan beberapa pertanyaan yang akan membuat *user* akan merasa tertantang dengan pertanyaan tersebut.

Kurangnya minat belajar peserta didik dalam bidang kriptografi khususnya bidang *affine cipher* dan *vigenere cipher*, membuat penulis ingin merancang sebuah aplikasi pembelajaran mengenai kriptografi dan khusus di bidang *affine cipher* dan *vigenere cipher* untuk meningkatkan minat belajar peserta didik khusus di bidang kriptografi agar dapat lebih tertarik terhadap kriptografi yang penulis buat ke dalam aplikasi berbasis *android*. *Computer Assisted Instruction* adalah salah satu metode pembelajaran yang digunakan penulis dari banyaknya metode pembelajaran lainnya. *Computer Assisted Instruction* ini mengindikasikan bahwa pembelajaran berbasis komputer merupakan suatu pembelajaran yang dibuat secara terprogram menggunakan bantuan komputer sebagai sarana untuk menyampaikan materi kepada peserta didik.

Berdasarkan latar belakang masalah, maka yang menjadi perumusan masalah adalah:

1. Bagaimana penyusunan dan mengajarkan materi bahan ajar algoritma pembelajaran affine cipher dan vigenere cipher?
2. Bagaimana menerapkan model pembelajaran *Computer Assisted Instruction* pada aplikasi pembelajaran pengenalan *affine cipher* dan *vigenere cipher* dalam kriptografi dan berbasis *android*?
3. Bagaimana merancang aplikasi pembelajaran pengenalan algoritma *affine cipher* dan *vigenere cipher* dalam kriptografi dengan menggunakan model *Computer Assisted Instruction* (CAI) ?

Adapun batasan masalah yang dibahas pada penulisan ini adalah sebagai berikut

1. Aplikasi pembelajaran yang dibangun

untuk membantu staff pengajar mahasiswa/i informatika yang mempelajari kriptografi serta membantu mempermudah mahasiswa/i informatika dalam mempelajari algoritma kriptografi klasik.
2. Membangun aplikasi dengan menggunakan model pembelajaran CAI (*Computer Assisted Instruction*) dimana berisi tentang materi , tutorial, latihan (*drill and practice*) dan permainan (*game*).
3. Dalam perhitungan algoritma, aplikasi pembelajaran menggunakan Tabel ASCII.
4. Aplikasi yang digunakan berbasis *mobile android*.

Adapun tujuan penyusunan penelitian ini dapat di jelaskan sebagai berikut:
1. Merancang perangkat lunak pembelajaran pengenalan algoritma *affine cipher* dan *vigenere cipher*.
2. Menambah pengetahuan dalam pembelajaran pengenalan algoritma *affine cipher* dan *vigenere cipher* dalam memainkan perangkat lunak ini.
3. Meningkatkan kemampuan user dalam proses belajar kriptografi khusus di algoritma *affine cipher* dan *vigenere cipher* pada aplikasi pembelajaran ini.

LANDASAN TEORI

2.1 Kecerdasan Buatan

Kecerdasan buatan berbeda dengan program konvensional. Pemograman konvensional berbasis pada algoritma yang mendefinisikan setiap langkah dalam penyelsaian masalah dengan menggunakan rumus matematika atau prosedur sekuensial untuk menghasilkan solusi. Kecerdasan buata berbasis pada representasi simbol dan manipulasi, dimana sebuah simbol dapat berupa kalimat, kata atau angka yang digunakan untuk mempresentasikan obyek, proses dan hubungannya [1]

2.2 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa yunani: " *cryptos*" yang artinya "*secret*" (rahasia) dan "*graphein*" yang artinya "*writing*" (tulisan). Jadi kriptografi berarti "*secret writing*" (tulisan rahasia) [8]. Ada beberapa defenisi kriptografi yang telah dikemukakan diberbagai literatur antara lain: (Scheneier Bruce, 1996) Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (*Cryptography is the art and science of keeping message secure*).

