Perancangan Aplikasi Pembelajaran Kriptografi Algoritma GOST dengan Menggunakan Metode Computer Based Instruction

Tita Arianti[1], Berto Nadeak[2]

[1,2] STMIK Budi Darma Medan, Jl. Sisingamangaraja No. 338 Simpang Limun Medan, Indonesia

ARTICLE INFORMATION

Received: March 3,2019
Revised: March 19,2019
Available online: April 08,2019

KEYWORDS

Pembelajaran Kriptografi algoritma Gost, Metode Computer Based Instruction

CORRESPONDENCE

Phone: +6282272979119

E-mail: titaarianti14@yahoo.com

A B S T R A K

Media pembelajaran adalah alat bantu yang digunakan dalam hal kegiatan belajar mengajar untuk menyampaikan isi pembelajaran agar pengetahuan, penguasaan dan kemahiran pembentukan sikap dan kepercayaan pada peserta didik, pembelajaran adalah proses untuk membantu peserta didik agar mendapat belajar dengan baik multi media telah mengembangkan proses pengajaran kearah yang dinamis Pembelajaran Kriptografi Algoritma Gost merupakan ilmu yang mempelajar teknik-teknik matematis yang berhubungan dengan keamanan seperti kerahasian data pada saat komunikasi.Prinsip kerja metode komputer based Instruction (CBI) adalah sebuah pembelajaran terpogram yang menggunakan komputer sebagai alat bantu yang mengkomunikaskan materi kepada siswa tujuan penelitian ini, pemrograman pembelajaran memanfaatkan metode Computer Based Instructions (CBI) untuk membantu memahami materi dan mempermudah proses belajar mengajar.

1. PENDAHULUAN

Media pembelajaran adalah alat bantu yang digunakan dalam hal kegiatan belajar mengajar untuk menyampaikan isi pembelajaran agar terjadi pengetahuan, penguasaan kemahiran dan pembentukan sikap dan kepercayaan pada mahasiswa, pembelajaran adalah proses untuk membantu mahasiswa agar mendapat belajar dengan baik, teknologi multimedia mampu memberi kesan yang besar dalam bidang komunikasi dan pendidikan. Multimedia telah mengembangkan proses pengajaran dan pembelajaran kearah yang lebih dinamis[1], [2].

Dalam kriptogrfi banyak ditemukan algoritma-algoritma salah satunya adalah Algoritma Gost. Gost adalah singkatan dari *"Government Standart"* artinya standart pemerintah, Algoritma gost merupakan suatu algoritma Blok chipper. Kriptografi Algoritma Gost ini merupakan kriptografi Modern, berbeda dengan klasik yang umumnya berorientasi pada karakter, penyandian modern berorientasi bit sebab penyandian modern menggunakan media komputer untuk mengolah pesan. pesan pada sandi modern tidak selalu berupa rangkaian karakter bisa saja berupa rangkaian bit seperti video atau berkas gambar.[3], [4]

Computer Based Instruction (CBI) merupakan materi pengajaran disusun secara sistematis dan dirancang dengan bahasa pemrograman ataupun dengan software, sistem komputer menyajikan serangkaian program pengajaran dengan cara berinteraksi dengan sistem komputer, maka kebutuhan akan tersedianya pemrograman pembelajaran yang memanfaatkan pembelajaran Metode *Computer Based Instruction* (CBI) semakin meningkat dan menggunakan metode pembelajaran strategis dengan materi, latihan, pertanyaan, quis. Media pembelajaran yang dikemas dalam program komputer ini bertujuan untuk membantu memahami materi sehingga dapat mempermudah proses belajar mengajar[5].

