BAB II

TINJAUAN PUSTAKA

II.1. Pengertian Folder

Folder adalah suatu tempat untuk menyimpan ataupun menampung *file-file*, baik itu *file* sistem maupun *file* data atau dokumen. *Icon* folder sendiri di komputer umumnya berbentuk kecil seperti amplop berwarna kuning atau coklat. Folder dapat kita buat pada *desktop* komputer maupun pada *drive-drive* dalam komputer sesuai dengan kebutuhan. *File* yaitu kumpulan data-data baik berupa angka, teks, gambar, video, *slide*, program dan sebagainya yang diberi nama tertentu secara digital, itulah pengertian *file*. Sedangkan folder atau *directory* yaitu tempat untuk menyimpan *file* tersebut.

II.1.1. Fungsi dan Manfaat Folder

Fungsi secara umum yaitu tempat dimana *file* di dalam suatu komputer disimpan dengan rapi agar si pengguna komputer tersebut dapat dengan mudah jika ingin mengakses *file* tersebut.

Dalam kaitannya dengan fungsi media pembelajaran, dapat ditekankan beberapa hal berikut ini:

1) Sebagai sarana mewujudkan situasi pembelajaran yang lebih efektif.
2) Sebagai salah satu komponen yang saling berhubungan dengan komponen lainnya dalam rangka menciptakan situasi belajar yang diharapkan.
3) Mempercepat proses belajar.

4) Meningkatkan kualitas proses belajar-mengajar.
5) Mengkongkritkan yang abstrak sehingga dapat mengurangi terjadinya penyakit verbalisme.

Pemanfaatan folder dalam pembelajaran dapat membangkitkan keinginan dan minat baru, meningkatkan motivasi dan rangsangan kegiatan belajar, dan bahkan berpengaruh secara psikologis . Ada beberapa manfaat folder dalam proses belajar, yaitu: (Tejo Nurseto, journal.uny.ac.id ; 2011 : 22).

1) Dapat menumbuhkan motivasi belajar karena pengajaran akan lebih menarik perhatian pengguna.
2) Makna bahan pengajaran akan menjadi lebih jelas sehingga dapat dipahami pengguna dan memungkinkan terjadinya penguasaan serta pencapaian tujuan pengajaran.
3) Metode mengajar akan lebih bervariasi, tidak semata-mata didasarkan atas komunikasi verbal melalui kata-kata, dan

Manfaat media pembelajaran adalah sebagai berikut:

1) Menyamakan Persepsi Siswa.

   Dengan melihat objek yang sama dan konsisten maka siswa akan memiliki persepsi yang sama.
2) Mengkonkritkan konsep-konsep yang abstrak.

   Misalnya untuk menjelaskan tentang sistem pemerintahan, perekonomian, berhembusnya angin, dan sebagainya. bisa menggunakan media gambar, grafik atau bagan sederhana.

3) Menghadirkan objek-objek yang terlalu berbahaya atau sukar didapat ke dalam lingkungan belajar.

   Misalnya guru menjelaskan dengan menggunakan gambar atau film tentang binatang-binatang buas, gunung meletus, lautan, kutup utara.

4) Menampilkan objek yang terlalu besar atau kecil.

   Misalnya guru akan menyampaikan gambaran mengenai sebuah kapal laut, pesawat udara, pasar, candi, dan sebagainya. Atau menampilkan objek-objek yang terlalu kecil seperti bakteri, virus, semut, nyamuk, atau hewan/benda kecil lainnya.

5) Memperlihatkan gerakan yang terlalu cepat atau lambat.

   Dengan menggunakan teknik gerakan lambat (*slow motion*) dalam media film bisa memperlihatkan tentang lintasan peluru, melesatnya anak panah, atau memperlihatkan suatu ledakan. Demikian juga gerakan-gerakan yang terlalu lambat seperti pertumbuhan kecambah, mekarnya bunga wijaya kusumah dan lain-lain.

II.1.2. Klasifikasi Media

Menurut bentuk informasi yang digunakan, dapat memisahkan dan mengklasifikasi media dalam lima kelompok besar, yaitu media visual diam, media visual gerak, media audio, media audio visual diam, dan media audio visual gerak.

Proses yang dipakai untuk menyajikan pesan, apakah melalui penglihatan langsung, proyeksi optik, proyeksi elektronik atau telekomunikasi. Dengan menganalisis media melalui bentuk penyajian dan cara penyajiannya,

mendapatkan suatu format klasifikasi yang meliputi tujuh kelompok media penyaji, yaitu:

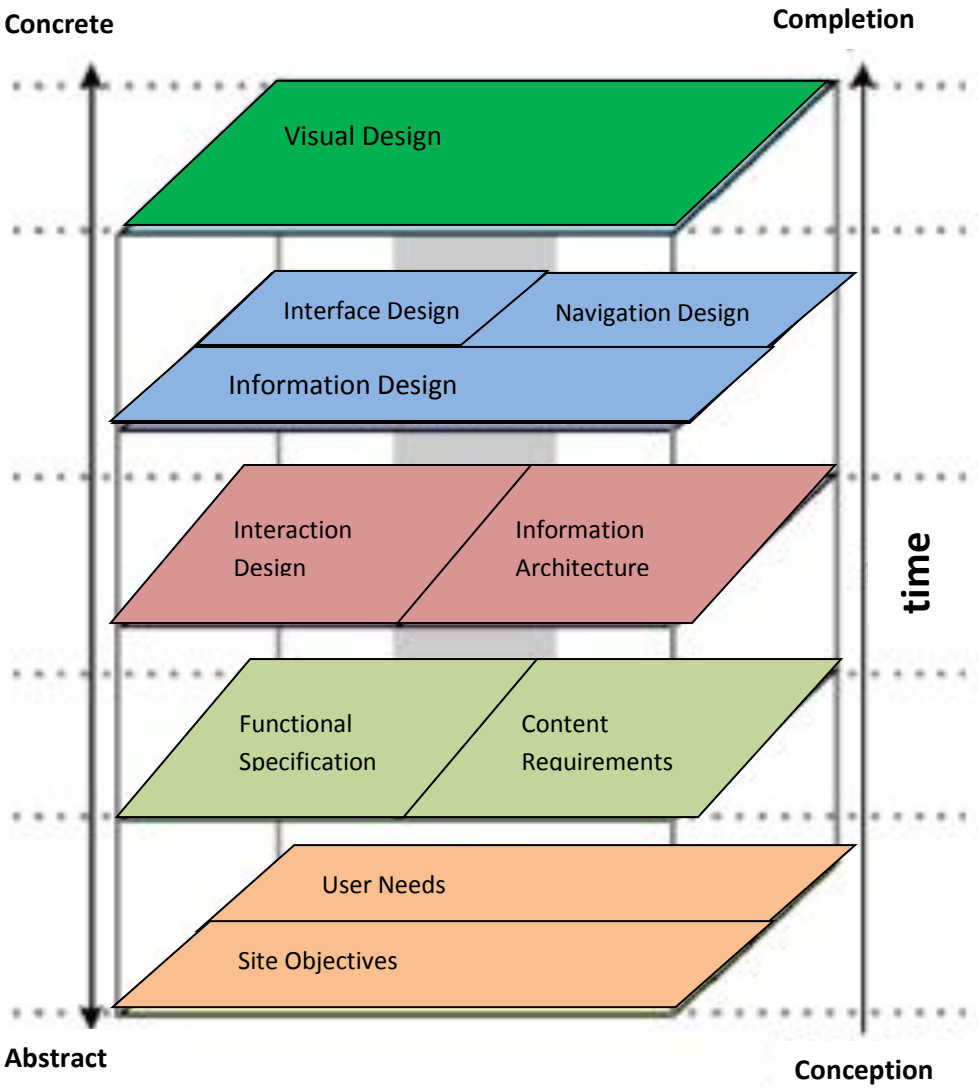
1. Grafis, bahan cetak, dan gambar diam
2. Media proyeksi diam.
3. Media audio.
4. Media audio visual diam.
5. Media Audio visual hidup/film.
6. Media televisi, dan
7. Multi media.

II.1.3. Media Pembelajaran Interaktif

Media Interaktif adalah integrasi dari media digital termasuk kombinasi *dari electronic text, graphics, moving images,* dan *sound,* ke dalam lingkungan digital yang terstruktur yang dapat membuat orang berinteraksi dengan data untuk tujuan yang tepat. Lingkungan digital meliputi Internet, Telekomunikasi, *Interactive digital television dan Game Interactive.* Tidak heran, sulit juga bagi pendatang baru untuk memahaminya. (Rudi Yulio Arindiono, dkk, ejurnal.its.ac.id, 2013 : 29).

User interface adalah bagian yang paling penting dari program komputer manapun. Karena dengan adanya *user interface*, proses komunikasi antara pengguna dengan sistem komputer dapat terjadi. Tujuan utama dari *interface design* adalah untuk membuat pekerjaan dengan menggunakan komputer menjadi

lebih sederhana, mudah, produktif, dan menyenangkan. Proses desain interaktif media dapat dilihat pada gambar II.2.



Gambar II.1 : Diagram *elements of user interface*
(Sumber : Rudi Yulio Arindiono, dkk, ejurnal.its.ac.id, 2013 : 29)

II.2. Perancangan

Untuk membuat tampilan yang menarik memang tidak mudah dilakukan. Seorang perancang tampilan selain harus mempunyai jiwa seni yang memadai, ia juga harus mengerti selera pengguna secara umum. Hal lain yang pelu disadari oleh seorang perancang tampilan adalah bahwa ia harus bisa meyakinkan pemrogramnya bahwa apa yang ia bayangkan dapat diwujudkan dengan peranti bantu yang tersedia (Insap Santoso ; 2009 : 185).

Bagi perancang antarmuka, hal yang sangat penting untuk ia perhatikan adalah mendokumentasikan semua pekerjaan yang dilakukan. Dokumentasi rancangan dapat dikerjakan atau dilakukan dengan beberapa cara :

1. Membuat sketsa pada kertas
2. Menggunakan peranti purwarupa GUI
3. Menuliskan keterangan yang menjelaskan tentang kaitan antara jendela.
4. Menggunakan peranti bantu CASE (*Computer Aided Software Engineering*).

Cara kedua dan keempat tidak selalu dapat diterapkan, karena peranti tersebut biasanya harus dibeli dan seringkali cukup mahal. Cara ini kebanyakan diterapkan pada pembuatan antarmuka grafis untuk suatu jenis pekerjaan berskala besar.