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi[2]. Kata "seni" didalam definisi diatas berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesan. Cara-cara unik tersebut berbeda-beda pada setiap pelaku kriptografi sehingga setiap cara menulis pesan rahasia, pesan mempunyai nilai estetika tersendiri sehingga kriptografi berkembang menjadi sebuah seni merahasiakan pesan [3].

2.2.1 Algoritma *Affine Cipher*

Sandi Affine merupakan sandi monoalfabetik yang menggunakan teknik substitusi yang menggunakan fungsi linier mP+b untuk enkripsi teks asli P dan m (c – b) untuk dekripsi teks sandi c pada mod 26. Kunci pada affine cipher adalah dua integer yaitu m dan b. Nilai m yang dapat dipakai adalah anggota elemen dari mod 26, yang memiliki invers yaitu memenuhi (a,26) = 1[9].

Enkripsi

Untuk melakukan proses enkripsi, dimana plainteks akan diubah ke cipherteks digunakan rumus sebagai berikut:

$$C=mP + b \pmod n \quad ... (1)$$

dimana :
C : Cipherteks
m : bilangan bulat yang harus relatif prima dengan n (jika tidak relatif prima, maka dekripsi tidak bisa dilakukan)
b : jumlah pergeseran
n : ukuran alfabet (menggunakan alfabetik (26))

Dekripsi

Untuk melakukan proses dekripsi, dimana plainteks akan diubah ke cipherteks digunakan rumus sebagai berikut:

$$P =m(C_1 - b)(\text{mod } n) \quad ... (2)$$

dimana :
P : Plainteks
m : invers dari m
b : jumlah pergeseran
n : ukuran alfabet (menggunakan alfabetik (26))

2.2.2 Algoritma *Vigenere Cipher*

Vigenere cipher merupakan sistem sandi poli-alfabetik yang sederhana. Sistem poli-alfabetik mengenkripsi sekaligus sebuah teks yang terdiri dari beberapa huruf. *Vigenere cipher* menggunakan substitusi dengan fungsi shift seperti pada *Caesar cipher*. Keamanan *Vigenere cipher* itu sendiri tergantung dengan jumlah kunci yang digunakan. [4]

Enkripsi

Enkripsi (penyandian) dengan sandi *Vigenère* juga dapat dituliskan secara matematis, dengan menggunakan penjumlahan dan operasi modulus, yaitu:

$$C_i = (P_i + K)_i \bmod 26 \quad .. (3)$$

Dekripsi

Untuk melakukan proses dekripsi, dimana cipherteks akan diubah ke plainteks digunakan rumus sebagai berikut :

$$P_i = (C_i -- K)_i \bmod 26 \quad .. (4)$$

Keterangan: C_i adalah huruf ke-i pada teks tersandi, P_i adalah huruf ke-i pada teks terang, K_i adalah huruf ke-i pada kata kunci, dan mod adalah operasi modulus (sisa pembagian)[4][5].

2.3 Model Computer Assisted Instruction

Computer Assisted Instruction (CAI) yang artinya komputer digunakan untuk membantu proses pembelajaran dalam menyampaikan materi yang sudah diprogramkan. Di *Computer Assisted Instruction* (CAI) peran guru tidak semuanya dihilangkan dan komputer hanya berperan sebagai pendamping guru dalam menyampaikan materi. Komputer sebagai media untuk menyampaikan materi pembelajaran atau informasi, petunjuk dalam menyelesaikan soal-soal latihan yang juga sekaligus sebagai penilai. *Computer Assisted Instruction* (CAI) mendukung pembelajaran dan pelatihan akan tetapi ia bukanlah penyampai utama materi pelajaran[6]. Format penyajian pesan dan informasi dalam *Computer Assisted Instruction* terdiri atas *tutorial* terprogram, *tutorial* intelijen, *drill and practice* dan simulasi.

Tutorial terprogram adalah seperangkat tayangan baik statis maupun dinamis yang telah terlebih dahulu diprogramkan. Secara berurut, seperangkat kecil informasi ditayangkan yang diikuti dengan pertayaan. Jawaban siswa dianalisis oleh komputer (dibandingkan dengan kemungkinan-kemungkinan jawaban yang telah diprogramkan oleh guru/perancang) dan berdasarkan hasil analisis itu umpan balik yang sesuai.

