APLIKASI PEMBELAJARAN KRIPTOGRAFI HILL CHIPER DENGAN MENGGUNAKAN METODE COMPUTER BASED INSTRUCTION

PENNY SEPTIANI SIANTURI

STMIK Budidarma
Jl. Singsingamangaraja Np.338 Simpang Limun Medan
http : // www.stmik-budidarma.ac.id // Email : vey_cha@ymail.com

ABSTRACT

Application of Information Technology in the current era of globalization is very important. Especially in our developing country, it is in dire need of various information and technology that can be applied to the progress of this nation. But to carry out this task, there are still many obstacles that must be faced both from the cultural conditions, the condition of the country and its human resources. This learning objective serves to facilitate the user in learning the material on Hill Chiper Cryptography and is an alternative in overcoming several problems such as limited time, and several other factors and can reduce the tedious learning atmosphere.

Cryptography Hill Chiper Learning Application by using CBI Method (Computer Based Instruction) is a method developed with computer media, where the teaching method is directly to the user through how to interact in learning topics that have been packaged in a software application.

Keywords: Learning, Cryptography Hill Chiper, Computer Based Instruction

ABSTRAK

Penerapan Teknologi Informasi pada era globalisasi saat ini menjadi sangat penting. Apalagi di Negara kita yang sedang berkembang,sangat membutuhkan berbagai informasi beserta teknologinya yang dapat diterapkan untuk kemajuan bangsa ini. Tapi untuk melaksanakan tugas tersebut,masih banyak kendala yang harus dihadapi baik dari kondisi budaya,kondisi Negara dan sumber daya manusianya. Tujuan pembelajaran ini berfungsi untuk mempermudah user dalam mempelajari materi pada Kriptografi Hill Chiper dan merupakan suatu alternatif dalam mengatasi beberapa masalah seperti waktu yang terbatas,dan beberapa faktor lainnya serta dapat mengurangi suasana belajar yang membosankan.

Aplikasi Pembelajaran Kriptografi Hill Chiper dengan menggunakan Metode CBI (Computer Based Instruction) adalah suatu metode yang dikembangkan dengan media komputer, dimana metode pengajaran secara langsung kepada user melalui cara berinteraksi dalam topic pembelajaran yang telah dikemas dalam suatu aplikasi perangkat lunak.

Kata Kunci : Pembelajaran, Kriptografi *Hill Chiper, Computer Based Instruction*

1. PENDAHULUAN

Pembelajaran merupakan bantuan yang diberikan pendidik agar dapat terjadi proses pemerolehan ilmu dan pengetahuan. Pembelajaran yang tepat akan menentukan seorang peserta didik dapat menyerap ilmu yang diberikan dengan baik. Dan proses pembelajaran selama ini masih cendurung

menggunakan metode manual, yaitu pengajar memberikan ceramah secara teoritas kepada peserta didik, memberikan tugas kemudian memberikan tes akhir, terkadang banyak dari peserta didik tidak menerima pembelajaran secara maksimal dengan cara tersebut, berbagai alasan menjadi penyebabnya diantaranya, kurangnya konsentrasi, suasana yang tidak kondusif dan tidak semua peserta didik yang memiliki daya tangkap yang baik dan cepat, tentu hal ini akan berdampak pada hasil belajar yang kurang maksimal.

Dalam pembelajaran Kriptografi Hill Cipher pada umumnya terdapat berbagai macam kendala yang dialami mahasiswa maupun pengajar, baik dalam segi waktu maupun tempat serta cara penyampaian materi yang konvensional dalam kata lain masih bersifat manual. Dibuatnya aplikasi ini bertujuan untuk menambah minat dan rasa ingin mempelajari lagi Kriptografi Hill Cipher ini secara berulang ulang dimanapun dan kapanpun walaupun tidak adanya seorang pengajar dalam kata lain mahasiswa dapat belajar sendiri walaupun tanpa didampingi pengajar

Sesuai dengan latar belakang pemilihan judul diatas, maka yang akan dibahas pada penelitian ini mencakup:

1. Bagaimana proses pembelajaran Kriptografi *Hill Cipher* dengan menggunakan metode *Computer Based Instruction* (CBI) ?
2. Bagaimana menerapkan metode *Computer Based Instruction* (CBI) dalam Pembelajaran Kriptografi *Hill Cipher* ?
3. Bagaimana merancang aplikasi untuk Pembelajaran Kriptografi Hill Cipher dengan menerapkan metode *Computer Based Instruction* (CBI) ?

Untuk menghindari kesalahpahaman dalam penulisan penelitian ini,dan sesuai judul serta latar belakang masalah yang diuraikan, maka perlu adanya batasan-batasan untuk menyederhanakan permasalahan yang dibahas, yaitu:.

