# PERANCANGAN APLIKASI PEMBELAJARAN KRIPTOGRAFI PADA ALGORITMA DATA ENCRYPTION SYSTEM (DES) MENGGUNAKAN METODE COMPUTER ASSISTED INTRUCTION

**RISKA OKTARIA**

STMIK Budidarma
Jl. Sisingamangaraja No. 338 Simpang Limun Medan
www.stmik-budidarma.ac.id // Email : Riskaoktaria3@gmail.com

***ABSTRACT***

*Learning is the process of interaction of students with educators and learning resources in a learning environment. Learning is assistance provided by educators so that an agreed process of knowledge and knowledge can occur, mastery of proficiency and character, and formation of attitudes and beliefs in students. In other words, learning is a process to help students learn well. Cryptography is a study of mathematical techniques related to aspects of information security, such as confidentiality data, validity data, integrity data, and authentication data. All information about information security can be regulated by cryptography. Cryptography can be interpreted as a science or senior for securing messages. Computer Assisted Instruction (CAI) is a system for delivering microprocessor-based subject matter that is designed and programmed into the system. Computer Assisted Instruction (CAI) defines as the use of computers in completing agreed materials with students actively and allows feedback.*

***Keywords: Learning, Cryptography, Computer Assisted Instruction (CAI)***

**ABSTRAK**

Pembelajaran adalah proses interaksi peserta didik dengan pendidik dan sumber belajar pada suatu lingkungan belajar. Pembelajaran merupakan bantuan yang diberikan pendidik agar dapat terjadi proses perolehan ilmu dan pengetahuan, penguasaan kemahiran dan tabiat, serta pembentukan sikap dan kepercayaan pada peserta didik. Dengan kata lain, pembelajaran adalah proses untuk membantu peserta didik agar dapat belajar dengan baik. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan.

Computer Assisted Instruction (CAI) adalah suatu system penyampaian materi pelajaran yang berbasis mikroprosesor yang pelajarannya dirancang dan diprogram kedalam sistemnya tersebut. Computer Assisted Instruction (CAI) didefinisikan sebagai penggunaan komputer dalam menyampaikan bahan pengajaran dengan melibatkan peserta didik secara aktif serta membolehkan umpan balik.

**Kata Kunci : Pembelaajaran, Kriptografi, Computer Assisted Instruction (CAI)**

## 1. PENDAHULUAN

Pembelajaran adalah proses interaksi peserta didik dengan pendidik dan sumber belajar pada suatu lingkungan belajar. Pembelajaran merupakan bantuan yang diberikan pendidik agar dapat terjadi proses perolehan ilmu dan pengetahuan, penguasaan kemahiran dan tabiat, serta pembentukan sikap dan kepercayaan pada peserta didik. Dengan kata lain,

pembelajaran adalah proses untuk membantu peserta didik agar dapat belajar dengan baik.

Disisi lain pembelajaran mempunyai pengertian yang mirip dengan pengajaran, tetapi sebenarnya mempunyai konotasi yang berbeda. Dalam konteks pendidikan, guru mengajar agar peserta didik dapat belajar dan menguasai isi pelajaran hingga mencapai sesuatu objektif yang ditentukan (aspek kognitif), juga dapat memengaruhi perubahan sikap (aspek afektif), serta keterampilan (aspek psikomotor) seorang peserta didik, namun proses pengajaran ini memberi kesan hanya sebagai pekerjaan satu pihak, yaitu pekerjaan pengajar saja. Sedangkan pembelajaran menyiratkan adanya interaksi antara pengajar dengan peserta didik.

Berdasarkan latar belakang pemilihan judul diatas, maka penulis akan mendefinisikan rumusan masalah yang dihadapi yaitu :

1. Bagaimana proses penyampaian pembelajaran kriptografi *Data Encryption System* (DES) kepada peserta pembelajaran?
2. Bagaimana menerapkan metode *Computer Assisted Intruction (*CAI) dalam pembelajaran kriptografi *Data Encryption System* (DES)?
3. Bagaimana merancang aplikasi pembelajaran Kriptografi *Data Encryption System* (DES) dengan menggunakan *Macromedia Flash* ?

