Karya Ilmiah

PEMBELAJARAN INTERAKTIF DENGAN MENGGUNAKAN WEBSITE

Oleh :

Fahmi Kurniawan, S.Kom., M.Kom.

SEKOLAH TINGGI MANAJEMEN ILMU KOMPUTER
TRIGUNADARMA
MEDAN
2012

BAB I

PENDAHULUAN

1.1. Latar Belakang

Kriptografi klasik merupakan cara penyamaran data atau informasi yang dilakukan oleh orang-orang dulu ketika belum ada komputer dengan tujuan untuk melindungi informasi dengan cara melakukan penyandian. Perlindungan informasi perlu dilakukan untuk mengamankan data yang bersifat rahasia agar tidak dapat diketahui oleh orang lain. Pada era komputer, pengiriman data atau informasi dilakukan menggunakan jaringan komputer dan data atau informasi tersebut disimpan di dalam komputer. Kriptografi juga dilakukan di era komputer tetapi di era komputer kirptografi yang digunakan disebut dengan kriptografi modern. Kritografi modern menggunakan algoritma matematika yang cukup rumit dengan penggunaan kunci. Kriptografi meliputi semua hal mengenai cara menghindari dan menemukan semua penipuan dan semua ketidakjujuran yang terjadi pada suatu pengiriman informasi baik secara manual pada kriptografi klasik ataupun secara matematika pada kriptografi modern. Kriptografi klasik dan kriptografi modern memiliki persamaan yaitu sama-sama melakukan penyandian dengan melakukan transposisi dan subtitusi huruf untuk menghasilkan susunan huruf atau angka yang teracak dan tak bisa terbaca atau dimengerti.

Kriptografi klasik tidak efektif digunakan pada era komputer karena kelemahan dari metode-metode kriptografi klasik telah banyak ditemukan.

Kelemahan-kelemahan Kriptografi klasik terdapat pada algoritmanya yang terlalu sederhana, di samping kerahasiaan algoritmanya tidak terjamin dan mudah terbongkar (Primanio,2006). Oleh karena hal tersebut maka pada penulisan tesis ini penulis akan mencoba menyajikan alternatif atau solusi untuk mengatasi kelemahan metode-metode kriptografi klasik dengan cara mengkombinasikan beberapa metode-metode kriptografi klasik, sehingga kelemahan-kelemahannya dapat saling tertutupi.

Perkembangan bidang teknologi informasi saat ini sangat mempengaruhi kemajuan bidang lainnya. Pendidikan salah satu bidang yang terkena dampak dari cepatnya perkembangan teknologi informasi tersebut. Pendidikan sangat diharapkan mampu mengimbanginya dan mengembangkan melalui ilmu pengetahuan.

Interaktif merupakan salah satu teknik pembelajaran yang sangat efektif untuk menigkatkan minat belajar seorang secara pribadi. Dengan meningkatnya minta belajar seorang siswa maka akan berbanding lurus dengan meningkatnya mutu pembelajaran. Pembelajaran interaktif memerlukan suatu perangkat multimedia yang menampilkan materi pembelajaran dengan cara yang menarik. Dengan menggunakan suatu perangkat seperti, Televisi, Laptop, Handphone, dan perangkat multimedia lainnya, pembelajaran dapat dilakukan secara interaktif.

Internet merupakan salah satu teknologi yang dapat digunakan sebagai satu sarana atau media untuk mewujudkan terciptanya sebuah pembelajaran interaktif. Melalui media Internet semua materi dapat ditampilkan secara lengkap, terstruktur dan dapat dipilih sesuai dengan kebutuhan. Melalui Internet semua materi pembelajaran dapat disajikan secara menarik dan interaktif sehingga menimbulkan

minat belajar yang tinggi. Selain itu dengan adanya pembelajaran interaktif dengan menggunakan media Internet, maka akan menjadi salah satu alternatif dari pemanfaatan dan penggunaan teknologi yang berkualitas dan mendidik. Pada masa sekarang ini masyarakat termasuk para siswa lebih cenderung suka mengakses situs-situs yang hanya bersifat menghibur, atau bahkan situs-situs yang menampilkan hal-hal yang tidak pantas.

Internet telah memberikan akses informasi tanpa mengenal batasan ruang dan waktu. Informasi dapat diakses kapan saja secara global. Pembelajaran berbantuan komputer melalui internet kini merupakan sebuah kebutuhan. Peranan dan implementasinya dalam dunia informasi semakin luas dan mendalam.

1.2. Perumusan Masalah

Berdasarkan latarbelakang di atas, maka permasalahan yang timbul dapat dirumuskan sebagai berikut :

1. Bagaimana merancang suatu pembelajaran interaktif dengan tampilan yang menarik?
2. Bagaimana pembelajaran interaktif dapat diakses melalui perangkat multimedia yang relatif murah dan mudah didapatkan?
3. Bagaimana teknik atau metode pembelajaran yang akan digunakan untuk menyajikan materi pembelajaran?
4. Bagaimana mendesain menu materi pembelajaran agar mudah dimengerti *user*?

5. Bagaimana memodifikasikan metode-metode kriptografi klasik agar dapat mengatasi kelemahan masing-masing metode?

1.3. Batasan Masalah

Agar tidak melebar dari latar belakang dan permasalahan yang telah dijelaskan sebelumnya maka dalam menyelesaikan tulisan ini penulis membuat batasan masalah sebagai berikut :

1. Pembelajaran dibangun dalam bentuk *Website* dengan menggunakan bahasa Pemograman PHP dan MySQL.
2. Interaktif yang dapat lakukan oleh *user* dengan sistem hanya dengan menggunakan fasilitas yang terdapat dalam perangkat multimedia yang digunakan.
3. Materi pembelajaran hanya sebatas memodifikasi metode-metode yang termasuk dalam kriptografi klasik.
4. Materi pembelajaran disajikan dengan metode pembelajaran CAI dengan pendekatan *Tutorial* dan *Drill And Practice (Computer Assisted Instruction)*

1.4. Tujuan

Tujuan yang ingin dicapai dalam penulisan tesis ini sesuai dengan latar belakang dan perumusan masalah diatas yaitu:

1. Untuk merancang suatu pembelajaran interaktif dengan tampilan yang menarik

2. Untuk membangun pembelajaran interaktif dapat diakses melalui perangkat multimedia yang relatif murah dan mudah didapatkan
3. Untuk menerapkan CAI *(Computer Aided Instruction)* sebagai teknik atau metode pembelajaran yang akan digunakan untuk menyajikan materi
4. Untuk mendesain menu materi pembelajaran agar mudah dimengerti *user*
5. Uuntuk memodifikasikan metode-metode kriptografi klasik agar dapat mengatasi kelemahan masing-masing metode

BAB II

URAIAN TEORITIS

2.1 *e-Learning*

Elektronik atau belajar dengan bantuan komputer sudah ada sejak 1970. Dengan menggunakan monitor layar hijau melalui sebuah komputer mainframe berkecepatan rendah, tetapi apakah metode tersebut dapat dikatakan sebagai *e-Learning*. Tentu saja hal tersebut bukan merupakan jawaban yang tepat mengenai *e-Learning*. Tanpa definisi yang jelas mengenai *e-Learning*, sangatlah sulit memutuskan benar atau tidak untuk disebut sebagai *e-Learning*.