II.2.1. Prinsip Dan Petunjuk Perancangan

Antarmuka pengguna secara alamiah terbagi menjadi empat komponen model pengguna, bahasa perintah, umpan balik, dan penampilan informasi. Model pengguna merupakan dasar dari tiga komponen yang lain (Insap Santoso ; 2009 : 188-189).

Model mental pengguna merupakan model konseptual yang dimiliki oleh pengguna ketika ia menggunakan sebuah sistem atau program aplikasi. Model ini memungkinkan seorang pengguna untuk mengembangkan pemahaman mendasar tentang bagian yang yang dikerjakan oleh program, bahkan oleh pengguna yang sama sekali tidak mengetahui teknologi komputer. Dengan pertolongan model itu pengguna dapat mengantisipasi pengaruh suatu tindakan yang ia lakukan dan dapat memilih strategi yang cocok untuk mengoperasikan program tersebut. Model pengguna dapat berupa suatu simulasi tentang keadaan yang sebenarnya dalam dunia nyata, sehingga ia tidak perlu mengembangkannya sendiri dari awal.

Setelah pengguna mengetahui dan memahami model yang di inginkan, dia memerlukan peranti untuk memanipulasi model itu. Peranti pemanipulasian model ini sering disebut dengan bahasa perintah (*command language*), yang sekaligus merupakan komponen kedua dari antarmuka pengguna. Idealnya program komputer kita mempunyai bahasa perintah yang alami, sehingga model pengguna dengan cepat dapat dioperasionalkan.

Komponen ketiga adalah umpan balik. Umpan balik di sini diartikan sebagai kemampuan sebuah program yang membantu pengguna untuk mengoperasikan program itu sendiri. Umpan balik dapat berbentuk pesan penjelasan, pesan penerimaan perintah, indikasi adanya obyek terpilih, dan penampilan karakter yang diketikkan lewat papan ketik. Beberapa bentuk umpan balik terutama ditujukan kepada pengguna pengguna yang belum berpengalaman dalam menjalankan program sebuah aplikasi. Umpan balik dapat digunakan untuk

member keyakinan bahwa program telah menerima perintah pengguna dan dapat memahami maksud perintah tersebut.

Komponen keempat adalah tampilan informasi. Komponen ini digunakan untuk menunjukkan status informasi atau program ketika pengguna melakukan suatu tindakan. Pada bagian ini perancang harus menampilkan pesan-pesan tersebut dengan baik sehingga mudah dipahami oleh pengguna. Setelah memahami beberapa prinsip dalam perancangan antarmuka pengguna. Pada bagian berikut ini akan diberikan petunjuk singkat tentang perancangan antarmuka yang akan Anda lakukan sebagai seorang perancang tampilan.

II.2.2. Urutan Perancangan

Perancangan dialog, seperti halnya perancangan sistem yang lain, harus dikerjakan secara atas ke bawah. Proses perancangannya dapat dikerjakan secara bertahap sampai rancangan yang diinginkan terbentuk, yaitu sebagai berikut : (Insap Santoso ; 2009 : 190).

1. Pemilihan ragam dialog

Untuk suatu tugas tertentu, pilihlah ragam dialog yang menurut perkiraan cocok untuk tugas tersebut. Ragam dialog dapat dipilih dari sejumlah ragam dialog yang telah dijelaskan pada bab-bab sebelumnya. Pemilihan ragam dialog dipengaruhi oleh karakterisiktik populasi pengguna, tipe dialog yang diperlukan, dan kendala teknologi yang ada untuk mengimplementasikan ragam dialog tersebut. Ragam dialog yang terpilih dapat berupa sebuah ragam tunggal, atau sekumpulan ragam dialog yang satu sama lain saling mendukung.

2. Perancangan Struktur Dialog

Tahap kedua adalah melakukan analisis tugas dan menentukan model pengguna dari tugas tersebut untuk membentuk struktur dialog yang sesuai. Dalam tahap ini pengguna sebaiknya banyak dilibatkan, sehingga pengguna langsung mendapatkan umpan balik dari diskusi yang terjadi. Pada tahap ini suatu purwarupa dialog seringkali dibuat untuk memberikan gambaran yang lebih jelas kepada calon pengguna.

3. Perancangan format pesan

Pada tahap ini tata letak tampilan dan keterangan tekstual secara terinci harus mendapat perhatian lebih. Selain itu, kebutuhan data masukan yang mengharuskan pengguna untuk memasukkan data ke dalam komputer juga harus dipertimbangkan dari segi efisiensinya. Salah satu contohnya adalah dengan mengurangi pengetikan yang tidak perlu dengan cara mengefektifkan pengguna tombol.

II.3. Keamanan Data

Keamanan data merupakan bagian dari perkembangan teknologi informasi. Ketika berpikir bahwa data yang dimiliki merupakan data yang sangat penting, semua berusaha untuk melindunginya agar jangan sampai jatuh ke tangan orang yang tidak bertanggung jawab. Tetapi buat sebagian orang, mereka justru tidak mengetahui sepenting apakah data yang mereka miliki. Karena ketidaktahuan tersebut, mereka baru menyadari bahwa data yang mereka miliki

sangat penting setelah mengalami kecurian data dan mengalami kerugian. Data di sini bisa bersifat umum tidak terbatas pada data digital saja, tetapi juga seperti data diri (ktp, ijasah, sertifikat, dan lain-lain). Data yang menyangkut informasi pribadi tidak seharusnya diumbar sembarang seperti pada situs blog yang tersedia, situs jejaring pertemanan, *email*, selebaran, fotokopi KTP di buang sembarangan dan lain-lain. (Andik Susilo ; 2010 : 59).

Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Masalah keamanan sering kurang mendapat perhatian dari para perancang dan pengelola sistem informasi. Masalah keamanan sering berada di urutan setelah tampilan, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu performansi sistem, masalah keamanan sering tidak dipedulikan, bahkan ditiadakan. (Doni Ariyus ; 2010 : 6).

Informasi menentukan hampir setiap elemen dari kehidupan manusia. Informasi sangat penting artinya bagi kehidupan karena tanpa informasi maka hampir semuanya tidak dapat dilakukan dengan baik. Contohnya, jika membeli tiket penerbangan dan membayarnya dengan menggunakan kartu kredit, informasi mengenai diri nantinya disimpan dan dikumpulkan serta digunakan oleh bank dan penerbangan. Demikian juga halnya saat membeli obat di apotik. Harus mendapat resep dari dokter dan memberikan resep tersebut ke pelayan apotik. Resep itu merupakan satu informasi yang disampaikan dokter ke pihak apotik tentang obat yang dibutuhkan.

Kemajuan sistem informasi memberikan banyak keuntungan bagi kehidupan manusia. Meski begitu, aspek negatifnya juga banyak, seperti

kejahatan komputer yang mencakup pencurian, penipuan, pemerasan, kompetisi, dan banyak lainnya. Jatuhnya informasi ke pihak lain, misalnya lawan bisnis, dapat menimbulkan kerugian bagi pemilik informasi. Sebagai contoh, banyak informasi milik perusahaan yang hanya boleh diketahui oleh orang-orang tertentu di perusahaan tersebut, seperti misalnya informasi tentang produk yang sedang dalam pengembangan. Algoritma dan teknik yang digunakan untuk menghasilkan produk tersebut. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas tertentu.

II.3.1. Ancaman Keamanan

Terjadi banyak pertukaran informasi setiap detiknya di internet. Juga banyak terjadi pencurian atas informasi oleh pihak-pihak yang tidak bertanggung jawab. Ancaman keamanan yang terjadi terhadap informasi adalah :

1) *Interruption*

   Merupakan ancaman terhadap *availability* informasi, data yang ada dalam sistem komputer dirusak atau dihapus sehingga jika data atau informasi tersebut dibutuhkan maka pemiliknya akan mengalami kesulitan untuk mengaksesnya, bahkan mungkin informasi itu hilang.

2) *Interception*

   Merupakan ancaman terhadap kerahasiaan (*secrecy*). Informasi disadap sehingga orang yang tidak berhak dapat mengakses komputer di mana informasi tersebut disimpan.

3) *Modification*

Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan kemudian mengubahnya sesuai keinginan orang tersebut.

4) *Fabrication*

Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru atau memalsukan informasi sehingga orang yang menerima informasi tersebut menyangka bahwa informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi. (Doni Ariyus ; 2010 : 6).

II.3.2. Aspek-aspek Keamanan Komputer

Keamanan komputer meliputi empat aspek, antara lain :

1) *Authentication*

Agar penerima informasi dapat memastikan keaslian pesan, bahwa pesan itu datang dari orang yang dimintai informasi. Dengan kata lain, informasi itu benar-benar datang dari orang yang dikehendaki.

2) *Integrity*

Keaslian pesan yang dikirim melalui jaringan dan dapat dipastikan bahwa informasi yang dikirm tidak dimodifikasi oleh orang yang tidak berhak.

3) *Non Repudiation*

Merupakan hal yang berhubungan dengan si pengirim. Pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.

4) *Authority*

   Informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak untuk mengaksesnya.

5) *Confidentiality*

   Merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses.

6) *Privacy*

   Lebih ke arah data-data yang bersifat pribadi.

7) *Availability*

   Aspek availabilitas berhubungan dengan ketersediaan informasi ketika dibutuhkan.

8) *Access Control*

   Aspek ini berhubungan dengan cara pengaturan akses ke informasi. Hal ini biasanya berhubungan dengan masalah otentikasi dan privasi. Kontrol akses seringkali dilakukan dengan menggunakan kombinasi *user id* dan *password* dengan mekanisme lain. (Doni Ariyus ; 2010 : 6).

II.4. Teori Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut *Bruce Schneier* dalam bukunya "*Applied Cryptography*", kriptografi adalah ilmu pengetahuan dan seni menjaga

message-message agar tetap aman (*secure*). (Aris Pamungkas, research.amikom .ac.id, diakses tanggal 8 Mei 2014).

Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni:

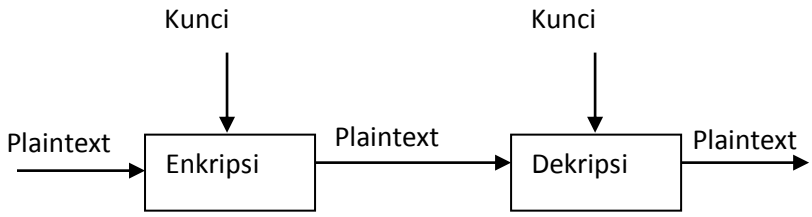
1. *Confidelity* (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain kecuali pihak pengirim, pihak penerima atau pihak-pihak memiliki ijin. Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.
2. *Data integrity* (keutuhan data) yaitu sebuah layanan yang mampu mengenali atau mendeteksi adanya manipulasi penghapusan, pengubahan atau penambahan data yang tidak sah oleh pihak lain.
3. *Authentication* (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
4. *Non-repudiation* (anti penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya.