Agar pembahasan lebih terarah, maka penulis memberikan batasan-batasan pembahasan masalah yaitu :

1. Materi yang dibahas pada aplikasi pembelajaran yaitu *Data Encryption System* (DES).
2. Metode yang diterapkan pada aplikasi pembelajaran yaitu *Computer Assisted Intruction (*CAI)
3. *Software* yang digunakan untuk merancang aplikasi pembelajaran yaitu *Macromedia Flash.*

Adapun tujuan dari penenlitian ini adalah :

1. Untuk mengetahui proses penyampaian pembelajaran kriptografi *Data Encryption System* (DES) kepada peserta pembelajaran.
2. Untuk menerapkan metode *Computer Assisted Intruction (*CAI) dalam pembelajaran kriptografi *Data Encryption System* (DES).
3. Untuk merancang aplikasi pembelajaran kriptografi *Data Encryption System* (DES) dengan menggunakan *Macromedia Flash.*
4. Untuk menerapkan algoritma *Data Encryption System* (DES) pada aplikasi perancangan pembalajaran kriptografi.

## 2. METODOLOGI PENELITIAN

### 2.1 Pembelajaran

Pembelajaran merupakan terjemahan dari kata *"instruction"* yang dalam bahasa yunani disebut *instructus* atau *intruere* yang berarti menyampaikan fikiran, Menurut Bambang W, (2008:265) arti instruktional adalah menyampaikan pikiran atau ide yang telah diolah secara bermakna melalui pembelajaran.

Ada lima prinsip yang menjadi landasan pengertian pembelajaran yaitu :

1. Pembelajaran sebagai usaha untuk memproleh perubahan prilaku.
2. Hasil pembelajaran ditandai dengan perubahan prilaku secara keseluruhan.
3. Pembelajaran merupakan suatu proses.
4. Proses pembelajaran karena adannya sesuatu yang mendorong dan adanya suatu tujuan yang akan dicapai.
5. Pembelajaran merupakan bentuk pengalaman.

#### 2.1.1 Teori-Teori Pembelajaran

Menurut Bambang W (2008:90) Berdasarkan teori yang mendasarinya yaitu teori psikologi dan teori belajar maka teori pembelajaran ini dapat dibedakan ke dalam lima kelompok yaitu :

1. Pendekatan Modifikasi Tingkah Laku
   Teori pembelajaran ini menganjurkan agar para mahasiswa menerapkan

prinsip penguatan *(reinforcement)* untuk mengidentifkiasi aspek situasi pendidikan yang penting dan mengatur kondisi sedemikian rupa yang memungkinkan peserta didik dapat mencapai tujuan-tujuan pembelajaran. Untuk itu guru sangat penting untuk mengenal karakteristik situasi belajar sehingga dosen mengetahui setiap kemajuan belajar yang di peroleh peserta didik.

1. Teori Pembelajaran *Konstruk Kognitif*

   Teori ini di turunkan dari prinsip atau teori belajar *kognitivisme.* Menurut teori ini prinsip pembelejaran harus di perhatikan perubahan kondisi internal peserta didik yang terjadi selama pengalaman belajar di berikan diruangan. Pengalaman belajar yang diberikan peserta didik harus bersifat penemuan yang memungkinkan peserta didik dapat memperoleh informasi keterampilan.

2. Teori Pembelajaran Berdasarkan Prinsip-Prinsip Pembelajaran.

   Daru berbagai teori belajar yang ada, *Bulgelsky* dan *Snelbaker* (1947) mengidentifikasikan beberapa puluhan prinsip pembelajaran kemudian di padatkan menjadi empat prinsip dasar yang dapat di terapkan oleh para dosen dalam melaksanakan tugas pembelajaran. Ke empat prinsip dasar tersebut adalah

   a. Untuk belajar peserta didik harus mempunyai perhatian dan responsive terhadap materi yang akan di pelajari. Jadi materi pembelajaran harus di atur sedemikian rupa sehingga dapat menarik perhatian dan mudah di pelajari peserta didik.
   b. Semua proses belajar memerlukan waktu, dan untuk suatu waktu tertentu hanya dapat di pelajari sejumlah materi yang sangat terbatas.
   c. Di dalam peserta didik yang sedang belajar selalu terdapat suatu alat pengatur internet yang dapat mengontrol motivasi serta menentukan sejauh mana dan dalam bentuk apa peserta didik bertindak dalam suatu situasi tertentu.
   d. Pengetahuan tentang hasil yang di peroleh di dalam proses belajar merupakan faktor penting sebagai pengontrol.