1. Metode yang digunakan dalam perancangan aplikasi ini adalah Metode *Computer Based Instruction* (CBI).
2. Bentuk dan format materi dikemas dalam bentuk teks dan video, hal ini bertujuan untuk mempermudah dan menambah pemahaman mahasiswa dalam mempelajari sebuah materi.
3. Aplikasi yang digunakan dalam pembuatan penelitian ini menggunakan *Macromedia Flash 8*.
4. Pembelajaran dalam aplikasi ini ditujukan kepada mahasiswa semester 7 dan 8.

Berdasarkan perumusan masalah diatas adapun tujuan dari pembuatan penelitian ini adalah :

1. Menjelaskan proses pembelajaran Kriptografi Hill Cipher.
2. Menerapkan metode *Computer Based Instruction* dalam Pembelajaran Kriptografi Hill Cipher.
3. Merancang aplikasi Pembelajaran Kriptografi Hill Cipher dengan metode *Computer Based Instruction*(CBI)

Dengan adanya perancangan dan pembuatan aplikasi pembelajaran Kriptografi Hill Cipher dengan metode *Computer Based Instruction* ini dapat memberikan manfaat yang baik bagi mahasiswa diantaranya :

1. Sebagai media untuk pembelajaran Kriptografi Hill Cipher
2. Memudahkan proses belajar mengajar dalam memberikan materi kepada peserta didik tanpa pengajar,kapan saja dan dimana saja tanpa harus mencatat.
3. Memberikan kemudahan bagi peserta didik untuk mempelajari materi pelajaran serta memudahkan peserta didik untuk mengulang kembali pelajaran Kriptografi Hill Cipher dimanapun dan kapan saja.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptographi (*Cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. "*Crypto*" berarti "*secret*" (rahasia), dan "*Graphy*" berarti "*writing*" (tulisan) (Sasangko,2005). Dalam hal ini kriptografi disebut juga dengan ilmu dan seni,karena sejak jaman dahulu orang-orang mempelajari dan memperdalam sistem pengamanan pesan ini, sehingga menghasilkan berbagai algoritma yang sudah banyak dikenal saat ini (Ariyus,2006).

Didalam kriptografi sering ditemukan berbagai istilah atau teminologi penting yang perlu diketahui seperti beberapa istilah dibawah ini :

1. Pesan, Plainteks dan Cipherteks
   Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan ini adalah plainteks (*plaintext*). Pesan dapat berupa data atau informasi yang dikirim (melalui saluran telekomunikasi atau sejenisnya) atau yang disimpan dalam media perekaman. Pesan tidak hanya berupa teks,tetapi juga berbentuk citra (*image*),suara/bunyi (*audio*)atau berkas biner lainnya. Agar pesan tidak dapat dimengerti oleh pihak lain maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut Cipherteks (*Ciphertext*) atau Kriptogram (*Cryptogram*).
2. Pengirim dan Penerima
   Komunikasi data melibatkan pertukaran pesan antara dua entitas.Pengirim (*sender*) adalah entitas yang mengirim pesan pada entitas lainnya.Penerima (*receiver*) adalah entitas yang menerima pesan. Entitas disini dapat berupa uang,mesin komputer,kartu kredit dan selanjutnya.
3. Enkripsi dan Dekripsi
   Proses menyandikan plainteks menjadi *cipherteks* disebut enkripsi (*Encryption*), sedangkan proses pengembalian *(ciphertext*) chiperteks menjadi plainteks menjadi lebih plainteks, semula dinamakan dekripsi (*Decryption).*
4. *Cipher* dan Kunci
   Dalam kriptografi modern, enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara kedua himpunan tersebut. Yang dlam hal ini algoritmanya tidak lagi dirahasiakan,tetapi kunci harus dijaga kerahasiaannya. Kunci adalah parameter yang digunakan untuk transformasi *enciphering* dan *deciphering*, misalnya P menyatakan plainteks dan C menyatakan Chiperteks, maka fungsi enkripsi E memetakan P ke C, dan dengan menggunakan kunci K, maka fungsi enkripsi dan dekripsi dapat ditulis sebagai berikut :

   $$E_k(P)= C$$

   Dan fungsi dekripsi D memetakan C ke P,

   $$D_k(C)= P$$

   Karena pada proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan asal maka kesamaan berikut benar, $D_k (E_k(P)) = P$
   Keterangan :
   E : Enkripsi
   K : Kunci
   P : Plainteks
   C : Cipherteks
   D : Dekripsi

2.1.1 Kriptografi *Hill Cipher*

Hill Cipher merupakan penerapan aritmatika pada Kriptografi.Teknik Kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang diguanakan untuk melakukan enkripsi dan dekripsi (Sasongko,2005).