2.1.1 Definisi *e-Learning*

Berbagai pendapat dikemukakan untuk dapat mendefinisikan *e-Learning* secara tepat. *e-Learning* sendiri adalah salah satu bentuk dari konsep *Distance Learning*. Bentuk *e-Learning* sendiri cukup luas, sebuah portal yang berisi informasi ilmu pengetahuan sudah dapat dikatakan sebagai situs *e-Learning*. *e-Learning* atau *Internet enabled learning* menggabungkan metode pengajaran dan teknologi sebagai sarana dalam belajar. *e-Learning* adalah proses belajar secara efektif yang dihasilkan dengan cara menggabungkan penyampaian materi secara digital yang terdiri dari dukungan dan layanan dalam belajar (Vaughan Waller, 2001). Definisi lain dari *e-Learning* dapat dijelaskan sebagai proses instruksi yang melibatkan penggunaan peralatan elektronik dalam menciptakan, membantu perkembangan, menyampaikan,

menilai dan memudahkan suatu proses belajar mengajar dengan menjadikan pelajar sebagai pusatnya serta dilakukan secara interaktif kapanpun dan di manapun.

2.1.2. Penyelenggara *e-Learning* yang Potensial

Beberapa instansi yang sangat potensial untuk dijadikan mitra kerjasama dalam pengembangan teknologi ini adalah kalangan akademisi (Universitas, LPK, sekolah umum) dan kalangan industri (misalnya perangkat lunak).

a. Kalangan Akademisi

Terutama perguruan tinggi dikenal sebagai gudangnya ilmu pengetahuan karena di dalamnya berkumpul para staf pengajar yang terlatih, materi pelajaran yang telah terstruktur, perpustakaan dengan buku-buku yang cukup memadai, serta diakui kualitasnya secara resmi melalui akreditasi.

b. Kalangan Industri

Memiliki modal yang cukup besar dan tenaga-tenaga ahli yang terlatih, disamping juga beberapa pengakuan akan kualitas perusahaan yang dapat digunakan sebagai sarana untuk menjaga mutu dari pendidikan yang dilakukan. Beberapa perusahaan besar yang ada di Amerika seperti Cisco System, Hewlet Packard, IBM, Oracle memanfaatkan sistem ini sebagai sarana promosi yang sangat efektif dan murah disamping usaha untuk peningkatan kualitas sumber daya manusia yang menguasai produk yang dihasilkan oleh perusahaan tersebut. Tidak hanya Amerika yang menerapkan sistem ini, beberapa negara Eropa seperti Swedia telah cukup berhasil dengan sistem *e-Learning* ini.

2.1.3. Konsep *e-Learning*

Metode pengajaran tradisional masih kurang efektif jika dibandingkan dengan metode pengajaran modern. Sistem *e-Learning* diharapkan bukan sekedar menggantikan tetapi diharapkan pula untuk dapat menambahkan metode dan materi pengajaran tradisional seperti diskusi dalam kelas, buku, CD-ROM dan pelatihan komputer non internet. Berbagai elemen yang terdapat dalam sistem *e-Learning* adalah :

1. Soal-soal : materi dapat disediakan dalam bentuk modul, adanya soal soal yang disediakan dan hasil pengerjaannya dapat ditampilkan. Hasil tersebut dapat dijadikan sebagai tolok ukur dan pelajar mendapatkan apa yang dibutuhkan.
2. Komunitas : para pelajar dapat mengembangkan komunitas *online* untuk memperoleh dukungan dan berbagi informasi yang saling menguntungkan. Pengajar *online* : para pengajar selalu *online* untuk memberikan arahan kepada para pelajar, menjawab pertanyaan dan membantu dalam diskusi.
3. Kesempatan bekerja sama : Adanya perangkat lunak yang dapat mengatur pertemuan *online* sehingga belajar dapat dilakukan secara bersamaan atau *realtime* tanpa kendala jarak.
4. Multimedia : penggunaan teknologi audio dan video dalam penyampaian materi sehingga menarik minat dalam belajar.

2.1.4. Kelebihan dan Kekurangan *e-Learning*

e-Learning memiliki beberapa kelebihan jika dibandingkan dengan sistem pembelajaran yang lain, namun demikian *e-Learning* juga memiliki kekurangan jika dilihat atau dibandingkan dengan sistem pembelajaran tradisional *(face to face)*. Kelebihan dan kekurangan dari *e-Learning* dapat dijelaskan dalam sub bab berikutnya.

a. Kelebihan *e-Learning*

Dalam bentuk beragam, *e-Learning* menawarkan sejumlah besar keuntungan yang tidak ternilai untuk pengajar dan pelajar.

1. Pengalaman pribadi dalam belajar : pilihan untuk mandiri dalam belajar menjadikan siswa untuk berusaha melangkah maju, memilih sendiri peralatan yang digunakan untuk penyampaian belajar mengajar, mengumpulkan bahanbahan sesuai dengan kebutuhan.
2. Mengurangi biaya : lembaga penyelenggara *e-Learning* dapat mengurangi bahkan menghilangkan biaya perjalanan untuk pelatihan, menghilangkan biaya pembangunan sebuah kelas dan mengurangi waktu yang dihabiskan oleh pelajar untuk pergi ke sekolah.
3. Mudah dicapai: pemakai dapat dengan mudah menggunakan aplikasi *e-Learning* dimanapun juga selama mereka terhubung ke internet. *e-Learning* dapat dicapai oleh para pemakai dan para pelajar tanpa dibatasi oleh jarak, tempat dan waktu.

4. Kemampuan bertanggung jawab : Kenaikan tingkat, pengujian, penilaian, dan pengesahan dapat diikuti secara otomatis sehingga semua peserta (pelajar,pengembang dan pemilik) dapat bertanggung jawab terhadap kewajiban mereka masing- masing di dalam proses belajar mengajar.

b. Kekurangan *e-Learning*

Beberapa kekurangan yang dimiliki oleh pemanfaatan *e-Learning*:

1. Kurangnya interaksi antara pengajar dan pelajar atau bahkan antar pelajar itu sendiri. Kurangnya interaksi ini bisa memperlambat terbentuknya *values* dalam proses belajar mengajar.
2. Kecenderungan mengabaikan aspek akademik atau aspek sosial dan sebaliknya mendorong tumbuhnya aspek bisnis/komersial.
3. Proses belajar mengajar cenderung ke arah pelatihan daripada pendidikan.
4. Berubahnya peran pengajar dari yang semula menguasai teknik pembelajaran konvensional, kini juga dituntut mengetahui teknik pembelajaran yang menggunakan ICT (*Information, Communication and Technology*).
5. Tidak semua tempat tersedia fasilitas internet (mungkin hal ini berkaitan dengan masalah tersedianya listrik, telepon ataupun komputer).
6. Kurangnya mereka yang mengetahui dan memiliki keterampilan tentang internet.
7. Kurangnya penguasaan bahasa komputer.

2.2. Metode CAI *(Computer Assistance Intruction)*

CAI *(Computer Assistance Intruction)* merupakan salah satu dari penerapan ICT terhadap sistem pendidikan, khususnya dalam mempermudah penyelengaraan kegiatan belajar-mengajar. Melalui CAI (*Computer Assisted Instructions*) ini para guru senantiasa dapat memastikan keikutsertaanya dalam melakukan bimbingan terhadap kegiatan belajar siswa baik dirumah atau dikelas dalam konteks pemberian materi pelajaran tingkat lanjut dari pemaparan yang ada dikelas. Para murid yang terkondisikan untuk lebih antusias terhadap materi pembelajaran melalui CAI dapat dengan mudah dan realeks dalam memperdalam maupun melakukan pengulangan pembahasan materi yang ada. Selain hal diatas dengan keberadaan CAI (*Computer Assisted Instructions*) yang dapat dijadikan andalan sebagai asisten pembelajaran dapat diseting dengan konten yang lebih memediasi skill dan kemampuan motorik (penerapan materi pembelajaran) selain pemahaman akan materi pelajaran yang diajarkan, Ada tiga jenis CAI (*Computer Assisted Instructions*) yakni:

1. *Drill and Practice*

   Merupakan cara yang paling mudah, terdiri dari tahap-tahap penampilan permasalahan, penerimaan respon pengguna, pemberian hasil analisis, umpan balik, dan pemberian pertanyaan lain. Secara umum jenis ini tidak menampilkan informasi baru tapi memberikan latihan dari konsep yang sudah ada.