Tutorial intelijen berbeda dari tutorial terprogram karena jawaban komputer terhadap pertayaan siswa dihasilkan oleh intelegensia artifisial, bukan jawaban-jawaban yang terprogram yang terlebih dahulu disiapkan oleh perancang pelajaran. Dengan demikian, ada dialog dari waktu ke waktu antara siswa dan komputer. Baik siswa maupun komputer dapat bertanya atau memberi jawaban.

Drill and practice digunakan dengan asumsi bahwa suatu konsep, aturan atau kaidah, atau prosedur telah diajarkan kepada siswa. Program ini menuntun siswa dengan serangkaian contoh untuk meningkatkan kemahiran menggunakan keterampilan. Hal terpenting adalah memberikan penguatan secara konstan terhadap jawaban yang benar.

Simulasi pada komputer memberikan kesempatan untuk balajar secara dinamis, interaktif dan perorangan. Dengan simulasi lingkungan pekerjaan yang kompleks dapat ditata hingga menyerupai dunia nyata.

2.3.1 Karakteeristik *Computer Assisted Instruction*

Karakteristik CAI yang efektif itu bervariasi, sesuai dengan kepentingannya dan tergantung pada situasi-situasi pelajaran yang dievaluasi[7]. Adapun karakteristik-karakteristik tersebut antara lain:

1. Sesuai dengan tujuan pembelajaran
   Computer Assisted Instruction (CAI) yang efekti harus sesuai dengan tujuan yang dicapai. CAI yang hanya menampilkan tampilan yang bagus saja tidak efektif bila tidak sesuai dengan tujuan pembelajaran.
2. Disesuaikan dengan karakteristik siswa
   Computer Assisted Instruction (CAI) yang efektif harus sesuai dengan karakteristik siswa, misalnya bila CAI itu akan digunakan untuk siswa SD, maka dalam CAI itu harus menampilkan warna-warni yang cerah, kata-kata yang sederhana dan suara yang dapat menarik perhatian siswa.
3. Mengacu pada prinsip desain pelajaran
   Subuah desain pembelajaran yang baik dapat memotivasi siswa, memberitahu siswa tentang tujuan pembelajaran, menampilkan perintah yang tersusun rapi, mengavaluasi perkembangan secara berkala, menyediakan variasi umpan balik.
4. Menggunakan sumber daya komputer yang baik
   Perancangan *Computer Assisted Instruction* yang efektif harus mengetahui kemampuan dari sistem komputernya untuk mengembangkan pelajaran dan mampuh membuat pelajaran lebih efektif.

2.3.2 Struktur *Computer Assisted Instruction*

Computer Assisted Instruction (CAI) merupakan program pembelajaran dengan memanfaatkan komputer yang memiliki struktur program diantaranya[1]:

1. Desain bentuk (aplikasi perangkat lunak)
2. Isi (perangkat pembelajaran)
3. Pendukung (perangkat lunak) yang dibutuhkan dalam pengoperasian, interaktifitas, kemenarikan dan dukungan perangkat evaluasi untuk mengukur tingkat pemahaman siswa melalui *multiple choisce system*.

Secara keseluruhan, "*Computer Assisted Instruction*" hendaknya memiliki beberapa kriteria diantaranya:

1. Dari sudut pandang pengajar
   Mudah digunakan baik pembuatan maupun pemanfaatan hanya memerlukan pelatihan minimal, memungkinkan pembelajaran dengan cara siswa sendiri. Memungkinkan pengendalian pembelajaran sesuai dengan lingkungan.
2. Dari sudut pandang siswa
   Bahan belajar lebih kaya dibandingkan dengan melalui kelas konvesional. Berjalan pada komputer yang telah tersedia memungkinkan kolabarasi yang memadai mencakup pengembangan materi lanjutan melalui diskusi kelas dan kerja kelompok.