2. LANDASAN TEORI

2.1 Pembelajaran

Pembelajaran adalah suatu proses atau upaya menciptakan kondisi belajar dalam mengembangkan kemampuan minat bakat siswa secara optimal, sehingga kompetensi dan tujuan pembelajaran dapat tercapai secara optimal, sehingga kompetensi dan tujuan pembelajaran dapat tercapai. Kompetensi dan tujuan pembelajaran tercapai secara optimal apabila pemilihan dan pendekatan, metode, strategi, dan model-model pembelajaran tepat dan disesuaikan dengan materi, tingkat kemampuan siswa, karakteristik siswa, kemampuan sarana dan prasarana dan kemampuan guru dalam menerapkan secara tepat guna pendekatan, metode, srategi dan model-model pembelajaran[6], [7]

2.2. Kriptografi

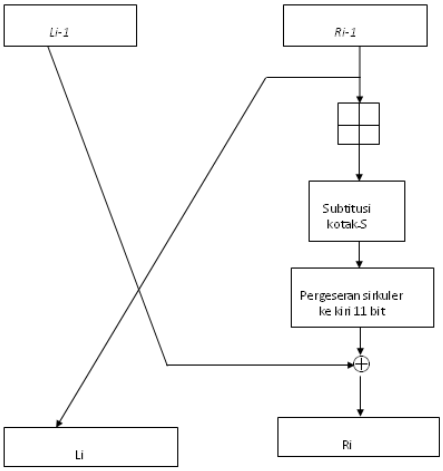
Kriptografi *(cryptography)* berasal dari bahasa yunani: *"criptos"* artinya *"secret"* (rahasia) sedangkan *"graphein"* artinya *"writing"* (tulisan). Jadi kriptografi berarti "secret writing" (tulisan rahasia).ada beberapa defenisi kriptografi yang telah dikemukakan dalam berbagai literatu. Defenisi yang dipakai dalam buku-buku yang lama (sebelum tahun 1980-an)

menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya, kriptografi dugunakan untuk keamanan komunikasi penting, kriptografi juga lebih dari sekedar privacy, tetapi juga untuk tujuan data integrity authentication dan non-repudidation[4], [8].

2.3. Algoritma Gost

Gost atau Gosudartstavany Standart, artinya standarat pemerintah,adalah algoritma enkripsi dan dikembangkan pada tahun 1970 gost dibuat oleh Soviet sebagai alternative terhadap algoritma enkripsi standard Amerika serikat, DES[3], GOST secara structural mirip dengan DES, struktur GOST menggunakan jaringan Fietsel. Satu putaran GOST untuk putaran Ki-1, digunakan kunci internal ki. Satu putaran Gost sama denagan DES diperhatikan pada rumus dibawah ini.

Li = Ri-1…….(1)
Ri = Li-1 f(Ri-1,Ki)……(2)



Gambar 1: Satu Putaran Gost [3]

3. HASIL DAN PEMBAHASAN

3.1 Analisa sistem

Proses pembelajaran merupakan suatu proses yang didalamnya terdapat peserta didik pendidik dan sumber atau belajar pada suatu lingkungan belajar. Aktivitas pembelajaran akan berjalan lancar apabila ketiga aspek tersebut ada.Penyampaipaian materi yang baik dan lebih spesifik merujuk pada tujuan pemebelajaran akan membuat peserta didik merasa tertarik untuk mempelajari materi yang disampaikan oleh pengajar. Selain mengajarkan materi ajar kepada mahasiswa, sebaiknya juga dilakukan tes ujian sesuai dengan materi yang disampaikan untuk mengetahui sebarapa paham mahasiswa mengerti tentang materi yang disampaikan pendidik, sehingga dengan demikian tujuan pembelajaran dapat diukur tercapai atau tidak [9]

3.2. Perancangan Sistem

Setelah melakukan analisa sistem yang berjalan selanjutnya melakukan proses perancangan sistem. Perancangan sistem akan dimulai setelah tahap analisis terhadap sistem yang sedang berjalan selesai dilakukan, perancangan sistem dapat didefinisikan sebagai penggambaran, perencanaan dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah ke dalam satu kesatuan yang utuh dan berfungsi. Langkah pertama yang dilakukan dalam perancangan sistem adalah menggambarkan sistem secara umum yang akan dibangun [10].