2. *Tutorial*

   Jenis ini berisi konsep atau prosedur yang disertai dengan pertanyaan atau latihan pada akhir dari pelatihan. Selama pelatihan, komputer mengajarkan informasi-

informasi yang baru kepada siswa seperti layaknya seorang guru pembimbing. Setelah itu, pemahaman siswa diukur melalui serangkaian tes dan komputer melanjutkan pengajaran berdasarkan hasil pengukuran tadi.

3. *Socratic*

   Berisi komunikasi antara pengguna dan komputer dalam *natural language*. Jenis ini sebenarnya berasal dari penelitian dalam bidang intelijensia semu (*artificial intelligence*). *Socratic* mampu melakukan interaksi dalam *natural language* dan bisa memahami apa yang ditanyakan pengguna.

2.2.1. Media Pembelajaran

1. Adalah sebuah alat yang mempunyai fungsi menyampaikan pesan.
2. Pembelajaran adalah sebuah proses komunikasi antara pembelajar, pengajar, dan bahan ajar.
3. Media Pembelajaran adalah sebuah alat yang berfungsi untuk menyampaikan pesan pembelajaran.

Adapun kriteria penilaian keefektifan media pembelajaran interaktif (*Thon*, 1995), yaitu Kemudahan navigasi, Kandungan kognisi, Pengetahuan dan presentasi informasi, Integrasi media, Estetika, dan Fungsi secara keseluruhan. CAI (*Computer Assistance Intruction*) adalah semua materi atau aktivitas pembelajaran yang disajikan melalui komputer. Klasifikasi CAI (*Computer Assisted Instructions*) ialah *tutorial*, *drill and practice*, simulasi, dan game intruksional.

2.2.2. Bentuk Interaksi Yang Dapat Diaplikasikan

Bentuk interaksi yang dapat disajikan dalam pembelajaran berbantuan komputer atau CAI (*Computer Assistance Intruction*) adalah sebagai berikut:

1. Praktek dan latihan (*Drill & Practice*)
2. Tutorial
3. Permainan (*Games*)
4. Simulasi (*Simulation*)
5. Penemuan (*Discovery*)
6. Pemecahan Masalah (*Problem Solving*)

2.2.3. Kelebihan Dan Kekurangan CAI (*Computer Assisted Instructions*)

Kelebihan CAI (*Computer Assisted Instructions*) :

1. Meningkatkan interaksi
2. Individualisasi
3. Kelebihan secara administratif dan biaya
4. Motivasi
5. Umpan balik yang bersifat segera dan cepat
6. Mudah menyimpan data
7. Integritas pembelajaran
8. Kendali siswa

Kekurangan CAI (*Computer Assisted Instructions*) :

1. Perangkat keras (*hardware*) yang mahal
2. Kesulitan untuk *mereview* materi
3. Bergantung pada kemampuan membaca dan *visual grafik* yang tidak realistik

4. Butuh keterampilan penegembangan tambahan
5. Waktu pengembangan yang lama
6. Terbatasnya belajar *insidental*
7. Persepsi hanya dari input yang telah terprogram

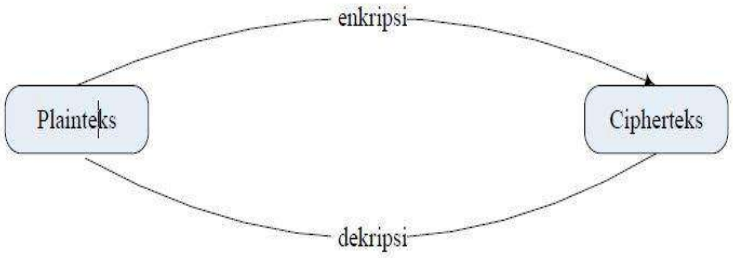
2.3. Kriptografi

Kriptografi saat ini telah menjadi salah satu syarat penting dalam keamanan teknologi informasi terutama dalam pengiriman pesan rahasia. Pengiriman pesan rahasia sangat rentan terhadap serangan yang dilakukan oleh pihak ketiga, seperti penyadapan, pemutusan komunikasi, pengubahan pesan yang dikirim, dan lain-lain. Kriptografi dapat meningkatkan keamanan dalam pengiriman pesan atau komunikasi data dengan cara menyandikan pesan tersebut berdasarkan algoritma dan kunci tertentu yang hanya diketahui oleh pihak-pihak yang berhak atas data/informasi tersebut. Hal ini menyebabkan pihak-pihak yang tidak berhak tidak dapat mengerti isi pesan tersebut.

2.3.1. Pengertian Kriptografi

Kriptografi (*chryptography*) berasal dari dua kata dalam Bahasa Yunani, yaitu "*cryptos*" yang berarti rahasia, dan "*graphein*" yang berarti tulisan. Secara umum, seni dalam menulis dan menyelesaikan sandi rahasia." (Manfredi, 2008) Secara umum, kriptografi terdiri dua proses utama, yaitu enkripsi dan dekripsi. Proses enkripsi akan mengubah pesan asli (plainteks) menjadi pesan terenkripsi dengan menggunakan algoritma dan kunci tertentu yang tidak dapat dibaca secara langsung

(cipherteks). Proses dekripsi merupakan kebalikan dari proses enkripsi, yaitu proses untuk memperoleh kembali plainteks dari cipherteks menggunakan kunci dan algoritma tertentu. Kedua proses tersebut dapat dilihat dari gambar berikut:



Gambar 2.1 Proses-proses kriptografi

2.3.2. Sejarah Kriptografi

Sejarah kriptografi sebagian besar merupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (*transposition cipher*) dan algoritma substitusi (*substitution cipher*). Cipher transposisi mengubah susunan huruf-huruf di dalam pesan, sedangkan cipher substitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain. Sejarah kriptografi klasik mencatat penggunaan cipher transposisi oleh tentara Sparta di Yunani pada permulaan tahun 400 SM. Mereka menggunakan alat yang bernama *Scytale*. *Scytale* terdiri dari sebuah kertas panjang dari daun *papyrus* yang dililitkan pada sebuah silinder dari diameter tertentu (diameter silinder menyatakan kunci penyandian). Pesan ditulis secara horizontal, baris per baris. Bila pita dilepaskan, maka huruf-huruf

di dalamnya telah tersusun secara acak membentuk pesan rahasia. Untuk membaca pesan, penerima pesan harus melilitkan kembali kertas tersebut ke silinder yang diameternya sama dengan diameter silinder pengirim. Sedangkan algoritma subsitusi paling awal dan paling sederhana adalah *Caesar cipher*, yang digunakan oleh raja Yunani kuno, Julius Caesar. Caranya adalah dengan mengganti setiap karakter di dalam alfabet dengan karakter yang terletak pada tiga posisi berikutnya di dalam susunan alfabet.

Di India, kriptografi digunakan oleh pencinta (*lovers*) untuk berkomunikasi tanpa diketahui orang. Bukti ini ditemukan di dalam buku "Kama Sutra" yang merekomendasikan wanita seharusnya mempelajari seni memahani tulisan dengan cipher.