3. Teori Pembelajaran Berdasarkan Analisis Tugas

   Teori pembelajaran yang diperoleh dari berbagai penelitian di laboratorium dan ini dapat di terapkan dalam situasi kampus, namun hasil penerapannya tidak selalu memuaskan. Oleh karena itu, sangat penting untuk mengadakan analisis tugas (*task analysis*) secara sistematis mengenai tugas-tugas pengalaman belajar yang akan di berikan kepada peserta didik, yang kemudian disusun secara hierarkis dan diurutkan sedemikian rupa tergantung dan tujuan yang ingin dicapai.

4. Teori Pembelajaran Berdasarkan Psikologis Humanitis.

   Teori pembelajaran ini sangat menganggap penting teori pembelajaran dari psikoterapi dari suatu teori belajar. Prinsip harus diterapkan adalah bahwa dosen harus memperhatikan pengalaman emosional dan karateristik khusus peserta didik seperti akualisasi dari peserta didik. Dengan memahami hal ini dapat dibuat pilihan-pilihan kearah mana peserta didik akan berkembang.

### 2.1.2 Pembelajaran Berbantuan Komputer

Program pembelajaran berbantuan komputer ini memanfaatkan seluruh kemampuan komputer, terdiri dari gabungan hampir seluruh media, yaitu teks, grafis, gambar, foto audio, video, dan animasi. Tutorial dalam program pembelajaran dengan berbantuan komputer ditujukan sebagai pengganti manusia yang

proses pembelajarannya diberikan lewat teks atau grafik pada layar yang menyediakan point-point pertanyaan atau permasalahan. Seluruh media tersebut secara *konvergen*, akan saling mendukung dan melebar menjadi satu media yang luar biasa kemampuannya. Salah satu keunggulan komputer ini yang telah dimiliki oleh berbagai media lain, ialah kemampuannya untuk memfasilitasi interaktivitas peserta didik dengan sumber belajar (*content)* yang ada pada komputer (*man and manchine interactivity).*

Menurut Bambang W (2008:137) adapun komputer sebagai sarana komunikasi interaktif juga memiliki beberapa kelemahan. Kelemahan pertama adalah tingginya biaya pengadaan dan pengembangan program komputer, terutama yang dirancang khusus untuk tujuan pembelajaran. Di samping itu, pengadaan, pemeliharaan, dan perawatan komputer yang meliputi perangkat keras (*hardware)* dan perangkat lunak (*software)* memerlukan biaya yang relative tinggi. Oleh karena itu, pertimbangan biaya dan manfaat (*cost benefit analysis*) perlu dilakukan sebelum memutuskan untuk menggunakan komputer sebagai media pembelajaran.

## 2.2 Metode *Computer Assisted Intruction* (CAI)

Pengajaran Berbantuan Komputer atau disingkat dengan CAI (*Computer Assisted Instruction*) adalah suatu sistem pengajaran dan pembelajaran yang menggunakan peralatan komputer sebagai alat bantunya bersama–sama dengan *knowledge base* (dasar pengetahuannya). CAI merupakan pengembangan dari pada teknologi informasi terpadu yaitu komunikasi (interaktif), *audio, video,* penampilan citra (*image*) yang dikemas dengan sebutan teknologi multimedia.

Komunikasi antara siswa dengan komputer dalam *Computer Assisted Instruction* (CAI) meliputi tahap-tahap sebagai berikut :

a. Komputer menyajikan materi pelajaran,
b. Siswa mempelajari materi tersebut,
c. Komputer mengajukan pertanyaan,
d. Siswa memberikan respon,
e. Komputer memeriksa respon tersebut, bila dinilai benar, komputer menyajika materi berikutnya, tetapi jika dinilai salah, komputer memberikan jawaban yang benar beserta penjelasannya.

*Computer Assisted Instruction* (CAI) adalah suatu cara penggunaan komputer secara langsung didalam proses pengajaran sebagai salah satu alternatif pengganti buku-buku dan pendidik.