Kriptografi juga berkembang menjadi kriptografi modern. Berbeda dengan kriptografi klasik yang menitikberatkan kekuatan pada kerahasiaan algoritma yang digunakan yang artinya apabila algoritma yang digunakan telah diketahui maka pesan sudah jelas bocor dan dapat diketahui isinya oleh siapa saja yang mengetahui algoritma tersebut, kriptografi modern lebih menitikberatkan pada kerahasiaan kunci yang

digunakan pada algoritma tersebut, sehingga algoritma tersebut dapat saja disebarkan ke kalangan masyarakat tanpa takut kehilangan kerahasiaan bagi para pemakainya. Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi :

1. *Plaintext* (M) adalah pesan yang hendak dikirimkan (berisi data asli).
2. *Ciphertext* (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
3. *Enkripsi* (fungsi E) adalah proses pengubahan *plaintext* menjadi *ciphertext*.
4. *Dekripsi* (fungsi D) adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga berupa data awal/asli.
5. Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Kriptografi terdiri dari dua proses utama yakni enkripsi dan dekripsi, proses enkripsi mengubah *plaintext* menjadi *ciphertext* sehingga isi informasi pada pesan tersebut sukar dimengerti.



Gambar II.2 : *Diagram proses enkripsi dan dekripsi*
(Sumber : Wahana Komputer ; 2011 : 6)

Peranan kunci sangatlah penting dalam proses enkripsi dan dekripsi (disamping pula algoritma yang digunakan) sehingga kerahasiaannya sangatlah penting, apabila kerahasiaannya terbongkar, maka isi dari pesan dapat diketahui.

Secara matematis, proses enkripsi merupakan pengoperasian fungsi E (enkripsi) menggunakan e (kunci enkripsi) pada M *(plaintext)* sehingga dihasilkan C *(ciphertext),* notasinya :

$$E_e(M) = C \quad \text{.....(1)}$$

Sedangkan untuk proses dekripsi, merupakan pengoperasian fungsi D (dekripsi) menggunakan d (kunci dekripsi) pada C *(ciphertext)* sehingga dihasilkan M *(plaintext),* notasinya :

$$D_d(C) = M \quad \text{.....(2)}$$

Sehingga dari dua hubungan diatas berlaku :

$$D_d(E_e(M)) = M \quad \text{.....(3)}$$

II.5. Algoritma Simetris

Algoritma simetris *(symmetric algorithm)* adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm.*

Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini disebut juga algoritma kunci rahasia *(secret-key algorithm).* (Aris Pamungkas, 2010, research .amikom.ac.id, diakses tanggal 8 Mei 2014).

Kelebihan :

1. Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik.
2. Karena kecepatannya yang tinggi, maka dapat digunakan pada sistem *real-time*

Kelemahan :

1. Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.
2. Permasalahan dalam pengiriman kunci itu sendiri yang disebut *key distribution problem*. Contoh algoritma : TwoFish, Rijndael, Camellia.

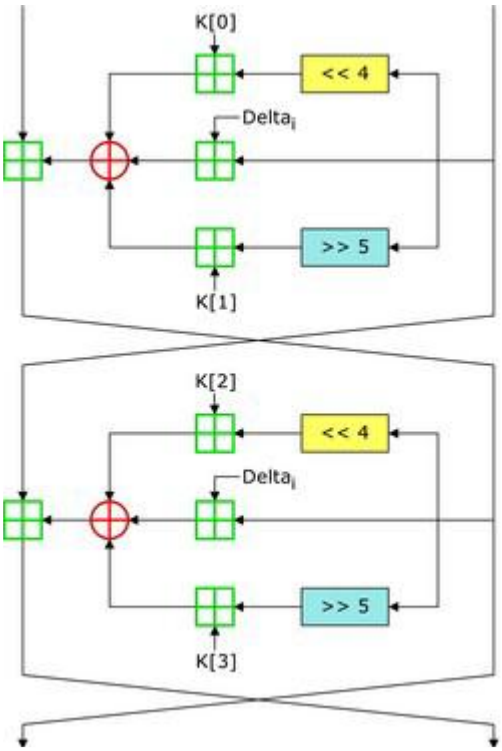
II.6. *TEA (Tiny Encryption Algorithm)*

TEA adalah algoritma *block cipher* yang diciptakan oleh David J. Wheeler dan Roger M. Needham dari Cambridge University tahun 1994. Hal yang paling menonjol dari TEA adalah kesederhanaan implementasi, ketiadaan S-Box maupun P-Box dan kecepatan yang tinggi.

TEA beroperasi dalam ukuran blok 64 bit dan panjang kunci 128 bit. TEA berbasiskan jaringan Feistel dan memiliki 32 putaran. Kunci K pertama-tama akan dibagi menjadi 4 kunci internal yaitu K[0..3] masing-masing panjangnya 32 bit. Setiap putaran TEA terdiri atas dua rondeFeistel (lihat gambar 1). Penjadwalan kunci TEA sangat sederhana, yaitu untuk ronde ganjil digunakan K[0] dan K[1], sedangkan untuk ronde genap digunakan K[2] dan K[3].