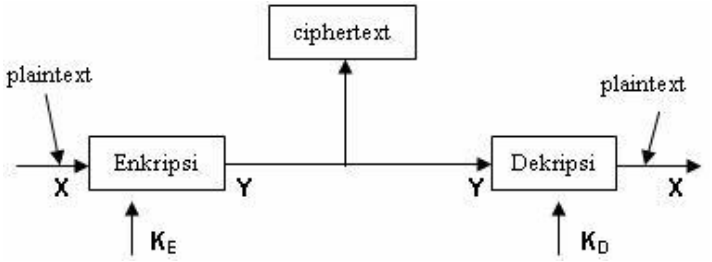
Pada abad ke-17, sejarah kriptografi mencatat korban ketika ratu Skotlandia, Queen Mary, dipancung setelah surat rahasianya dari balik penjara (surat terenkripsi yang isinya rencana membunuh Ratu Elizabeth I) berhasil dipecahkan oleh seorang pemecah kode. Kriptografi umum digunakan di kalangan militer. Pada Perang Dunia ke-2, pemerintah Nazi Jerman membuat mesin enkripsi yang dinamakan *Enigma*. Mesin yang menggunakan beberapa buah *rotor* (roda berputar) ini melakukan enkripsi dengan cara yang sangat rumit. Namun *Enigma cipher* berhasil dipecahkan oleh pihak Sekutu dan keberhasilan memcahkan *Enigma* sering dikatakan sebagai faktor yang memperpendek perang dunia ke-2. Kriptografi modern dipicu oleh perkembangan peralatan komputer digital. Dengan komputer digital, cipher yang lebih kompleks menjadi sangat mungkin untuk dapat dihasilkan. Tidak seperti

kriptografi klasik yang mengenkripsi karakter per karakter (dengan menggunakan alfabet tradisional), kriptografi modern beroperasi pada string biner. (Munir, 2006. hal: 10-12) . Ada banyak sekali algoritma kriptografi yang telah diciptakan hingga saat ini, baik kriptografi klasik maupun kriptografi modern. Namun algoritma kriptografi yang dibahas dalam karya ilmiah ini hanya algoritma *Affine Cipher* karena algoritma tersebutlah yang digunakan untuk menambah lapisan keamanan pada program steganografi yang dibuat oleh penulis.

2.3.3. Metoda Kriptografi Klasik

Kriptografi klasik yang pada dasarnya adalah melakukan substitusi *cipher* abjad majemuk (*polyalphabetic substitution*), yaitu mengubah plaintext dengan kunci tertentu biasanya berupa sebuah kata atau kalimat yang berulang sepanjang plaintext sehingga didapatkan *ciphertext*.

Algoritma Kriptografi dari setiap kriptografi klasik selalu terdiri dari dua bagian yaitu enkripsi dan dekripsi. Secara sederhana proses kriptografi dapat digambarkan sebagai berikut :



Gambar. 2.2. Kriptografi Secara Umum

Operasi enkripsi dan dekripsi dijelaskan secara umum sebagai berikut :

$$Y = E_{KE}\ (X) \quad \text{(enkripsi) (1)}$$

$$X = D_{KD}\ (Y) \quad \text{(dekripsi) (2)}$$

keterangan:

X = *plaintext*, Y = chipertext, KE = key enkripsi, KD = key dekripsi

Ada dua teknik yang paling dasar pada kriptografi klasik. yaitu adalah Transposisi dan Subsitusi :

1. Transposisi adalah mengubah susunan huruf pada *plaintext* sehingga urutannya berubah. Contoh yang paling sederhana adalah mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik.

   Plaintext : SAYA KULIAH DI UPI PADANG
   CipherText : AYAS HAILUK ID IPU GNADAP

2. Substitusi adalah setiap huruf pada *plaintext* akan digantikan dengan huruf lain berdasarkan suatu cara atau rumus tertentu, ada dua macam substitusi yaitu *polyalphabetic substitution cipher* dan *monoalphabetic substitution cipher.* Pada *polyalphabetic substitution cipher ,* enkripsi terhadap satu huruf yang sama bisa menghasilkan huruf yang berbeda sehingga lebih sulit menemukan pola enkripsinya. Pada *monoalphabetic substitution cipher* maka satu huruf tertentu pasti akan berubah menjadi huruf tertentu yang lain, sehingga pola enkripsinya lebih mudah diketahui, karena satu huruf pada *ciphertext* pasti merepresentasikan satu huruf pada *plaintext*.

Kriptografi kalsik terdiri dari beberapa metode-metode yang menggunakan kedua teknik dasar tersebut yang tidak rumit, metode-metode tersebut antara lain:

a. Caesar Cipher

Algoritma kriptografi yang mula-mula digunakan oleh kaisar Romawi, Julius Caesar (sehingga dinamakan juga *caesar cipher*), untuk menyandikan pesan yang dikirim kepada para gubernurnya. Berikut langkah-langkah pencariaan enkripsi dan deskripsi pada *caesar cipher*:

1. Dimulai dengan melakukan penggantian (substitusi) setiap karakter dengan karakter lain dalam susunan abjad(alfabet).
2. Misalnya, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan abjad. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu $k = 3$).
3. Karena hanya ada 26 huruf abjad, maka pergeseran huruf yang mungkin dilakukan adalah dari 0 sampai 25. Secara umum, untuk pergeseran huruf sejauh k (dalam hal ini k adalah kunci enkripsi dan deksripsi), fungsi enkripsi dan dekripsi adalah:

$$ci = E(pi) = (pi + k) \bmod 26 \quad (1)$$

$$pi = D(ci) = (ci - k) \bmod 26 \quad (2)$$

Tabel 1. Pergeseran Huruf Pada Kriptografi Caesar

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

Contoh :

Plaintext : S E L A M A T P A G I

Kunci : 3

Berdasarkan rumus di atas maka dapat hasilkan ciphertext sebagai berikut:

Untuk S:

$ci = E(pi) = (pi + k) \bmod 26$

$= (18 + 3) \bmod 26$

$= 21 \bmod 26 = 21$ (V)

Untuk E :

$ci = E(pi) = (pi + k) \bmod 26$

$= (4 + 3) \bmod 26$

$= 7 \bmod 26 = 7$ (H)

Untuk L :

$ci = E(pi) = (pi + k) \bmod 26$

$= (11 + 3) \bmod 26$

$= 14 \bmod 26 = 14$ (O)

Untuk A :

$ci = E(pi) = (0 + k) \bmod 26$

$= (0 + 3) \bmod 26$

$= 3 \bmod 26 = 3$ (D)

Untuk M :

$ci = E(pi) = (pi + k) \bmod 26$

$= (12 + 3) \bmod 26$

$= 15 \bmod 26 = 15$ (P)

Untuk A :

$ci = E(pi) = (0 + k) \bmod 26$

$= (0 + 3) \bmod 26$

$= 3 \bmod 26 = 3$ (D)

Untuk T :

Untuk P :

$ci = E(pi) = (pi + k) \bmod 26$

$= (19 + 3) \bmod 26$

$= 22 \bmod 26 = 7$ (W)

$ci = E(pi) = (pi + k) \bmod 26$

$= (15 + 3) \bmod 26$

$= 18 \bmod 26 = 10$ (S)

Untuk A :

$ci = E(pi) = (0 + k) \bmod 26$

$= (0 + 3) \bmod 26$

$= 3 \bmod 26 = 3$ (D)

Untuk G :

$ci = E(pi) = (pi + k) \bmod 26$

$= (6+3) \bmod 26$

$= 9 \bmod 26 = 9$ (J)

Untuk I :

$ci = E(pi) = (pi + k) \bmod 26$

$= (8 + 3) \bmod 26$

$= 11 \bmod 26 = 11$ (L)

Berikut cipher yang dihasilkan: "V H O D P D W S D J L"

b. Vigenere Cipher

Vigenere Cipher ditemukan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16. Pada kriptografi caesar pergeseran akan sama pada seluruh pesan, Jika kunci yang digunakan adalah huruf E, maka setiap huruf pada pesan akan bergeser 4 huruf. Begitu juga bila digunakan kunci-kunci lainnya, pada kriptografi Vigenere, *plaintext* akan dienkripsi dengan pergeseran huruf seperti pada kriptografi Caesar tetapi setiap huruf di dalam *plaintext* akan mengalami pergeseran yang berbeda.