PEMBAHASAN

3.1. Analisa Penyajian Materi Kriptografi

Penyampaian materi kritpografi algoritma *Affine cipher dan Vigenere cipher* terhadap peserta didik di kelas, sering mengalami masalah karana kurangnya pemahaan terhadap materi tersebut. Jika menggunakan teknik yang lama seperti mengajarkan peserta didik secara langsung dengan menggunakan media papan tulis akan sulit bagi peserta didik tersebut untuk dapat memahami apa yang diajarkan oleh pengajar karena setiap peserta didik memiliki karakteristik yang berbeda-beda, misalnya daya tangkap dalam menyerap pelajaran ataupun motivasi belajar peserta didik tersebut. Selain itu, faktor eksternal yang juga dapat mempengaruhi kegiatan pembelajaaran tersebut, misalnya cara pengajar dalam menyampaikan pelajaran ataupun lingkungan yang kurang nyaman untuk belajar.

Dari masalah yang dikemukan di atas maka salah satu solusi untuk menyampaikan materi dengan mudah dan dapat membantu peserta didik mudah serta memahami materi yang disampaikan oleh pengajar yaitu dengan menerapkan model pembelajaran *Computer Assisted Instruction* (CAI). Model pembelajaran ini komputer digunakan untuk membantu proses pembelajaran dalam menyampaikan materi yang sudah diprogramkan. Dalam menerapkan model pembelajaran *Computer Assisted Instruction* dibutukan sebuah aplikasi pembejaran yang digunakan oleh pengajar untuk menyampaikan materi kriptografi Algoritma *Affine Cipher* dan *Vigenere Cipher*.

Aplikasi pembelajaran yang digunakan untuk membantu peserta didik dalam memahami materi tersebut adalah aplikasi yang dirancang atau dibuat dengan aplikasi Adobe Flash CS6 yang nantinya jadikan sebuah aplikasi pembelajaran yang berbasis *android* yang dijalankan menggunakan di *handphone* yang bersistem operasi *android*. Kelebihan dari aplikasi yang dibuat mampu menyampaikan materi kriptografi algoritma *Affine Cipher dan Vigenere Cipher* dengan menerapkan metode pembelajaran *Computer Assisted Instruction.*

3.2. Penerapan Computer Assisted Instruction

3.2.1. Materi

1. Materi 1 : Sekilas Kriptografi
   Pada materi 1 berisi mengenai sekilas tentang kriptografi, dimana pada materi 1 ini berisi tentang sedikit sejarah kriptografi, pengertian kriptografi, serta jenis-jenis kriptografi.

Adapun materi yang yang ditampilkan pada Sekilas Kriptografi ini adalah:

a. Pengertian Kriptografi
   Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi.
b. Tujuan Kriptografi
   Kriptografi memiliki tujuan sebagai berikut :
   1. Kerahasiaan
   2. Integritas Data
   3. Otentikasi
   4. Nir-Penyangkalan

2. Materi 2 : Pengertian Algoritma *Affine* dan *Vigenere Cipher*
   Pada materi 2 berisi mengenai pengertian algoritma affine cipher serta vigenere cipher. Dimana materi 2 ini membahas tentang pengertian masing-masing algoritma dan sedikit sejarah algoritma ini.

Adapun isi pada materi 2 ini berisikan tentang :

a. Pengertian *Affine Cipher*
Sandi *Affine* merupakan sandi monoalfabetik yang menggunakan teknik substitusi yang menggunakan fungsi linier mP_i+b untuk enkripsi teks asli P dan $m = c – b$ untuk dekripsi teks sandi c pada mod 26. Kunci pada affine cipher adalah dua integer yaitu m dan b. Nilai m yang dapat dipakai adalah anggota elemen dari mod 26, yang memiliki invers yaitu memenuhi (a,26) = 1.

b. Pengertian *Vigenere Cipher*
Vigenere cipher merupakan sistem sandi poli-alfabetik yang sederhana. Sistem poli-alfabetik mengenkripsi sekaligus sebuah teks yang terdiri dari beberapa huruf. *Vigenere cipher* menggunakan substitusi dengan fungsi shift seperti pada *Caesar cipher*. Keamanan *Vigenere cipher* itu sendiri tergantung dengan jumlah kunci yang digunakan.
Rumus yang digunakan adalah :
Enkripsi : $C_i = (P_i + K_i) \bmod 26$
Dekripsi : $P_i = (C_i - K_i) \bmod 26$