Ada lima jenis model dalam CAI yaitu:

a. Penjelasan (*Tutorial*)
   Dalam metode ini komputer berperan layaknya sebagai seorang guru. Siswa berpartisipasi secara aktif dalam proses belajarnya dengan berinteraksi melalui komputer. Tutorial memakai teori dan strategi pembelajaran dengan memberikan materi, pertanyaan, contoh, latihan dan kuis agar siswa dapat menyelesaikan suatu masalah, tujuannya adalah membuat siswa memahami suatu konsep atau materi yang baku. Akan tetapi bila sistem ini disertai dengan modul *remedial*, maka bila gagal, siswa akan diberikan remedial terhadap topik yang ia jawab salah saja (tidak mengulang semua).
b. Latihan dan Praktek (*Drill and Practice*)
   Program *Computer Assisted Instruction* (CAI) *drill and practice* adalah metode pengajaran yang dilakukan dengan memberikan latihan yang berulang–ulang, tujuannya yaitu siswa akan lebih terampil, cepat, dan tepat dalam melakukan suatu keterampilan. Program ini berisi rangkaian soal-soal latihan guna meningkatkan keterampilan dan kecepatan berfikir pada materi tertentu.
c. Simulasi
   Merupakan suatu model atau penyederhanaan dari situasi, obyek atau

kejadian sesungguhnya. Program *Computer Assisted Instruction* (CAI) dengan metode simulasi memungkinkan siswa memanipulasi berbagai aspek dari sesuatu yang disimulasikan tanpa harus menanggung resiko yang tidak menyenangkan. Siswa seolah-olah terlibat dan mengalami kejadian sesungguhnya dan umpan balik diberikan sebagai akibat dari keputusan yang diberikannya.

d. Permainan (*Game*)
Materi dari permainan merupakan hal yang ingin diajarkan, sekaligus ia juga berperan sebagai motivator. Pendekatan motivasi, dibedakan antara: motivasi intrinsik yaitu tidak ada *reward* di luar atau tanpa *reward* seperti "*point*" misalnya siswa menyenangi permainan tersebut.

Penggunaan komputer sebagai alat bantu pengajaran atau *Computer Assisted Instruction* (CAI) mempunyai keuntungan antara lain :

1. Mampu mengurangi biaya pelatihan.
2. Fleksibilitas waktu.
3. Fleksibilitas kecepatan pembelajaran.
4. Standarisasi pembelajaran.
5. Efektivitas pembelajaran.
6. Dapat menyimpan data pelajar, pelajaran dan proses pembelajaran yang berlangsung.

## 2.3 Kriptografi

Menurut Ariyus (Pengantar Kriptografi, 2006) kriptografi berasal dari bahasa yunani. Menurut bahasa tersebut kata "kriptografi" dibagi menjadi dua, yaitu *kripto* dan *graphia*. Kripto berarti secret (rahasia) dan Graphio berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat yang lain. Kriptografi adalah seni dan ilmu untuk menjaga keamanan data dengan metode tertentu, dan pelakunya disebut *cryptographer*. Kriptografi disebut sebagai ilmu karena di dalamnya terdapat metode (rumusan) yang digunakan, dan dikatakan, sebagai seni karena dalam membuat satu teknik kriptografi itu sendiri merupakan salah satu ciri tersendiri dari sipembuat memerlukan teknik khusus dalam mendesainnya. Sedangkan *cryptanalysis* adalah suatu ilmu dan seni memecahkan *ciphertext* menjadi *plaintext* tanpa melalui cara yang seharusnya dan orang yang melakukannya disebut *cryptanalyst.*

Kriptografi juga dapat disebut dengan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, kebebasan data, serta autentikasi data. Sebuah pesan rahasia yang harus terjaga keamanannya, salah satu cara dengan penyandian pesan yang bertujuan meyakinkan privasi dengan menyembunyikan informasi dari orang-orang yang ditunjuk informasi tersebut kepadanya.

Menurut Kessel (2006), adapun tujuan sistem kriptografi adalah sebagai berikut :

a. *Authentication*
Proses penguji identitas seseorang.
b. *Privacy/Confidentiality*
Memastikan bahwa tidak ada yang dapat membaca pesan kecuali penerima yang dituju.
c. *Integrity*
Memastikan penerima yang menerima pesan tidak diubah dengan cara apapun.
d. *Non-repudation*
Mekanisme yang membuktikan bahwa pengirim benar-benar mengirim pesan tersebut.