Kunci pada kriptografi Vigenere adalah sebuah kata bukan sebuah huruf. Kata kunci ini akan dibuat berulang sepanjang *plaintext*, sehingga jumlah huruf pada kunci akan sama dengan jumlah huruf pada *plaintext*. Pergeseran setiap huruf pada *plaintext* akan ditentukan oleh huruf pada kunci yang mempunyai posisi yang sama dengan huruf pada *plaintext*. fungsi enkripsi dan dekripsi adalah

$$ci = E(pi) = (pi + k) \bmod 26) \quad (1)$$

$$pi = D(ci) = (ci - k) \bmod 26) \quad (2)$$

Cara lain untuk melakukan enkripsi dan dekripsi adalah dengan menggunakan *Vigenere Square* sebagai berikut :

Plaintext

Kunci

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar. 2.3 *Vigenere Square*

Contoh :

PlainText : S E L A M A T P A G I

Kunci : M A L A M

Berdasarkan tabel di atas maka untuk melakukan enkripsi dapat dilakukan dengan langkah-langkah sebagai berikut:

1. Sesuaikan jumlah karakter kunci dengan jumlah karakter *plaintext* dengan mengulang karakter kunci
2. Konversi pasangan karakter *plaintext* dan karakter kunci berdasarkan tabel 2.
3. Karakter hasil konversi tersebut kemudian dikumpulkan dan disusun menjadi *ciphertext*

Plaintext	S	E	L	A	M	A	T	P	A	G	I
Kunci	M	A	L	A	M	M	A	L	A	M	M
Cipher	E	E	W	A	Y	M	T	A	A	S	U

Jika penyelesaian dilakukan dengan menggunakan rumus, maka hasil yang didapatkan tidak akan berbeda, contohnya untuk pasangan karakter S dan M serta pasangan karakter E dan A jika dirumuskan maka hasilnya adalah sebagai berikut:

Untuk S dan M :

$ci = E(pi) = (pi + ki) \bmod 26$

$= (18 + 12) \bmod 26$

$= 30 \bmod 26 = 4$ (E)

Untuk E dan A :

$ci = E(pi) = (pi + ki) \bmod 26$

$= (4 + 0) \bmod 26$

$= 4 \bmod 26 = 4$ (E)

c. *Autokey* Cipher

Kriptografi *Autokey* adalah pengembangan dari kriprografi Caesar dan Vigenere. Cara melakukan enkripsi sama dengan kedua kriptografi sebelumnya. Pada kriptografi *Autokey* juga digunakan sebuah kata sebagai kunci. Kunci ini kemudian diikuti dengan *plaintext* sehingga membentuk huruf-huruf yang sama panjang dengan *plaintext*. Urutan huruf-huruf ini yang akan digunakan sebagai kunci pada saat enkripsi. Rumus yang berlaku untuk kriptografi *Autokey* sama dengan untuk Caesar dan Vigenere dan bisa menggunakan *vigenere square*.

Contoh :

PlainText : S E L A M A T P A G I

Kunci : M A L A M

Enkripsi dengan menggunakan metode *autokey* tidak jauh berbeda dengan metode *vigenere,* di mana langkah-langkah yang digunakan untuk menyelesaikan atau mencari *ciphertext* masih terbilang sama. Letak perbedaannya hanya terletak pada penyesuaian jumlah karakter *plaintext* dengan karakter kunci, di mana jika jumlah kunci lebih kecil dari *plaintext*, maka kunci akan ditambah dengan karakter *plaintext*. Untuk lebih jelasnya dapat dilihat pada urutan di bawah ini:

Plaintext	S	E	L	A	M	A	T	P	A	G	I
Kunci	M	A	L	A	M	S	E	L	A	M	A
Cipher	E	E	W	A	Y	S	X	A	A	S	I

Ciphertext yang dihasilkan dengan menggunakan metode *autokey* didapatkan dengan menggunakan cara yang sama dengan metode *vigenere*, di mana pasangan karakter *plaintext* dan karakter kunci akan dikonversi dengan menggunakan tabel *Vigenere Square*

d. *Reverse* Cipher

Metode *reverse* tidak memiliki rumus karna tidak mengandung perhitungan matematis sama sekali. Ini adalah salah satu metode kriptografi klasik yang menggunakan substitusi yaitu mengganti satu huruf dengan huruf lain. Metode *reverse* merupakan contoh yang paling sederhana dari substitusi yaitu mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik.

Contoh :

PlainText : S E L A M A T P A G I Maka

CipherText : T A M A L E S I G A P

e. *Column Cipher*

Pada kriptografi kolom *(column cipher), plaintext* disusun dalam kelompok huruf yang terdiri dari beberapa huruf. Kemudian huruf-huruf dalam kelompok ini dituliskan kembali kolom per kolom, dengan urutan kolom yang bisa berubah-ubah. Metode *Column* juga tidak menggunakan rumus matematis karena tidak mengandung perhitungan matematis sama sekali. Berikut langkah-langkah enkripsi dengan menggunakan metode *Column*:

1. Tentukan jumlah kolom untuk menyusun karakter *plaintext*, kemudian susun karakter *plaintext*
2. Kemudian tentukan kunci berupa urutan nomor dari kolom yang di bentuk. Jika jumlah karakter *plaintext* tidak memenuhi kolom, maka ditambahkan dengan karakter bebas
3. Ciphertext didapatkan dengan menyusun huruf berdasarkan kunci

Contoh :

PlainText : S E L A M A T P A G I

Dengan jumlah kolom = 4 dan Kunci : 3 1 2 4

S	E	L	A
M	A	T	P
A	G	I	A

Maka ciphertext yang dihasilkan adalah : " L T I S M A E A G A P A "

2.3.4 Kelemahan-kelemahan Kriptografi Klasik

Kelemahan-kelemahan kriptografi klasik ini terletak pada algoritmanya yang terlalu sederhana. Selain itu kerahasiaan algoritmanya tidak terjamin dan mudah terbongkar. Contohnya pada kriptografi caesar, jika kita mengetahui beberapa huruf depan maka kita akan mengetahui polanya, dan kunci akan dengan muda ditemukan. Atau dengan cara menganalisis kemunculan huruf dalam satu bahasa tertentu maka akan didapatkan pola-pola tertentu yang diterapkan pada *Ciphertext* tersebut.

Kriptografi caesar juga bisa dipecahkan dengan cara *brute-force.* Hanya ada 26 jenis kunci dan dapat dicoba satu persatu kunci pada sebuah potongan kata di kalimat *ciphertext*.

Pada kriptografi *reverse*, secara fisik kriptograf ini mudah dipecahkan dengan melihat kata-kata pendek atau kata-kata yang merupakan palindrome pada *ciphertext* maka akan dengan mudah.

Berikut beberapa alasan mengapa kriptografi klasik mudah di pecahkan:

1. Terdapat bagian pesan atau kata-kata yang berulang pada *ciphertext*nya. Tanpa perulangan, akan sulit untuk memperkirakan *plaintext* suatu kata. Bila diffusion berjalan baik maka akan sulit melihat perulangan-perulangannya.
2. Terdapat hubungan yang jelas antara *plaintext* dengan *chipertext.*
3. Terdapat keteraturan pada susunan *plaintext*, *ciphertext* ataupun kuncinya
4. Bila mengetahui bahasa penyusun *plaintext*nya, orang akan lebih mudah mendekripsinya.
5. Dalam kasus tertentu, penyembunyian algoritma enkripsi memang dapat meningkatkan keamanan sistem, namun hal ini tidak mutlak karena berdasarkan *ciphertext*nya analisis sandi dapat memperkirakan sistem enkripsi yang digunakan.

2.3.5. Modifikasi Kriptografi Klasik

Kelemahan-kelemahan kritografi klasik dapat dikurangi dengan memodifikasikan metode-metode yang ada sehinggan algoritma kriptografinya

menjadi lebih rumit dan tidak dapat ditebak dengan dengan sekali melihat. Konsekuensinya, modifikasi yang dilakukan pada metode yang ada akan menigkatkan keamanan dari enkripsi itu sendiri. Berikut ini beberapa modifikasi dari kriptografi klasik.