3.2.2 Tutorial

Pada bagian tutorial akan menampilkan tentang pembahasan algoritma kriptografi *affine cipher* serta *vigenere cipher*, disertai dengan tutorial rumus-rumus dan metode penyelesaian algoritma tersebut serta cara penyelesaian dan proses pengerjaan algoritma tersebut dengan menggunakan rumus dan metode yang sudah ditentukan.

3.2.3 *Drill And Practice*

Di dalam materi ini ada juga *Drill And Practice* atau latihan yang dibuat oleh penulis untuk meningkatkan kreatifitas siswa untuk lebih mengetahui kriptografi serta *affine* dan *vigenere cipher*. Melalui model *drill and practice* akan ditanamkan kebiasaan tertentu dalam bentuk latihan. Dengan latihan yang terus menerus, maka akan tertanam dan kemudian akan menjadi kebiasaan. Selain itu untuk menanamkan kebiasaan, model ini juga dapat menambah kecepatan, ketepatan, kesempurnaan dalam melakukan sesuatu serta dapat pula dipakai sebagai suatu cara mengulangi bahan latihan yang telah disajikan, juga dapat menambah kecepatan, contoh sebagai berikut :

1. Proses mengubah plaintext menjadi ciphertext disebut dengan ?
   a. Secret key
   b. Enkripsi
   c. Dekripsi
   d. Kriptografi
2. Pesan atau data yang dalam bentuk asli dalam istilah kriptografi disebut dengan ?
   a. Kriptografi
   b. Chipertext
   c. Plaintext
   d. Algoritma
3. Berikut yang tidak termasuk dalam algoritma kriptografi klasik ?
   a. Caesar Cipher
   b. Knapsack
   c. Vigenere Cipher
   d. Affine Cipher
4. Affine cipher menggunakan sandi?
   a. monoalfabetik
   b. polialfabetik
   c. triplealfabetik
   d. Semua Salah
5. Vigenere Cipher menggunakan sandi?
   a. monolfabetik
   b. polialfabetik
   c. triplealfabetik
   d. Semua Salah
6. (3+12) mod26 = ?
   a. 3
   b. 12
   c. 11
   d. 15
7. (15+12) mod26= ?
   a. 3
   b. 27
   c. 1
   d. 26
8. Cryptos dalam istilah kriptografi dapat diartikan sebagai ?
   a. Kunci
   b. Rahasia
   c. Data
   d. Seni
9. Graphein dalam istilah kriptografi dapat diartikan sebagai ?
   a. seni
   b. rahasia
   c. tulisan
   d. keamanan
10. Kriptografi adalah suatu kegiatan seni ?
    a. Penyandian data
    b. Perubahan data
    c. Penyisipan data
    d. Pengambilan data

3.2.4 Model *Instructional Game*

Model ini merupakan salah satu bentuk model pembelajaran berbasis komputer yang didesain dan dirancang untuk menjadikan siswa senang dan tidak bosan. *Games* ini bertujuan untuk memotivasi siswa (user) untuk belajar sambil bermain. Didalam aplikasi pembelajaran ini *games* yang akan dirancang adalah berupa *Game* Hitung-

Hitung. Game ini dimainkan dengan cara menghitung dan menyelesaikan soal yang muncul dengan benar. Didalam *game* ini juga terdapat waktu permainan, apabila user/mahasiswa berhasil menyelesaikan soal sebelum waktu yang ditentukan selesai maka akan mendapatkan penilaian.