Menurut Flourensia Sapty Rahayu (2005) kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptoanalis *(cryptoanalysis)*, yaitu ilmu dan seni dipelajari untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan untuk memecahkan mekanisme kriptografi dengan cara mendapatkan *plaintext* atau kunci

*ciphertext* yang digunakan untuk menipu penerima yang sesungguhnya, memecahkan *ciphertext.*

Secara sederhana adalah seorang yang ingin menebus kerahasian dari sebuah kode dengan cara membangun algoritma baru yang bisa memecahkan algoritma yang sudah ada, pelakunya disebut kriptonalis. "Rinaldi Munir (kriptografi, 2004) mengatakan jika seorang kriptografer menstransformasi *plaintext* dan *ciphertext* dengan suatu algoritma dan kunci maka sebaliknya seorang kriptonalis berusaha memecahkan *ciphertext* untuk menemukan *plaintext* atau kunci".

Setiap detiknya dalam dunia internet terjadi banyak sekali pertukaran informasi dan banyak pula pencurian informasi oleh pihak-pihak yang bertanggung jawab.

Ada beberapa ancaman keamanan yang terjadi terhadap informasi di antaranya :

1. *Interruption* adalah ancaman terhadap *avaibabiity* informasi, yaitu data yang ada dalam komputer di rusak atau dihapus sehingga dapat informasi tersebut tidak dibutuhkan lagi.
2. *Interception* adalah ancaman terhadap kerahasiaan. Informasi yang disadap oleh orang yang tidak berhak mendapat akses ke komputer dimana informasi di simpan.
3. *Modification* adalah ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan dirubah sesuai keinginan orang tersebut.
4. Menurut Ariyus (2006) *Fabrication* adalah ancaman terhadap integritas. Orang yang tidak berhak menirukan ataau memalsukan informasi yang ada sehingga si penerima informasi mengira telah mendapatkan informasi dari pengirim sebenarnya. Jadi, dari sini dapat diketahui kriptografi diciptakan dengan tujuan, kerahasiaan, yaitu menjamin bahwa pesan dalam keadaan dari pihak yang tidak berhak, integritas data, yaitu menjamin bahwa pesan masih asli atau tidak di manipulasi, autentikasi, yaitu mengidenfikasi pesan dan mengirim pesan, dan *non-repudation* yaitu mencegah penyangkalan pihak yang berkomunikasi.

## 2.4 Algoritma Kriptografi

Algoritma adalah urutan langkah-langkah logis untuk penyelesaian masalah yang disusun secara sistematis, jadi algoritma kriptografi atau sering disebut dengan cipher merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut.

Menurut Ariyus (2006) Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu :

1. *Enkripsi*, merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirim agar terjaga kerahasiaannya. Pesan asli disebut palainteks yang diubah menjadi kode-kode yang tidak dimengerti. *Enkripsi* bisa diartikan sebagai *cipher* atau kode.
2. *Deskripsi*, merupakan kebalikan dari *enkripsi.* Pesan yang telah di enkripsi dikembalikan ke bentuk aslinya. Algoritma yang digunakan berbeda dengan algoritma yang digunakan untuk *enkripsi.*
3. Kunci, merupakan kunci yang digunakan untuk proses *enkripsi* dan *deskripsi.* Kunci terbagi menjadi dua bagian yaitu kunci rahasia *(private key)* dan kunci umum *(public key).*

## 2.5 Algoritma *Data Encryption System* (DES)

Berbeda dengan penyandian 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

rangkain karakter bisa saja berupa rangkaian bit seperti berkas video atau berkas gambar.

Bab ini membahas prinsip dasar penyandian modern yang menggunakan kunci simetri dan salah satu standar penyandian dengan kunci simetri yaitu *Data Encryption System* (DES). Meskipun DES bisa dianggap sistem penyandian yang sudah tua dibanding sistem penyandian kunci simetriyang lebih baru namun DES masih banyak dipakai pada sistem keamanan jaringan. Selain itu, DES dapat dijadikancontoh kasus yang sederhana untuk mempelajari prinsip-prinsip penyandian modern dengan kunci simetri.