Tahap pertama, *plainteks* yang diinputkan dioperasikan dengan kunci eksternal pertama (K1) dan melakukan proses *enkripsi* dengan menggunakan algoritma TEA. Sehingga menghasilkan pra *cipherteks* pertama. Tahap kedua, pra *cipherteks* pertama yang dihasilkan pada tahap pertama, kemudian dioperasikan dengan kunci eksternal kedua (K2) dan melakukan proses enkripsi atau proses

dekripsi dengan menggunakan algoritma TEA. Sehingga menghasilkan cipherteks kedua. Tahap terakhir, cipherteks kedua yang dihasilkan pada tahap kedua, dioperasikan dengan kunci eksternal ketiga (K3) dan melakukan proses enkripsi dengan menggunakan algoritma TEA, sehingga menghasilkan *cipherteks* (C).



Gambar II.3 : Satu putaran enkripsi TEA
(Sumber : pustaka.unpad.ac.id; 2011)

II.6.1. Pemilihan Kunci

David Wagner dan Kelsey pada tahun 1997 menemukan kerentanan TEA terhadap *equivalent key* dan *related key attack* karena kesederhanaan penjadwalan kuncinya. *Equivalent key* yang dimiliki TEA adalah untuk setiap kunci terdapat tiga buah kunci lain yang menghasilkan *ciphertext* yang sama. Kuncikunci tersebut didapatkan dengan membalik nilai *most significant bit* (MSB) pada K[0]

dan K[1] atau K[2] dan K[3]. Sehingga panjang kunci 128 bit hanya akan menghasilkan 2 kunci yang berbeda.

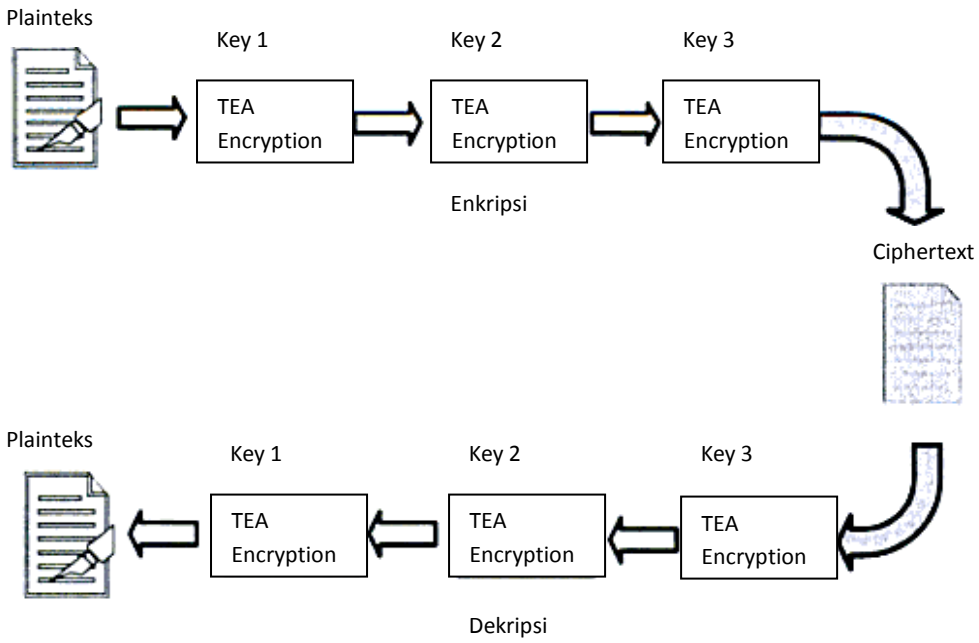
Berikut adalah contoh bukti dari dua pilihan untuk pemilihan kunci eksternal algoritma TEA, yaitu :

a. K1, K2, dan K3 adalah kunci-kunci yang saling bebas

K1 ≠ K2 ≠ K3 ≠ K1

b. K1 dan K2 adalah kunci-kunci yang saling bebas, dan K3 sama dengan K1

K1 ≠ K2 dan K3 = K1, Perhatikan gambar II.6 dibawah ini :



Gambar II.4 : Proses Enkripsi pada Algoritma TEA
(Sumber : Dony Ariyus, Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi ; 2010)

Pada gambar II.3 terdapat 3 kunci, yaitu K1, K2, K3. Proses kerja dari TEA, K1 berfungsi untuk enkripsi, K2 untuk dekripsi, dan K3 untuk enkripsi, atau juga dikenal denga mode *Encrypt Descrypt Encrypt* (EDE).