Hill Cipher diciptakan oleh Lesier S.Hill pada tahun 1992.Teknik Kriptografi ini

diciptakan dengan maksud untuk dapat menciptakan kode (*Cipher*) yang tidak dapat dipecahkan dengan teknik analisis frekuensi.*Hill Cipher* tidak mengganti setiap abjad yang sama pada *plainteks* dengan abjad lainnya yang sama pada *cipherteks* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya (Sasongko,2005).

2.1.2 Teknik Dasar *Hill Cipher*

Dasar dari teknik *Hill Cipher* adalah aritmatika modul terhadap matriks,dalam penerapannya *Hill Cipher* adalah matriks n x n dengan n merupakan ukuran blok. Matriks K yang menjadi kunci ini harus merupakan matriks yang invertible (yaitu memiliki invers K^{-1} sehingga :

$K.K^{-1} = I$……..(1)

Keterangan :
K : Kunci
K^{-1} : Invers Kunci
I : Matriks Identitas
Kunci harus memiliki invers matriks K yaitu K^{-1} akan dipakai melakukan dekripsi (Sansani,2008)

3. HASIL DAN PEMBAHASAN

3.1 Analisa Masalah

Sebelum merancang aplikasi pembelajaran ini, maka hal pertama yang harus dilakukan adalah melakukan analisis terhadap sistem yang akan dirancang terlebih dahulu.

Teknik Enkripsi Pada *Hill Cipher*

Proses enkripsi pada Hill Cipher dilakukan perblok plainteks. Ukuran blok tersebut sama dengan ukuran matriks kunci, sebelum membagi teks menjadi menjadi deretan blok-blok, plainteks terlebih dahulu dikonversi menjadi angka, masing- masing sehingga A=1, B=2, hingga Y=25 dan Z diberi nilai 0

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

Secara matematis, proses enkripsi pada Hill Cipher adalah :

$$C = K \,.\, P$$

Keterangan :
C = Cipherteks
K = Kunci
P = Plainteks
Contoh soal :
Jika terdapat Plainteks (P) : STRIKE NOW
Maka plainteks tersebut dikonversi menjadi : P = 19 20 18 9 11 5 14 15 23
Plainteks tersebut akan dienkripsi dengan teknik Hill Cipher, dengan kunci yang merupakan matriks 2 x 2

$$K = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}$$

Karena matriks kunci berukuran 2, maka plainteks dibagi menjadi blok yang masing-masing bloknya berukuran 2 karakter. Karena karakter yang terakhir tidak memiliki pasangan, maka diberi karakter yang sama yaitu W. Sehingga plainteks berubah menjadi STRIKENOWW, blok pertama dari plainteks P adalah :

$$P_{1 \times 2} = \begin{pmatrix} 19 \\ 20 \end{pmatrix}$$

Blok plainteks ini kemudian dienkripsi dengan kunci K melalui persamaan

$$C_{1x2} = \begin{pmatrix} 5 \\ 2 \end{pmatrix} \begin{pmatrix} 6 & 19 \\ 3 & 20 \end{pmatrix} = \begin{pmatrix} 215 \\ 98 \end{pmatrix}$$

Hasil perhitungan menghasilkan angka yang tidak berkorespondensi dangan huruf-huruf, maka lakukan modulo (mod) 26 pada hasil tersebut sehingga C_{1x2}menjadi :

$$C_{1x2} = \begin{pmatrix} 215 \\ 98 \end{pmatrix} = \begin{pmatrix} 7 \\ 20 \end{pmatrix} \pmod{26}$$

Karakter yang berkorespondensi dengan 7 dan 20 adalah G dan T. Maka S menjadi G dan T menjadi T. Setelah melakukan enkripsi semua blok pada plainteks P maka dihasilkan cipherteks C sebagai berikut :
P = STRIKENOW
C = 7 20 14 11 4 21 19 11
C = GTNKGKDUSK

Dari cipherteks yang dihasilkan terlihat bahwa Hill Cipher menghasilkan cipherteks yang tidak memiliki pola yang mirip dengan plianteksnya

B. Teknik Depenelitian Pada Hill Cipher
Proses depenelitian pada Hill Cipher pada dasarnya sama dengan proses enkripsinya. Namun matriks kunci harus dibalik (invers) terlebih dahulu, secara matematis proses depenelitian pada Hill Cipher dapat diturunkan dari persamaan (2)
C = K.P
K^1.C = K^1.K.P
K^1.C = I.P