Terdapat dua jenis operasi sandi modern yaitu, sandi *stream* yang beroperasi pada data *stream* sehingga operasi penyandian dilakukan per satu bit atau per satu *byte* pada satu waktu. Jenis kedua adalah sandi blok biasa mengolah teks asli sebagai satu kesatuan (dengan ukuran tertentu) dan menghasilkan teks sandi dengan ukuran yang sama. Baik sandi blok atau sandi *stream* mempunyai wilayah aplikasinya sendiri-sendiri. Sandi blok dengan kunci simetri memiliki dua algoritma yaitu enkripsi dan dekripsi seperti yang diilustrasikan Gambar 2.5.3 masukan untuk enkripsi disebut dengan teks asli memiliki panjang bit *n* (ukuran blok adalah *n*) dan sebuah kunci rahasia yang memiliki panjang *k* bit. Sedangkan keluaran algoritma enkripsi adalah sebuah teks sandi yang memiliki panjang *n* bits. Algoritma dekripsi melakukan hal kebalikan algoritma enkripsi yaitu mengubah teks sandi menjadi teks asli. Apabila kunci *k* bit yang dipakai algoritma enkripsi, maka algoritma dekripsi akan menghasilkan teks asli yang sama., 2012

### 2.5.1 Komponen Sandi Blok Modern

Sistem sandi blok modern dalam melakukan enkripsi maupun dekripsi menggunakan beberapa komponen dasar dan operasi-operasi yang bekerja pada level-bit. Komponen sandi blok modern dapat dibagi menjadi 2 jenis yaitu, boks permutasi dan boks subsitusi. Keduanya dipakai sebagai komponen dasar standar DES.

1.Komponen Boks Permutasi

Komponen boks permutasi memiliki satu masukan berukuran *n* bin dan satu keluaran berukuran *m* bit. Cara kerja komponen permutasi adalah mengubah posisi bit masukan pada blok keluaran (mirip dengan transposisi di sandi klasik). Komponen permutasi tidak memerlukan kunci karena bersifat sudah ditentukan. Cara kerja boks permutasi adalah memindah bit berposisi ke-*i* pada masukan menjadi bit berposisi ke-*j* pada keluaran sesuai dengan permutasi yang digunakan.

Boks permutasi dapat direpresentasikan dalam bentuk fungsi sebagai berikut :

$P(\alpha 1\ \alpha 2 \ldots \alpha n) = \alpha\pi(1)\ \alpha\pi(2) \ldots \alpha\pi(n))$

2. Komponen Boks Subtitusi

Komponen kedua yang dipakai pada sandi blok dengan kunci simetri adalah boks subtitusi. Cara kerja boks subtitusi adalah mengganti nilai masukan menjadi nilai lain dengan menggunakan fungsi pemetaan tertentu. Boks subtitusi disebut linier bila dapat direpresentasikan sebagai sebuah fungsi linier terhadap masukan. Misalnya masukan *x*dengan panjang bit *n* direpresentasikan sebagai *x*1, *x*2, . . . *x*n dan keluaran boks subsitusi adalah *y* memiliki panjang bit *m*, maka boks subtitusi linier dapat direprentasikan sebagai sehimpunan fungsi linier.

Contoh Soal : Misal masukan untuk boks substitusi S0 dan S1 adalah (1010) apakah nilai keluarannya?

Jawab :

Indeks baris adalah *x*1 *x*4 yaitu (10) atau 2 dalam desimal, sedangkan indeks kolom adalah *x*2 *x*3 yaitu (01) atau 1 dalam desimal. Berdasarkan tabel 2.8, nilai keluaran untuk boks substitusi S0 adalah 2 atau biner (10) dan untuk boks subsitusi S1 adalah 0 atau biner (00).