Contoh :

Diberikan tiga kunci :

K1 = 0x260b152f31b51c68

K2 = 0x321f0d61a773b558

K3 = 0x519b7331bf104ce3

16 putaran kunci yang cocok diberikan K1, K2, dan K3. Untuk melakukan perhitungan, coba lihat di bawah ini :

Putaran	K1	K2	K3
1	000ced9158c9	5a1ec4b60e98	03e4ee7c63c8
2	588490792e94	710c318334c6	8486dd46ac65
3	54882eb9409b	c5a8b4ec83a5	575a226a8ddc
4	a2a006077207	96a696124ecf	aab9e009d59b
5	280e26b621e4	7e16225e9191	98664f4f5421
6	e03038a08bc7	ea906c836569	615718ca496c
7	84867056a693	88c25e6abb00	4499e580db9c
8	c65a127f0549	245b3af0453e	93e853d116b1
9	2443236696a6	76d38087dd44	cc4a1fa9f254
10	a311155c0deb	1a915708a7f0	27b30c31c6a6
11	0d02d10ed859	2d405ff9cc05	0a1ce39c0c87
12	1750b843f570	2741ac4a469a	f968788e62d5
13	9e01c0a98d28	9a09b19d710d	84e78833e3c1
14	1a4a0dc85e16	9d2a39a252e0	521f17b28503
15	09310c5d42bc	87368cd0ab27	6db841ce2706
16	53248c80ee34	30258f25c11d	c9313c0591e3

Enkripsi :

Tahap pertama : EK1 = 0x7a39786f7ba32349

Tahap kedua : DK2 = 0x9c60f85369113aea

Tahap ketiga : EK3 = 0xe22ae33494beb930 = C (teks-kode)

Dekripsi :

Tahap keempat : DK3 = 0x9c60f85369113aea

Tahap kelima : EK2 = 0x7a39786f7ba32349

Tahap akhir : DK1 = 0x403da8a295d3fed9 = P (teks asli)

II.6.2. Proses *Enkripsi* dan *Dekripsi*

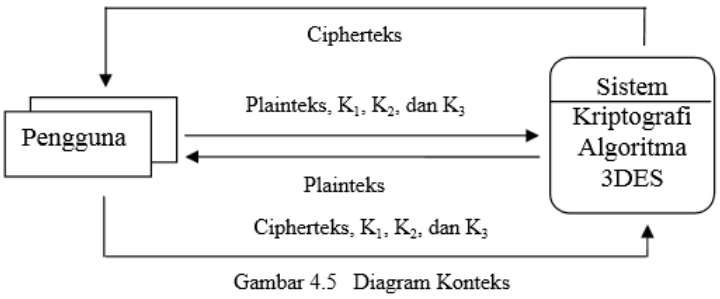
Proses enkripsi dan dekripsi algoritma TEA dapat dicapai dengan beberapa cara, yaitu :

Tabel II.1. Cara Pengenkripsian dan Pendekripsian

Cara	Enkripsi	Dekripsi
1	DES – EDE2 ▪ $K_1 \neq K_2, K_3 = K_1$ ▪ $C = E [D \{E (P, K_1), K_2\}, K_3]$	DES – DED2 ▪ $K_1 \neq K_2, K_3 = K_1$ ▪ $P = D [E \{D (C, K_3), K_2\}, K_1]$
2	DES – EEE2 ▪ $K_1 \neq K_2, K_3 = K_1$ ▪ $C = E [E \{E (P, K_1), K_2\}, K_3]$	DES – DDD2 ▪ $K_1 \neq K_2, K_3 = K_1$ ▪ $P = D [D \{D (C, K_3), K_2\}, K_1]$
3	DES – EDE3 ▪ $K_1 \neq K_2 \neq K_3 \neq K_1$ ▪ $C = E [D \{E (P, K_1), K_2\}, K_3]$	DES – DED3 ▪ $K_1 \neq K_2 \neq K_3 \neq K_1$ ▪ $P = D [E \{D (C, K_3), K_2\}, K_1]$
4	DES – EEE3 ▪ $K_1 \neq K_2 \neq K_3 \neq K_1$ ▪ $C = E [E \{E (P, K_1), K_2\}, K_3]$	DES – DDD3 ▪ $K_1 \neq K_2 \neq K_3 \neq K_1$ ▪ $P = D [D \{D (C, K_3), K_2\}, K_1]$

II.7. Perancangan Sistem

Perancangan dimulai dengan pembuatan diagram konteks, berupa gambaran sistem penerapan algoritma TEA secara garis besar.



Gambar 4.5 Diagram Konteks

Gambar II.5 : Perancangan Sistem
(Sumber : pustaka.unpad.ac.id; 2011)

II.8. UML

UML (*unified modeling language*) adalah bahasa pemodelan untuk sistem atau perangkat lunak yang berparadigma berorientasi objek. Pemodelan (modeling) sesungguhnya digunakan untuk penyederhanaan permasalahan-permasalahan yang kompleks sedemikian rupa sehingga lebih mudah dipelajari dan dipahami. Adapun tujuan pemodelan adalah sebagai sarana analisis, pemahaman, visualisasi dan komunikasi antar anggota tim pengembang, serta sebagai sarana dokumentasi.(Adi Nugroho ; 2010 : 6).

Unified Modelling Language (UML) adalah suatu alat untuk memvisualisasikan dan mendokumentasikan hasil analisa dan desain yang berisi sintak dalam memodelkan sistem secara visual. Juga merupakan satu kumpulan konvensi pemodelan yang digunakan untuk menentukan atau menggambarkan sebuah sistem *software* yang terkait dengan objek. (Haviluddin, informatika mulawarman.files.wordpress.com, diakses tanggal 08 Mei 2014).