3.3. Algoritma GOST

Algoritma GOST merupakan blok kode dari bekat Uni Soviet, yang merupakan singkatan dari Gosudarstvennyi Standard atau standar pemerintah. GOST merupakan blok kode 64 bit dengan panjang kunci 256 bit. Algoritma ini mengiterasi algoritma enkripsi sederhana sebanyak 32 putaran. Untuk mengenkripsi pertama-tama plainteks 64 bit dipecah menjadi 32 bit bagian kiri, L dan 32 bit bagian kanan, R. Subkunci (subkey) untuk putaran i adalah Ki. Pada satu putaran ke-i operasinya adalah sebagai berikut:
Li = R i-1
Ri = L i-1 xor f(R i-1, Ki)

1. Proses Pembangkitan Kunci
Kunci internal pada algoritma GOST dibangkitkan dari kunci eksternal yang diberikan oleh pengguna.

Pembangkitan kunci internal dilakukan dengan membagi kunci eksternal 256 bit (k1, k2, k3, k4, …, k256) ke dalam delapan bagian yang masingmasing panjangnya 32 bit.
Pembagiannya adalah sebagai berikut :
K0 = (k32, ……. ,k1)
K1 = (k64, ……. ,k33)
K2 = (k96, ……. ,k65)
K3 = (k128, ……. ,k97)
K4 = (k160, ……. ,k129)
K5 = (k192, ……. ,k161)
K6 = (k224, ……. ,k193)
K7 = (k256, ……. ,k225)

2. Proses Enkripsi
Proses Enkripsi pada algoritma GOST untuk satu putaran (iterasi), adalah sebagai berikut :

1) 64 bit plainteks dibagi menjadi 2 buah bagian 32 bit, yaitu Li dan Ri. Caranya : Input a1(0), a2(0), ….. ,a32(0) ; b1(0), b2(0), ….. ,b32(0) R0 = a32(0), a31(0), ….. ,a1(0)
   L0 = b32(0), b31(0), ….. ,b1(0)
2) (Ri + Ki) mod 232.
   Hasil dari penjumlahan modulo 232 berupa 32 bit.
3) Hasil dari penjumlahan modulo 232 dibagi menjadi 8 bagian, dimana masing-masing bagian terdiri dari 4 bit. Setiap bagian dimasukkan ke dalam table S-box yang berbeda, 4 bit pertama menjadi input dari SBox 0, 4 bit kedua menjadi S-Box 1 dan seterusnya.

Tabel 1 : S-Box Algoritma GOST

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0x	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3
1x	14	11	4	12	6	13	15	10	2	3	8	1	0	7	5	9
2x	5	8	1	13	10	3	4	2	14	15	12	7	6	0	9	11
3x	7	13	10	1	0	8	9	15	14	4	6	12	11	2	5	3
4x	6	12	7	1	5	15	13	8	4	10	9	14	0	3	11	2
5x	4	11	10	0	7	2	1	13	3	6	8	5	9	12	15	14
6x	13	11	4	1	3	15	5	9	0	10	14	7	6	8	2	12
7x	1	15	13	0	5	7	10	4	9	2	3	14	6	11	8	12

4) Hasil yang didapat dari substitusi ke S-Box kemudian digabungkan kembali menjadi 32 bit dan kemudian dilakukan RLS (Rotate Left Shift) pergeseran ke kiri sebanyak 11 bit.
5) Ri + 1 = RLS XOR Li
6) Li + 1 = Ri sebelum dilakukan proses Langkah nomor 2 sampai 6 dilakukan sebanyak 32 kali (putaran). Pada langkah nomor 2 penggunaan kunci dijadwalkan penggunaannya sesuai dengan putarannya.