## 3. HASIL DAN PEMBAHASAN

### 3.1 Penerapan Metode *Computer Assisted Instruction*

Keberadaan Aplikasi pembelajaran *Computer Assisted Instruction* (CAI) mampu memberikan balikan *(feedback)* sehingga *user* dapat aktif berinteraksi dengan media yang dirancang. Selain itu, metode *Computer Assisted Instruction* (CAI) memiliki beberapa bentuk interaksi yang dapat diaplikasikan seperti: Tutorial, Praktek dan latihan *(drill & practice)*, Simulasi, dan Permainan *(game).*

1. 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 teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi.
   b. Sejarah Data Encryption System
      Pada sekitar tahun 1960, IBM 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 cipher yang artinya bahwa input maupun output dari algoritma tersebut merupakan 1 blok 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 bantuan pengetahuan khusus. Enkripsi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi yang aman, terutama untuk memastikan integritas dan autentikasi dari sebuah pesan.
   d. Dekripsi
      Dekripsi adalah proses untuk mengubah cipherteks menjadi plainteks atau pesan asli. Jd dekripsi merupakan kebalikan dari enkripsi upaya pengolahan data menjadi sesuatu yang dapat di utarakan secara jelas dan tepat dengan tujuan agar dapat dimengerti oleh orang yang tidak langsung mengalaminya sendiri.
   e. Plainteks
      Plainteks yaitu pesan asli (pesan yang memiliki arti atau makna).
   f. Cipherteks
      Cipherteks yaitu pesan yang sudah dikodekan (tidak memiliki arti atau makna).
2. Praktek dan Latihan
   Di dalam materi ini ada juga *drill and practice* atau latihan yang dibuat oleh penulis untuk meningkatkan kreaktifitas mahasiswa untuk lebih mengetahui tentang kriptografi. 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 di pakai sebagai suatu cara mengulangi bahan latihan yang telah disajikan, juga dapat menambah kecepatan, contoh sebagai berikut :
   1. Istilah-istiah dari kriptografi terdiri dari 4 bagian,yaitu?
      a. Plainteks,deskripsi,enkripsi dan kriptografi
      b. Deskripsi,enkripsi,cipherteks dan steganografhy
      c. Kriptografi,steganografhy,deskripsi dan enkripsi

d. Enkripsi,deskripsi,plainteks dan cipherteks

2. Layanan yang ditunjukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak – pihak yang tidak berhak. Berikut ini merupakan pengertian dari…
   a. Kerahasiaan
   b. Integritas data
   c. Otentikasi
   d. Nirpenyangkalan
3. Input dari encryption disebut…..
   a. Plainteks
   b. Chiperteks
   c. Decryption
   d. Salah semua
4. Dibawah ini yang merupakan pengertian Enkripsi adalah….
   a. Proses pengubahan dari plainteks ke cipherteks
   b. Semua data yang belum diproses melalui suatu algoritma kriptografi, plainteks dapat berupa teks, *image* atau bentuk lain.
   c. Informasi hanya dapat diakses oleh yang berhak
   d. Layanan yang menjamin bahwa pesan masih asli\utuh atau belum tentu pernah memanipulasi selama pengiriman.
5. Proses pengubahan dari cipherteks ke plainteks, pernyataan ini merupakan pengertian dari….
   a. Secrecy
   b. Integrity
   c. Deskripsi
   d. Message Digest

3. Simulasi
   Pada bagian ini berisi cara menyelesaikan soal – soal , dimana Aplikasi akan memberikan simulasi dalam bentuk animasi flash yang berbentuk soal – soal pilihan berganda, kemudian user akan memberikan jawaban sebagai feedback.
4. Permainan
   Penulis juga menambahkan game pada materi ini untuk menyediakan suasana yang memberikan fasilitas belajar yang menambah kemampuan mahasiswa, game merupakan lingkungan pelatihan yang baik bagi dunia nyata dalam organisasi yang menuntut pemecahan masalah secara kolaborasi, tidak perlu menirukan realita namun dapat memiliki karakter yang menyediakan tantangan yang menyenangkan bagi mahasiswa. Game menyediakan soal ujian bagi mahasiswa, tes terdiri dari 5 soal pilihan berganda dimana dalam penyelesaian diberi batas waktu 50 detik.