Sejarah UML sendiri terbagi dalam dua *fase* sebelum dan sesudah munculnya UML. Dalam fase sebelum, UML sebenarnya sudah mulai

diperkenalkan sejak tahun 1990 namun notasi yang dikembangkan oleh para ahli analisis dan desain berbeda-beda, sehingga belum memiliki standarisasi.

Fase kedua dilandasi dengan pemikiran untuk mempersatukan metode tersebut dan dimotori oleh *Object Management Group* (OMG) maka pengembangan UML dimulai pada akhir tahun 1994 ketika *Grady Booch* dengan metode OOD(*Object-Oriented Design*), Jim Rumbaugh dengan metode OMT (*Object Modelling Technique*) mereka ini bekerja pada Rasional *Software Corporation* dan *Ivar Jacobson* dengan metode OOSE (*Object-Oriented Software Engineering*) yang bekerja pada perusahaan *Objectory* Rasional.

Sebagai pencetus metode-metode tersebut mereka bertiga berinisiatif untuk menciptakan bahasa pemodelan terpadu sehingga pada tahun 1996 mereka berhasil merilis UML versi 0.9 dan 0.91 melalui *Request for Proposal* (RFP) yang dikeluarkan oleh OMG. Kemudian pada Januari 1997 IBM, *ObjecTime, Platinum Technology, Ptech, Taskon, Reich Technologies* dan *Softeam* juga menanggapi *Request for Proposal* (RFP) yang dikeluarkan oleh OMG tersebut dan menyatakan kesediaan untuk bergabung.

Fokus dari UML versi rilis 1.1 ini adalah untuk meningkatkan kejelasan UML Semantik versi rilis 1.0. Hingga saat ini UML versi terbaru adalah versi 2.0. Saat ini sebagian besar para perancang sistem informasi dalam menggambarkan informasi dengan memanfaatkan UML diagram dengan tujuan utama untuk membantu tim proyek berkomunikasi, mengeksplorasi potensi desain, dan memvalidasi desain arsitektur perangkat lunak atau pembuat program.

Tabel I.1 : Diagram dalam UML

Major Area	View	Diagram	Main Concepts
Structural	Static view	Class diagram	Class, association, generalization, dependency, realization, interfaces
	Use case view	Use case diagram	Use case, actor, association, extend, include, use case generalization
	Implementation view	Component diagaram	Component, interface, dependency, realization
	Deployment view	Deployment diagram	Node, component, dependency, location
Dynamic	State machine view	Statechart diagram	State, event, transition, action
	Activity view	Activity diagram	state, activity, completion transition, fork, join
	Interaction view	Sequence diagram	Interaction, object, message, activation
		Collaboration diagram	Collaboration, interaction, collaboration role, message
Model management	Model management view	Class diagram	Package, subsystem, model
Extensibility	All	All	Constraint, stereotype, lagged values.

(Sumber : Adi Nugroho ; Rekayasa Perangkat Lunak Berorientasi Objek dengan Metode USDP ; 2010)

Secara filosofi UML diilhami oleh konsep yang telah ada yaitu konsep permodelan *Object Oriented* karena konsep ini menganalogikan sistem seperti kehidupan nyata yang didominasi oleh obyek dan digambarkan atau dinotasikan dalam simbol-simbol yang cukup spesifik.

II.8. Visual Studio .NET 2010

Visual Basic adalah bahasa pemrograman klasik, legendaries, dan tiada duanya yang paling banyak dipakai oleh programmer di dunia. Bahasa pemrograman ini dipakai oleh jutaan programmer, dan tercatat sebagai program yang paling dikuasai oleh mayoritas orang. (Edy Winarno, dkk ; 2010 : 1).

Dari mulai programmer professional yang mencari nafkah dari pembuatan program dan coding, hingga para hobies dan para mahasiswa yang membuat program untuk tugas kuliah dan tugas akhir, visual basic memang bisa dihandalkan.

II.8.1. Menjalankan Visual Basic 2010

Pertama kali, harus menginstal visual basic 2010 ke dalam komputer. Tapi sebelum bisa menginstal, pastikan hardware dan sistem operasi memenuhi persyaratan yang diharapkan. Berikut ini prasyarat sistem untuk bisa diinstal visual basic 2010, yaitu :

1. Sistem operasi windows 7, windows vista, windows xp, windows 2003 atau windows server 2008.
2. Visual studio 2010 (professional, premium, atau ultimate).
3. Prosesor 1,6 GHz
4. Ruang kosong di hard disk 3 GB
5. Kecepatan hard disk 5400 RPM

6. Video Card yang mendukung Directx 9, yang bisa menjalankan resolusi 1024 x 768.
7. Drive DVD

II.8.2. Mengetahui Antarmuka Visual Basic 2010

Saat menjalankan visual basic 2010 pertama kali, muncul jendela choose default environment settings. Disini, bisa memilih apakah ingin memilih tipe antarmuka di visual studio. Untuk programmer visual basic, lebih baik pilih visual basic development settings.

Gambar II.6 : Pemilihan Default Environment Settings.
(Sumber : Dasar-dasar Pemrograman dengan Visual Basic 2010 ; 2010)

Di bagian awal visual basic, bisa melihat adanya *start page*. *Start page* ini adalah halaman yang mencantumkan informasi-informasi seputar program, dan juga informasi RSS dari sumber tertentu. Jika tidak ingin menampilkan hal ini, hilangkan tanda centang pada *show page on startup*.