1. Kriptografi Kombinasi

   Beberapa kelemahan kriptografi klasik bisa ditutupi dengan mengkombinasikannya, karena kekurangan sebuah metode kriptografi klasik dapat ditutupi oleh kelebihan metode kriptografi lain. Selain itu, kombinasi juga dapat dilakukan dengan mengkombinasikan metode enkripsi atau dengan kata lain dengan cara melakukan enkripsi berlapis ganda.

   Contohnya Metode *autokey* dapat dikombinasikan dengan metode *reverse* di mana kelemahan metode *reverse* akan ditutupi oleh kesulitan memecahkan enkripsi *autokey*. Huruf-huruf pada hasil enkripsi *autokey* akan disamarkan posisinya karena proses enkripsi dan dekripsi yang sebenarnya dilakukan dari belakang bukan dari depan seperti enkripsi *autokey* normal.

   Contoh :

   PlainText : S E L A M A T P A G I

   Kunci : M A L A M

   Maka penyelesaiannya seperti pembahasan di atas :

Plaintext	S	E	L	A	M	A	T	P	A	G	I
Kunci	M	A	L	A	M	S	E	L	A	M	A
Cipher	E	E	W	A	Y	S	X	A	A	S	I

Untuk selanjutnya *Ciphertext* yang dihasilkan akan kembali dienkripsi dengan metode *reverse,* sehingga menghasilkan *ciphertext* yang baru sebagai berikut :

Ciphertext 1 : E E W A Y S X A A S I

Ciphertext 2 : X S Y A W E E I S A A

2. Kriptografi *One-time pad*

One-time pad adalah kriptografi yang merupakan perbaikan terhadap kriptografi caesar. *One-time pad* menggunakan kunci yang mempunyai panjang sama dengan *plaintext* dan kunci ini akan digunakan satu kali, oleh karena itu cara ini dikenal dengan *One-time pad* dan kriptografi ini tidak dapat dipecahkan karena kunci hanya digunakan satu kali sehingga tidak ada suatu pola tertentu. Satu-satunya cara melakukan dekripsi adalah dengan mengetahui kunci yang digunakan.

Contoh :

PlainText : S E L A M A T P A G I

Kunci : M A L A M M I N G G U

Berikutnya dilakukan penyusunan karaker sebagai berikut :

Plaintext	S	E	L	A	M	A	T	P	A	G	I
Kunci	M	A	L	A	M	M	I	N	G	G	U
Cipher	E	E	W	A	Y	M	B	C	G	M	C

J

i

Maka dirumuskan maka hasil yang didapat adalah sebagai berikut:

Untuk S dan M :

ci = E(pi) = (pi + ki) mod 26

= (18 + 12) mod 26

= 30 mod 26 = 4 (E)

Untuk L dan L :

ci = E(pi) = (pi + k) mod 26

= (11 + 11) mod 26

= 22 mod 26 = 22 (W)

Untuk M dan M:

ci = E(pi) = (pi + k) mod 26

= (12 + 12) mod 26

=24 mod 26 = 24 (Y)

Untuk T dan I :

ci = E(pi) = (pi + k) mod 26

= (19 + 8) mod 26

= 27 mod 26 = 1 (B)

Untuk A dan G:

ci = E(pi) = (0 + k) mod 26

= (0 + 6) mod 26

= 6 mod 26 = 6

(G) Untuk I dan U:

ci = E(pi) = (pi + k) mod 26

Untuk E dan A :

ci = E(pi) = (pi + ki) mod 26

= (4 + 0) mod 26

= 4 mod 26 = 4

(E) Untuk A dan A:

ci = E(pi) = (0 + 0) mod 26

= (0 + 0) mod 26

= 0 mod 26 = 0 (A)

Untuk A dan M:

ci = E(pi) = (0 + 12) mod 26

= (0 + 12) mod 26

= 12 mod 26 = 12

(M) Untuk P dan N :

ci = E(pi) = (pi + k) mod 26

= (15 + 13) mod 26

= 28 mod 26 = 2

(C) Untuk G dan G :

ci = E(pi) = (pi + k) mod 26

= (6+6) mod 26

= 12 mod 26 = 12 (M)

Alfabet	A	B	C	D	E	F	G	H	I	J	K	L	M
Konversi	M	A	L	I	N	G	U	B	C	D	E	F	H
Alfabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Konversi	J	K	O	P	Q	R	S	T	V	W	X	Y	Z

= (8 + 20) mod 26

= 28 mod 26 = 2 (C)

Ciphertext yang dihasilkan : " E E W A Y M B C G M C "

3. Kriptografi Random Subtitution

Ide dari metode kriptografi ini adalah mengurutkan abjad secara acak dimana huruf-huruf awalnya diambil dari huruf-huruf yang muncul pada kunci setelah itu dilanjutkan dengan huruf alfabet sisanya.

Contoh :

PlainText : S E L A M A T P A G I

Kunci : M A L A M M I N G G U

Berdasarkan frekuensi penggunaan karakter kunci maka kunci yang digunakan adalah " M A L I N G U" , selanjutnya akan dibentuk tabel konversi alfabet sebagai berikut :

Berdasarkan tabel konversi di atas maka cipher yang di hasilkan adalah sebagai berikut :

PlainText : S E L A M A T P A G I

CipherText : R N F M H M S O M U C

4. Penerapan karakter selain alfabet

Pada kriptografi klasik biasa, kebanyakan *plaintext* hanya berisi alfabet saja diamana bila yang jadi masukan angka atau karakter lain maka tesk tidak bisa dienkripsi. Untuk mengakomodasikan hal ini, maka kita akan menggunakan standar ASCII untuk merepresentasikan karaker-karakter standar yang ada.

Plaintext : S A Y A di ubah menjadi 5 4 Y

4

Kunci : K I T A

Plaintext	5	4	Y	4
Kunci	K	I	T	A

Dengan rumus maka hasilnya adalah sebagai berikut :

Untuk 5 dan K :

ci = E(pi) = (pi + k) mod 128

= (53 + 75) mod 128

= 128 mod 128 = 0 (^@)

Untuk 4 dan I :

ci = E(pi) = (pi + k) mod 128

= (52 + 73) mod 128

= 125 mod 128 = 125 (})

Untuk Y dan T :

ci = E(pi) = (pi + k) mod 128

= (89 + 84) mod 128

= 173 mod 128 = 45 (-)

Untuk 4 dan A :

ci = E(pi) = (pi + k) mod 26

= (52+ 65) mod 128

= 117 mod 128 = 117 (u)

Maka ciphertext yang dihasilkan adalah sebagai berikut :" ^@ } – u "

2.4. PHP *(Personal Home Page)*

Menurut dokumen resmi PHP *(Personal Home Page)*, PHP *(Personal Home Page)* merupakan bahasa berbentuk skrip yang ditempatkan dalam *server* dan diproses di *server.* Bermula pada tahun 1994 saat Rasmus Lerdorf membuat sejumlah skrip yang dapat mengamati siapa saja yang melihat-lihat riwayat hidupnya. Skrip-skrip ini selanjutnya dikemas mejadi tools yang disebut *Personal Home Page*. Paket inilah yang menjdi PHP *(Personal Home Page)*. Pada tahun 1995 Rasmus menciptakan PHP/FI versi 2. Pada versi ini pemogram dapat menempelkan kode terstruktur di dalam tag HTML. Selain itu, kode PHP *(Personal Home Page)* juga bisa berkomunikasi dengan database dan melakukan perhitungan-perhitungan yang kompleks.