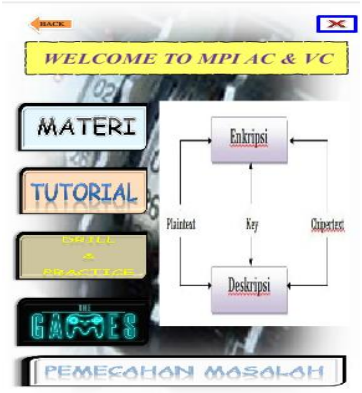
IMPLEMENTASI

Pembelajaran sistem operasi yang telah dirancang menggunakan Adobe Flash CS6, dimana untuk mengetik *listing program* dilakukan pada *action script*. Pada setiap menu akan menuju ke frame-frame yang berhubungan, misalnya untuk menu utama terdapat pada frame 2, dan lain sebagainya.

Pembelajaran sistem operasi yang dirancang menggunakan metode *Computer Assisted Instruction* (CAI), dimana pada metode tersebut berguna agar peserta didik dan masyarakat yang menggunakan aplikasi tersebut dapat melakukan simulasi dari program materi yang diberikan. Aplikasi pembelajaran algoritma affine cipher dan vigenere cipher ini menggunakan model CAI untuk proses belajar, dimana model pembelajaran *Computer Assisted Instruction* berguna bagi para pamakai yang menginginkan cara cepat untuk belajar menyelesaikan algoritma yang ada ke dalam *handphone* dengan sistem operasi android.

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

a. Materi
b. Tutorial
c. Drill and Practice
d. Games
e. Pemecahan Masalah



Gambar 1 Menu Utama

Menu utama ini menampilkan pilihan menu yang ingin dijalankan atau dipergunakan.

Gambar 2 Materi

Pada menu tutorial ini terdapat rumus serta langkah penyelesaian algoritma affine cipher dan vigenere cipher. Menu tutorial dapat dilihat pada gambar dibawah ini.

Gambar 3 Menu Tutorial

Pada menu Drill and Practice ini terdapat soal-soal mengenai kriptografi dan algoritma affine cipher dan vigenere cipher. Menu drill and practice dapat dilihat pada gambar dibawah ini.

Gambar 4 Tampilan Drill and Practice

Pada menu games ini terdapat seperti game hitung-hitung mengenai operasi perhitungan modulus, dengan guna meningkatkan kecepatan peserta didik dalam operasi modulus. Menu games dapat dilihat pada gambar dibawah ini.

Gambar 5 Tampilan Menu Games

KESIMPULAN

Dari kesimpulan ini dapatlah diambil suatu perbandingan yang akhirnya dapat memberikan perbaikan-perbaikan pada masa yang akan datang, Adapun kesimpulan yang penulis peroleh adalah sebagai berikut :

1. Penyusunan serta mengajarkan materi dapat dilakukan dengan menggunakan beberapa proses penjadwalan. Dengan adanya penyusunan materi yang tepat serta proses penjadwalan dan pengorganisasian yang tepat, materi dapat tersampaikan dengan cukup baik.
2. Penerapan model pembelajaran *Computer Assisted Instruction* (CAI) pada aplikasi pembelajaran pengenalan affine cipher dan vigenere cipher dapat membantu para peserta didik dalam penggunaan aplikasi yang berbasis android tersebut.
3. Model *Computer Assisted Instruction* (CAI) diterapkan pada pembelajaran enkripsi dan dekripsi algoritma *affine cipher* dan *vigenere cipher* untuk mempermudah peserta didik dalam memahami pembelajaran enkripsi dan dekripsi algoritma *affine cipher* dan *vigenere cipher* tanpa terbatas oleh waktu dan jarak.

DAFTAR PUSTAKA

[1] 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.

[2] D. Ariyus, *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*. Penerbit Andi.

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

[4] R. Sadikin, “Kriptografi untuk keamanan jaringan,” *Penerbit Andi, Yogyakarta*, 2012.

[5] T. Limbong and P. D. P. Silitonga, “Testing the Classic Caesar Cipher Cryptography using of Matlab,” *Int. J. Eng. Res. Technol.*, vol. 6, no. 2, pp. 175–178, 2017.

[6] 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.

[7] T. Limbong *et al.*, “The implementation of computer based instruction model on Gost Algorithm Cryptography Learning,” in *IOP Conference Series: Materials Science and Engineering*, 2018, vol. 420, no. 1, p. 12094.