Tabel 2 :Penjadwalan Kunci Internal Enkripsi

Putaran	0	1	2	3	4	5	6	7
Kunci Internal	K0	K1	K2	K3	K4	K5	K6	K7
Putaran	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Kunci Internal	K0	K1	K2	K3	K4	K5	K6	K7
Putaran	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**
Kunci Internal	K0	K1	K2	K3	K4	K5	K6	K7
Putaran	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
Kunci Internal	K7	K6	K5	K4	K3	K2	K1	K0

Untuk putaran ke-31, langkah nomor 5 dan 6 sedikit berbeda. Langkah 5 dan 6 untuk putaran 31 adalah sebagai berikut :
R32 = R31 sebelum dilakukan proses
L32 = L31 XOR R31
Sehingga cipherteks yang dihasilkan adalah,
L32 : b(32), b(31), ….. ,b(1)
R32 : a(32), a(31), ….. ,a(1)

Chiperteks = a(1), ….. ,a(32); b(1), ….. ,b(32).

3. Proses Dekripsi

Proses dekripsi merupakan kebalikan dari proses enkripsi. Penggunaan kunci pada masing-masing putaran pada proses dekripsi adalah sebagai berikut:

Tabel 3 :Penjadwalan Kunci Internal Dekripsi

Putaran	0	1	2	3	4	5	6	7
Kunci Internal	K0	K1	K2	K3	K4	K5	K6	K7
Putaran	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Kunci Internal	K7	K6	K5	K4	K3	K2	K1	K0
Putaran	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**
Kunci Internal	K7	K6	K5	K4	K3	K2	K1	K0
Putaran	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
Kunci Internal	K7	K6	K5	K4	K3	K2	K1	K0

Di dalam proses dekripsi terdapat aturan sama dengan proses enkripsi yaitu untuk langkah ke-5 dan ke-6 pada putaran ke-31 sebagai berikut :

R32 = R31

sebelum dilakukan proses

L32 = L31 XOR R31

Sehingga, plainteks yang dihasilkan pada proses dekripsi adalah [4],

L32 : b(32), b(31), ….. ,b(1)

R32 : a(32), a(31), ….. ,a(1)

Plainteks = a(1), ….. ,a(32); b(1), ….. ,b(32).

3.4. Tutorial

Pada menu Tutorial berisi materi-materi atau pengertian dan penjelasan tentang pembelajaran kriptografi yang berguna untuk menjawab soal-soal.

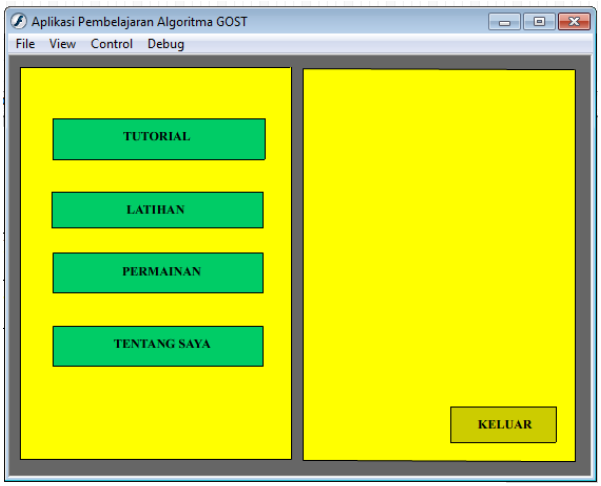
a. Materi Kriptografi
   Kriptografi adalah ilmu yang mempelajari tekni-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data dan, serta otentikasi.
b. Sejarah Data Encryption system
   Pada siketitar tahun 1960, IMB melakukan riset pada bidang kriptografi yang pada akhirnya disebut Lucifer, Lucifer dijual pada tahun 1971 pada sebuah perusahaan di London. Lucifer merupakan algoritma berjenis block chipher yang artinya bahwa input maupun output dari algoritma tersebut merupakan 1 block yang terdiri dari banyak bit seperti 64 bit atau 128 bit.
c. Enkripsi
   Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa pengetahuan khusus. Enkripsi dapat digunakan untuk membuat komunikasi yang aman, terutama untuk memastikan integritas dan autentikasi dari sebuah pesan.
d. Dekripsi
   Dekripsi adalah proses untuk mengubah chiperteks menjadi plainteks atau pesan asli jadi dekripsi merupakan kebalikann dari enkripsi upaya pengelolaan data menjadi suatu yang dapat diutarakan secara jelas dan tepat dengan tujuan agar dapat dimengerti oleh orang yang tidak langsung mengalaminya sendiri.
e. Plainteks
   Plainteks merupakan pesan asli (pesan yang memiliki arti atau makna).
f. Chiperteks
   Chiperteks merupakan pesan yang sudah dikodekan (tidak memiliki arti atau makna):