P = K^1.C menjadi persamaan proses dekripsi P = K^1.C
Dengan menggunakan kunci

$$K = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}$$

maka proses depenelitian diawali dengan mencari invers darimatriks K. Mencari invers dapat menggunakan metode operasi baris atau metode determinan [3].
Setelah melakukan perhitungan, didapat matriks K^{-1} yang merupakan invers dari matriks K, yaitu :

$$K^{-1} = \begin{pmatrix} 27 & -24 \\ -18 & 45 \end{pmatrix} = \begin{pmatrix} 1 & 24 \\ 8 & 19 \end{pmatrix} \pmod{26}$$

Cipherteks C = GTNKGKDDUSK, akan didepenelitian dengan menggunakan kunci depenelitian K^{-1} dengan persamaan (3). Proses depenelitian ini dilakukan blok per blokseperti pada proses enkripsi. Pertama ubah huruf – huruf pada cipherteks menjadi urutan numerik.

C = 7 20 14 11 7 11 4 21 19 11
Proses depenelitian dilakukan sebagai berikut :

$P_{1,2} = K^{-1}.C_{1,2}$

$$P_{1,2} = \begin{pmatrix} 1 & 24 \\ 8 & 19 \end{pmatrix} \begin{pmatrix} 7 \\ 20 \end{pmatrix} = \begin{pmatrix} 487 \\ 436 \end{pmatrix} = \begin{pmatrix} 19 \\ 20 \end{pmatrix} \pmod{26}$$

Dan blok kedua :
$P_{3,24} = K^{-1}. C_{3,4}$

$$P_{1,2} = \begin{pmatrix} 1 & 24 \\ 8 & 19 \end{pmatrix} \begin{pmatrix} 7 \\ 20 \end{pmatrix} = \begin{pmatrix} 278 \\ 321 \end{pmatrix} = \begin{pmatrix} 19 \\ 20 \end{pmatrix} \pmod{26}$$

Setelah semua blok selesai didekripsi, maka didapatkan hasil plainteks.
P = 19 20 18 9 11 5 14 15 23
P = STRIKENOW

4. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, maka penulis dapat memberi beberapa kesimpulan sebagai berikut :

1. Pembelajaran Kriptografi *Hill Cipher* dengan menggunakan bantuan komputer ini dibuat untuk memudahkan *user*dalam pemahaman materi Kriptografi *Hill Cipher*.
2. Penerapan metode Computer Based Instruction pada perancangan pembelajaran Kriptografi *Hill Cipher* lebih menekankan pada bentuk penyajian materi (*interface*) aplikasi yang dirancang. Hai ini bertujuan agar peserta didik tertarik untuk mempelajari materi Kriptografi *Hill Cipher* selain itu materi dapat disajikan dengan berbagai model seperti tutorial, simulasi, latihan, dan *games.*
3. Merancang aplikasi pembelajaran Kriptografi *Hill Cipher* dengan menerapkan metode *Computer Based Instruction* merupakan alternatif yang sangat tepat karenadengan metode tersebut diharapkan akan menambah pemahaman dari materi yang disajikan.

5. SARAN

Untuk kepentingan lebih lanjut dari penelitian ini maka penulis memberikan beberapa saran sebagai masukan bagi pembaca :

1. Sebelum mempelajari materi yang ada diKriptografi *Hill Cipher* sebaiknya *user* harus mengetahui apa itu Kriptografi dan apa saja bagian dari kriptografi tersebut
2. User sebaiknya mengetahui apa yang membedakan *Computer Assited Instruction* (CAI) *Computer Based Learning* (CBL) dengan metode *Computer Based Instruction* (CBI).

REFERENSI

[1]. Ariyus “Defenisi Kriptografi”, 2006

[2].Hamdani, Anindita, Septiarini, Fajri Hugraha, “Hill Chiper”, (2009)

[3].Hermida Lumbantoruan “ Jurnal Penelitian Pelita-Informatika Budidarma Volume IV 2 Agustus 2013”

[4].Limbong, T. (2015). Pengujian Kriptografi Klasik Caesar Chipper Menggunakan Matlab. No. September, 2017.

[5]. Limbong, T., & Silitonga, P. D. P. (2017). Testing the Classic Caesar Cipher Cryptography using of Matlab. International Journal of Engineering Research & Technology, 6(2), 175–178. https://doi.org/10.17605/OSF.IO/PEMA5

[6]. Rusman Dr, M.pd “Model-model Pembelajaran”, penerbit PT.Raja Grafindo Persada,Jakarta, 2012.

[7]. Sasongko “Kriptografi Hill Chiper”, 2005

[8].Suryanto,Tabrani “Tampilan Macromedia Flash 8” Penerbit Bintang Indonesia, Jakarta, 2009

[9]. Fauzi Achmad dan Maulita Yani , *Analisis Hybrid Cryptosystem Algoritma Elgamal Dan Algoritma Triple Des*, 2016