## 4. IMPLEMENTASI PENELITIAN

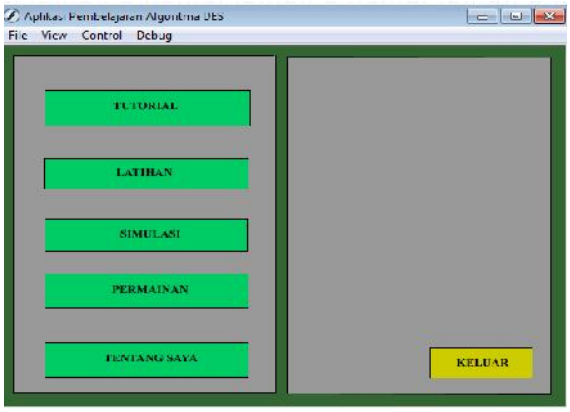
Pembelajaran kriptografi pada algoritma DES yang telah dirancang menggunakan bahasa pemrograman macromedia flash 8, dimana untuk mengetik *listing program* dilakukan pada *action script* yang merupakan perintah *script*.

Pembelajaran kriptografi pada algoritma DES yang dirancang menggunakan metode *Computer Assisted Instruction* (CAI), dimana pada metode ini berguna agar peserta didik yang menggunakan aplikasi pembelajaran ini dapat melakukan simulasi dari program materi yang telah diberikan. Berikut hasil dari implementasi program keseluruhan yang telah dirancang :

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

a. Tutorial
b. Latihan
c. Permainan
d. Tentangsaya

Menu tersebut dapat dilihat pada gambar 1




**Gambar 1 Tampilan Menu Utama**

## 5. KESIMPULAN

Dari pembahasan pada bab sebelumnya penulis dapat membuat beberapa kesimpulan yang merupakan inti sari dari perancangan pembelajaran Kriptograpi Pada Algoritma Data Encryption System dengan metode *Computer Assisted Instruction* (CAI). Merupakan satu faktor yang menentukan apakah aplikasi yang dirancang dapat menjadi suatu acuan atau tidak untuk menyelesaikan permasalahan dalam pembelajaran, dalam hal ini memahami dan menangkap secara langsung pelajaran yang diberikan.

Adapun kesimpulan yang dapat diambil pada pembahasan ini antara lain:

1. Pemanfaatan multimedia dalam proses belajar sangat perlu diterapkan dan dikembangkan, dimana pembelajaran dengan menggunakan gambar, teks dan suara dapat memotivasi keinginan untuk belajar.
2. Perancangan media pembelajaran dengan metode CAI pada pokok pembahasan Algoritma Data Encryption System sangat bermanfaat karena dapat menutupi kekurangan dari media belajar lainnya seperti buku yang tidak dapat bersuara dan tidak atraktif.
3. Dengan bantuan macromedia flash yang merupakan *software*untuk membuat animasi, sangat membantu penulis dalam merancang media pembelajaran.

## 6. SARAN

Adapun saran yang penulis kemukakan sebagai berikut:

1. Diharapkan untuk selanjutnya aplikasi ini dapat dikembangkan menjadi suatu sistem pembelajaran jarak jauh melalui sistem online.
2. Diharapkan agar aplikasi ini ditambahkan bentuk permainan dan animasinya, sehingga terlihat lebih menarik dan variatif.
3. Pembuatan aplikasi ini masih tergolong sederhana, karena penulis sadar untuk membuat media pembelajaran yang baik diperlukan banyak pengalaman.

## REFERENSI

[1]. Bin Ladjamudin, Al-Bahra, “Analisis dan Desain Sistem Informasi”, Penerbit Graha Ilmu, Yogyakarta, 2005.

[2]. Jogianto, H.M, “Analisa dan Desain Sistem”, Penerbit Andi Offset, Yogyakarta, 2005.

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

[4]. 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

[5]. M. Scott pada buku Principle Of Management Information System, Perancangan, 2005.

[6]. Sadikin Rifki, “Kriptografi”, Penerbit Andi, Yogyakarta, 2012

[7]. Warsita, Bambang, “Teknologi Pembelajaran Landasan dan Aplikasinya”, Penerbit Rineka Cipta, Jakarta, 2008.

[8]. Zeembry, “Animasi Macromedia Flash 5”, Penerbit PT Elex Media Komputindo, Jakarta, 2001.

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

[10]. Dony Ariyus Dan Rum Andri K.R (2008). Komunikasi Data. Yogyakarta. Penerbit Andi.

[11]. Fauzi, Achmad, *Analisa Kombinasi Pesan Teks Ke Dalam File Audio Memanfaatkan Algoritma Data Encryption Standard Dan Metode End Of File,*Vol. 3 No. 1, 2019