3.5. Implementasi

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

a. Tutorial
b. Latihan
c. Permainan
d. Tentang saya

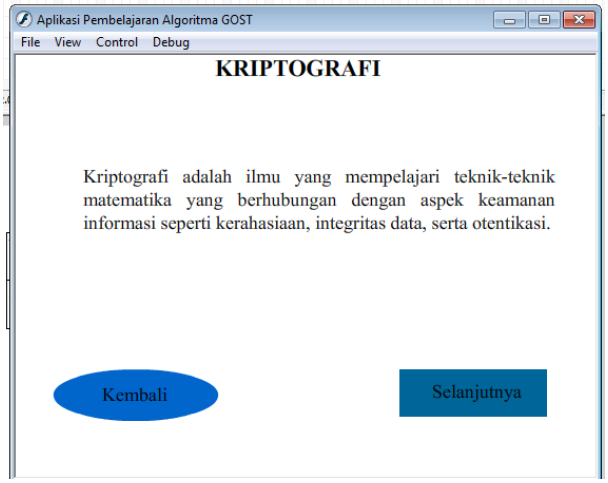
Menu tersebut dapat dilihat pada gambar 1 berikut:



Gambar 1 : Tampilan Menu Utama

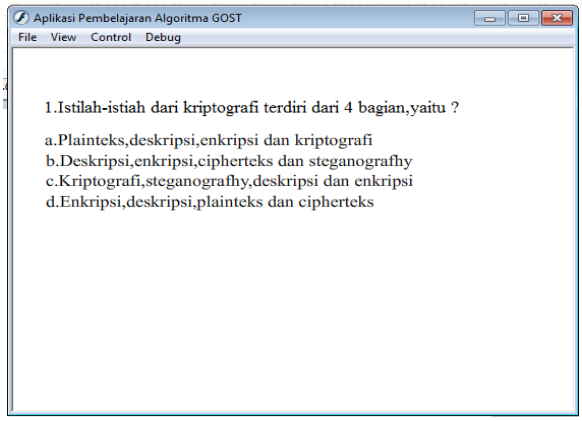
a. Tombol materi untuk memulai materi
b. Tombol latihan untuk memberikan latihan dan menjawab latihan
c. Tombol pernainan untuk memulai games
d. Tombol tentang saya untuk data penulis

Pada menu tutorial ini terdapat materi-materi yang membahas mengenai pemebelajaran kriptografi. Menu tutorial dapat dilihat pada gambar 2 berikut::



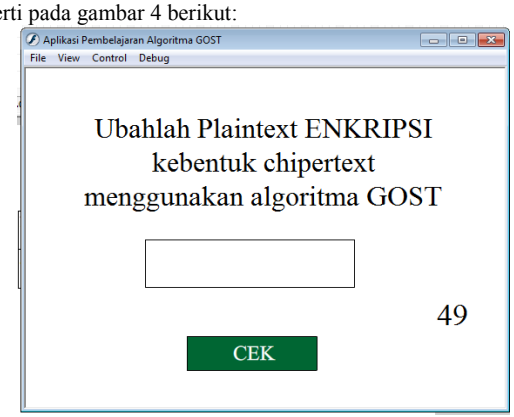
Gambar 2 : Tampilan Halaman Tutorial

Pada menu ini menampilakn butiran-butiran soal yang membahas tentang kriptografi dan algoritma GOST, tampilan menu dapat dilihat pada gambar 3 di bawah ini.