Saat ini PHP *(Personal Home Page)* cukup popular sebagai piranti pemograman *web,* terutama di lingkungan Linux. Namun demikian PHP sebenarnya juga dapat berfungsi pada *server-server* yang berbasis UNIX, Windows NT dan *Macintosh*. Bahkan versi untuk Windows 95/98 pun tersedia. Pada awalnya PHP dirancang untuk diintegrasikan dengan *web server Apache*. Namun saat ini PHP juga dapat bekerja dengan web server seperti PWS (*Personal Web Server*), IIS (*Internet Information Server*) dan Xintami. PHP *(Personal Home Page)* dapat di-*download* secara bebas dan gratis.

Skrip PHP *(Personal Home Page)* berkedudukan sebagai tag dalam bahasa HTML *(Hypertex Markup Language)* adalah bahasa standar untuk membuat

halaman-halaman web. Berikut contoh kode PHP *(Personal Home Page)* yang berada di kode HTML:

```
<HTML>
<HEAD>
<TITLE> CONTOH </TITLE>
</HEAD>
<BODY>
  SELAMAT DATANG
        <BR> <? php
                printf (“Tanggal : %s”, Date (“D M Y “));
        ?>
</BODY>
</HTML>
```

Kode di atas disimpan dengan ekstensi .php. Kode PHP *(Personal Home Page)* diawali dengan <? dan diakhiri dengan ?>. Pasangan kedua kode inilah yang berfungsi sebagai tag kode PHP *(Personal Home Page)*. Berdasarkan tag inilah server dapat memahami kode PHP *(Personal Home Page)* dan kemudian memprosesnya. Hasilnya dikirim ke *browser.*

Prinsip kerja HTML diawali dengan permintaan suatu halaman *web* oleh *browser*. Berdasarkan URL *(Uniform Resource Locator*) dikenal dengan alamat *internet*, *browser* mendapatkan alamat dari *web server*, mengidentifikasi halaman yang dikehendaki dan menyampaikan segala informasi yang dibutuhkan oleh *web server*. Selanjutnya *web server* mencari berkas yang diminta dan memberikan isinya

ke *browser*. *Browser* menampilkan isinya ke layar pemakai. Sedangkan prinsip kerja PHP mirip dengan kode HTML, hanya saja ketika berkas PHP *(Personal Home Page)* yang diminta didapatkan oleh *web server*, isinya segera dikirim ke mesin PHP *(Personal Home Page)* dan mesin inilah yang memproses dan memberikan hasilnya berupa kode HTML ke *web server* dan selanjutnya *web server* menyampaikan ke *clien*t.

2.5. MySQL *(Structured Query Language)*

MySQL *(Structured Query Language)* adalah salah satu dari sekian banyak sistem *database* yang merupakan terobosan solusi yang tepat dalam aplikasi *database*. MySQL *(Structured Query Language)* merupakan turunan salah satu konsep utama dalam database sejak lama yaitu SQL *(Structured Query Language)*.

MySQL *(Structured Query Language)* dikembangkan pada tahun 1994 oleh sebuah perusahaan pengembang software dan konsultan *database* di Swedia bernama TcX Data Konsullt AB. Tujuan awal dikembangkan MySQL *(Structured Query Language)* adalah untuk mengembangkan aplikasi berbasis *web* pada *client*. Sebagai *database server* yang memiliki konsep *database* modern, MySQL *(Structured Query Language)* memiliki banyak sekali keistemewaan antara lain :

1. *Portabilitas,* dapat berjalan stabil pada berbagai sistem operasi, seperti Windows, Linux, MacOS, dan lain-lain.
2. *Open Source,* didstribusikan secara gratis dibawah lisensi GPL *(General Public License)*.

3. *Multiuser,* dapat digunakan oleh beberapa user dalam waktu yang bersamaan tanpa mengalami masalah.
4. *Performance Tuning,* memiliki kecepatan yang menakjubkan dalam menangani *query* yang sederhana, dapat memproses lebih banyak SQL *(Structured Query Language)* per satuan waktu.
5. *Security,* memiliki beberapa lapisan sekuritas seperti level subnet mask, nama *host*, izin akes user dengan sistem perizinan yang mendetail serta *password* yang terenskripsi.
6. *Scalability and Limits,* mampu menangani *database* dalam skala besar, dengan jumlah *record* lebih dari 50 juta dan 60 ribu tabel serta 5 miliar baris. Selain itu batas indeks yang dapat ditampung mencapai 32 indeks pada tiap tabelnya
7. *Connectivity,* dapat melakukan koneksi dengan *client* menggunakan protocol TCP/IP, *Unix socket* (Unix), atau *Named pipes* (NP).
8. *Localisation,* dapat mendeteksi pesan kesalahan pada *client* dengan mengunakan lebih dari 20 bahasa.
9. *Interface,* memiliki antarmuka (interface) terhadap beberapa aplikasi dan bahasa pemrograman dengan menggunakan fungsi API *(Application Programming Interface).*
10. *Clients and Tools*, dilengkapi dengan berbagai tools yang dapat digunakan untuk administrasi *database*, dan pada setiap tools yang ada disertakan petunjuk *online.*

2.6. Macromedia Dreamweaver

Salah satu *software web* editor adalah *Macromedia Dreamweaver* yang merupakan penyempurnaan dari versi sebelumnya dan tentu saja semakin mudah dalam penggunaannya. Oleh karena itu, *software* ini paling inovatif dan lebih lengkap dibandingkan *software web editor* lain. Adapun pengertian dari *Macromedia Dreamweaver* ini adalah program aplikasi professional untuk mengedit HTML secara *visual*. Program Aplikasi *Macromedia Dreamweaver* menyertakan banyak perangkat yang berkaitan dengan pengkodean dan fitur seperti HTML, CSS (*Cascading Style Sheet)*, serta *JavaScript*. Fasilitas terbaru dari *Macromedia Dreamweaver* adalah *Zoom Tool and Guides*, Panel CSS (*Cascading Style Sheet)* yang baru, *Code Collapse*, *Coding Toolbar*, dan *Insert Flash Video*. *Macromedia Dreamweaver* mendukung pemrograman *script server-side*, seperti PHP, ASP, ASP.NET, *ColdFusion* dan JSP. Pemrograman *script server-side* maksudnya adalah *script* yang digunakan dalam pemrograman *web* dinamis dimana semua perintahnya dieksekusi pada *server.* Fungsi *server* disini adalah sebagai pemroses *script* dan hasilnya dikembalikan dalam bentuk tag-tag HTML yang kemudian ditampilkan dalam *browser.*

Dreamweaver MX dalam hal ini digunakan untuk *web desain*. *Dreamweaver* MX mengikutsertakan banyak *tools* untuk kode-kode dalam halaman *web* beserta fasilitas-fasilitasnya, antara lain, Referensi HTML, CSS (*Cascading Style Sheet)* dan Javascript, Javascript debugger, dan editor kode (tampilan kode dan *Code inspector*)

yang mengizinkan kita mengedit kode Javascript, XML, dan dokumen teks lain secara langsung dalam *Dreamweaver*.

Teknologi *Dreamweaver Roundtrip* HTML mampu mengimpor dokumen HTML tanpa perlu memformat ulang kode tersebut dan kita dapat menggunakan *Dreamweaver* pula untuk membersihkan dan memformat ulang HTML bila kita menginginkannya. Selain itu *Dreamweaver* juga dilengkapi kemampuan manajemen situs, yang memudahkan kita mengelola keseluruhan elemen yang ada dalam situs. Kita juga dapat melakukan evaluasi situs dengan melakukan pengecekan *broken link*, kompatibilitas *browser*, maupun perkiraan waktu *download* halaman *web*.