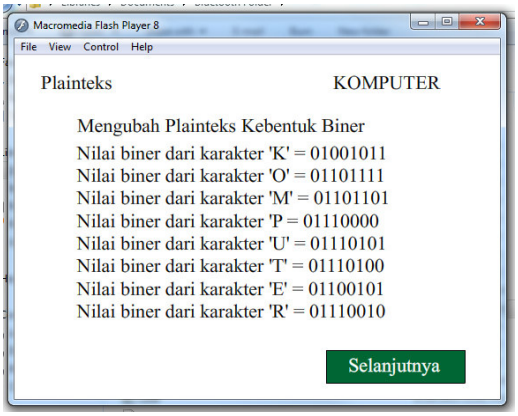
Gambar 3 : Tampilan Halaman Latihan

Pada menu ini hanya terdapat soal-soal latihan mengubah plainteks ke bbentuk chiperteks yang dalam penyelesaiannya diberikan waktu batas waktu seperti pada gambar 4 berikut:



Gambar 4 : Tampilan Halaman Latihan

Pada menu ini hanya terdapat bantuan cara pengerjaan mengubah plainteks ke bbentuk chiperteks yang dalam penyelesaiannya seperti pada gambar 5 berikut:



Gambar 5 : Tampilan Halaman Latihan

4. KESIMPULAN

Sebagai penutup yang pembahasan dalam penelitian, penulis mengambil kesimpulan-kesimpulan sekaligus memberikan saran kepada pembaca yang menggunakan aplikasi pembelajaran kriptografi algoritma gost ini. Dengan adanya kesimpulan dan saran ini dapatlah diambil suatu perbandingan yang akhirnya dapat memberikan perbaikan-perbaikan untuk kedapannya. Adapun kesimpulan yang penulis peroleh sebagai berikut :

1. Dapat merancang suatu aplikasi pembelajaran kripografi algoritma gost dengan teknologi komputer sebagai alat bantu yang digunakan agar mendapat belajar dengan baik dan menghasilkan suatu pembelajaran yang cepat dan jelas.
2. Dalam membuat aplikasi pembelajaran kriptografi algoritma gost menggunakan computerbasedinstruction (CBI).
3. Untuk mengetahui hasil aplikasi yang berisi pembelajaran computer dimana penyajiannya berupa materi-materi pembelajaran kriptografi dengan tampilan menarik serta dapat meningkatkan pemahaman oleh yang menggunakannya.

DAFTAR PUSTAKA

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

[2] 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.

[3] 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.

[4] R. Munir, "Kriptografi," *Inform. Bandung*, 2006.

[5] K. P. Tripathi, "Decision Support System Is a Tool for Making Better Decisions in the Organization,"

Indian J. Comput. Sci. Eng., vol. 2, no. 1, pp. 112–117, 2011.
[6] R. W. Dahar, "Teori-Teori Belajar," 1989.
[7] I. K. Sudarsana *et al.*, "Paradigma Pedidikan Bermutu Berbasis Teknologi Pendidikan," *Jayapangus Press Books*, vol. 0, no. 0, Mar. 2018.
[8] D. Ariyus, "Kriptografi keamanan data dan komunikasi," *Yogyakarta Graha Ilmu*, 2006.
[9] T. Sutabri, *Analisa Sistem Informasi*. Yogyakarta: Andi, 2012.
[10] H. M. Jogiyanto, *Analisis dan Desain (Sistem Informasi Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis)*. Yogyakarta: Penerbit Andi, 2017.