BAB III

PEMBAHASAN

3.1. Analisa Kebutuhan

Analisa yang dilakukan pada bab ini adalah analisa kebutuhan dari *e-Learning* yang akan di bangun serta analisa mengenai metode pembelajaran yang digunakan. Analisa kebutuhan terbagi dalam 3 bagian yaitu; analisa kebutuhan data, analisa kebutuhan proses dan analisa kebutuhan infrastruktur dari sistem yang akan dibangun.

a. Analisa Kebutuhan Data

Analisa kebutuhan data yang dilakukan terhadap sistem *e-Learning* modifikasi metode-metode kriptografi klasik yang dibangun merupakan analisa terhadap data-data yang perlukan sebagai input untuk selanjutnya akan digunakan dalam analisa kebutuhan proses.

Analisa kebutuhan data mendefenisikan data-data secara terperinci dimana data-data tersebut merupakan entiti yang terlibat atau yang akan digunakan pada tahap pemrosesan.

Data-data yang diperlukan dalam pembangunan *e-Learning* modifikasi metode-metode kriptografi klasik dapat dilihat pada Tabel 3.

Tabel 3. Tabel Hasil Analisa Kebutuhan Data

No	Data	Atribut	Proses
1	*User*	Id*User* Nama Password Email Status	*Login* Registrasi
2	Buku Tamu	IdTanggal Tanggal Nama E-mail Komentar	Input Buku Tamu
3	Materi	IdMateri Nama Video File Keterangan	Input Materi: Upload Materi Download Materi
5	Forum	Id*member* Komentar Tanggal	Forum Diskusi

b. Analisa Kebutuhan Proses

Analisa kebutuhan proses yang dilakukan dalam *e-Learning* modifikasi metode-metode kriptografi klasik adalah menganalisa perangkat lunak apa saja yang butuhkan dalam proses pembangunannya.

Untuk lebih jelasnya analisa kebutuhan proses telah diuraikan secara rinci dapat dilihat pada Tabel 4.

Tabel 4. Tabel Hasil Analisa Kebutuhan Proses

No	Proses	Deskripsi	*User*
1	*Login*	*Login* dilakuan oleh *User* dengan status yang berbeda yaitu: *member*(peserta) dan admin, dimana setiap status dari *user* memiliki hak akses yang berbeda	*Member* (Peserta) & Admin
2	Registrasi	Registrasi dilakukan oleh pengunjung untuk menjadi *member* agar mendapatkan hak akses yang lebih dari sekedar pengunjung biasa	Pengunjung
3	Input Buku Tamu	Buku Tamu diinputkan oleh pengunjung yang telah melihat materi pembelajaran dan ingin meninggalkan komentar	Pengunjung & Admin
4	Upload Materi	Upload materi dilakukan untuk menambahkan materi pembelajaran yang dilakukan oleh admin dan *member* dimana *member* hanya menambahkan saja dan tidak bisa mengedit atau menghapus materi	*Member* (Peserta) & Admin
5	Download Materi	Download Materi merupakan akses tambahan bagi peserta dimana peserta dapat mendownload materi yang ditampilkan	*Member* (Peserta)
6	Forum	Forum Diskusi merupakan komunikasi antar *member* yang ingin mendiskusikan tentang isi materi	*Member* (Peserta)

c. Analisa Kebutuhan Infrastruktur

Analisa kebutuhan infrastruktur yang dilakukan dalam *e-Learning* modifikasi metode-metode kriptografi klasik adalah pengolahan data-data hasil analisa kebutuhan data yang telah dilakukan sebelumnya. Proses-proses yang dapat dilakukan merupakan fitur-fitur atau fasilitas-fasilitas yang tersedia dalam *e-*

Learning, dimana setiap *user* yang berbeda status memiliki hak akses yang berbeda untuk setiap proses.

Untuk lebih jelasnya analisa kebutuhan proses telah diuraikan secara rinci dapat dilihat pada Tabel 5.

Tabel 5. Tabel Hasil Analisa Kebutuhan Infrastruktur

No	Perangkat Lunak	Proses
1	PHP Triad	PHP Triad digunakan saat pembangunan Database dengan MySQL sebagai DBMSnya dan Apache sebagai localhost servernya untuk mengeksekusi Program
2	Dream Weaver 8	Dream Weaver 8 digunakan pada proses perancangan program diaman Dream Weaver digunakan sebagai editor prorgam
3	Camtasia Studio 6	Camtasia Studio digunakan untuk proses pembuatan materi yang berbentuk Video

d. Analisa CAI *(Computer Assisted Instructions)*

Metode *CAI (Computer Assisted Instructions)* memiliki beberapa bentuk interaksi yang dapat diaplikasikan seperti: Praktek dan latihan *(drill & practice)*, Tutorial, Permainan *(games)*, Simulasi *(simulation)*, Penemuan *(discovery)* dan Pemecahan Masalah *(Problem Solving)*. Dalam perancangan *e-Learning* modifikasi metode-metode kriptografi klasik dengan menggunakan PHP dan MySQL bentuk interaksi yang ditawarkan dapat dirincikan sebagai berikut:

1. Praktek dan Latihan *(Drill and Pratice)*

   Praktek yang ditawarkan dalam *e-Learning* modifikasi metode-metode kriptografi klasik berupa praktek penyelesaian contoh-contoh soal yang disajikan secara detail, dengan penjelasan yang lengkap sehingga *user* dapat memahami langkah-langkah penyelesaiannya.

2. Tutorial

   Tutorial yang ditawarkan dalam *e-Learning* modifikasi metode-metode kriptografi klasik berupa langkah langkah dalam memodifikasi metode-metode kriptografi seperti, mengkombinasikan beberapa metode, implementasi kriptografi *One time pad,* kriptografi *Random Subtitution* dan melakukan penerapan karakter selain alfabet. Langkah-langkah tersebut akan disajikan secara terurut satu per satu, sehingga *user* dapat mengerti proses-proses yang dijelaskan.

3.2. Materi Pembelajaran Modifikasi Kriptografi Klasik

Materi pembelajaran dalam *e-Learning* modifikasi metode-metode kriptografi klasik merupakan pemanfaatan kembali metode-metode kriptografi klasik dengan cara melakukan pemodifikasian agar kelemahan-kelemahan kritografi klasik dapat dikurangi. Pemodifikasian metode-metode kriptografi klasik dilakukan hingga algoritma kriptografinya menjadi lebih rumit dan tidak dapat ditebak dengan dengan sekali melihat. Konsekuensinya, modifikasi yang dilakukan pada metode yang ada

akan menigkatkan keamanan dari enkripsi itu sendiri. Berikut ini beberapa modifikasi dari kriptografi klasik.

BAB IV

PENUTUP

1. Pembelajaran modifikasi metode kriptografi klasik dengan menggunakan media internet dapat membantu proses pembelajaran dari segi waktu di mana peserta dapat mengakses materi kapan saja.
2. Penyajian materi kriptografi klasik melalui *e-Learning* yang menarik dapat membantu minat belajar matakuliah kriptografi bagi para peserta atau pengujung *e-Learning.*
3. Menyajikan materi modifikasi kriptografi klasik dengan berbasis multimedia dapat membantu mempermudah pemahaman bagi para peserta ataupun pengunjung tentang konsep kriptografi dan metode-metode yang ada di dalamnya.
4. Dengan melakukan modifikasi metode-metode dari kriptografi klasik, maka tingkat keamanan dari metode-metode tersebut dapat meningkat.

DAFTAR PUSAKA

Nugroho, Bunafit., ***Database Relasional*** **dengan** ***MySQL***., Penerbit Andi.,2005.

Yusuf, Mudasiru Olalere dan Afolabi, Adedeji Olufemi, **Effects Of Computer Assisted Instruction (Cai) On Secondary School Students' Performance In Biology,** TOJET. 2010.

Surjono, H. **Pengembangan Computer-Assisted Instruction (CAI) Untuk Pelajaran**. Elektronika. Jurnal Kependidikan. No. 2 (XXV): 95-106. 1995

http://licence.blogdetik.com/2008/12/04/vigenere-

cipher/ http:// Security in Computing, Prientice Hall

http:// www.bimacipta.com/ga.htm, tanggal akses 16/06/2009