MEDIA PEMBELAJARAN KRIPTOGRAFI
(ALGORITMA RSA DAN ALGORITMA KNAPSACK)
BERBASIS MULTIMEDIA

LAPORAN PROYEK ILMIAH

Sebagai salah satu syarat untuk memperoleh gelar ahli madya pada jurusan Teknik Komputer Universitas Islam Sultan Agung

Disusun Oleh:

Tri Mustikaningtyas

86206.0060

JURUSAN TEKNIK KOMPUTER

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM SULTAN AGUNG

2010

LEMBAR PENGESAHAN PEMBIMBING

Laporan Proyek Ilmiah dengan judul **"Media Pembelajaran Kriptografi (Algoritma RSA dan Algoritma Knapsack) Berbasis Multimedia"** ini disusun oleh:

Nama : Tri Mustikaningtyas

NIM : 86206060

Program Studi : Teknik Komputer

Telah diterima dan disetujui sebagai syarat untuk memenuhi Proyek Ilmiah pada program Diploma Tiga (D3) Jurusan Teknik Komputer Fakultas Teknologi Industri Universitas Islam Sultan Agung Semarang.

Dosen Pembimbing

Moch. Taufik S.T., MT.

Mengetahui,

Kepala Jurusan Prodi Teknik Komputer

Universitas Islam Sultan Agung

M. Khosyi'in ST., MT.

LEMBAR PENGESAHAN PENGUJI

Laporan Proyek Ilmiah dengan judul **"Media Pembelajaran Kriptografi (Algoritma RSA dan Algoritma Knapsack) Berbasis Multimedia"** ini telah dipertahankan didepan sidang Penguji Proyek Ilmiah pada :

Hari: Jum'at
Tanggal: 12 - Maret - 2010

Penguji	Tanda Tangan
Moch Taufik ST, MT	.....
M. Khosyi'in ST., MT	.....

PERSEMBAHAN

- Bapak dan Ibu tercinta, atas segala jerih payah dan doanya yang begitu berarti serta dukungan dan semangat untuk maju terus dalam terselesaikannya proyek ilmiah ini.
- Bapak / Ibu Dosen UNISSULA yang telah memberikan bimbingan dan pengetahuan, terutama kepada Bapak Moch. Taufik ST, MIT yang selalu mendukung, membimbing dan memberikan semangat, Terimakasih banyak.
- Teman-teman TIKOM 2006 yang telah terlibat dan ikut membantu dalam pembuatan proyek ilmiah ini. Terutama nisa, emi, kalian teman-teman seperjuangan. Thank you very much.
- Mas Muslik yang telah membantu memecahkan masalah dan menciptakan ide-ide imajinatif
- Yupati dan Crew griya
- Keluarga besar FTI yang selalu siap membantu keperluan akademis.

MOTTO

- Keberhasilan tidak bisa dikatakan sukses dan berhasil jika kita tidak mampu mengatasi segala macam rintangan dan hambatan yang ada di depan kita.
- Orang yang benar bukanlah orang yang tidak pernah salah. Tetapi orang yang benar adalah orang yang mampu memperbaiki kesalahan.
- Kegagalan adalah yang membuat hidup kita lebih baik. Kebanyakan kesalahan terbesar kita adalah kita lari dari masalah.
- Sikap optimis merupakan kunci kesuksesan dan kebahagiaan.
- Kesabaran itu pahit, tetapi buahnya manis.
- Berani melakukan tindakan yang tepat adalah jalan menuju sukses.
- Yakinlah dengan sebenar-benarnya akan pertolongan ALLAH. Karena buah keyakinan adalah kemenangan.

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kepada Allah SWT, pemberi kehidupan dan ilmu serta penerang hati, sehingga karena ridho-Nya, penulis dapat menyelesaikan Laporan Proyek Ilmiah yang bertema media pembelajaran dengan judul "Media Pembelajaran Kriptografi untuk Algoritma RSA dan Algoritma Knapsack Berbasis Multimedia", meskipun pada awalnya penulis menemui banyak kendala. Penyusunan Laporan Proyek Ilmiah ini merupakan salah satu kewajiban dan persyaratan dalam rangka menyelesaikan perkuliahan program studi Diploma III Teknik Komputer pada Fakultas Teknologi Industri Universitas Islam Sultan Agung Semarang. Tidak lupa ucapan terima kasih yang tulus penulis tujukan kepada semua pihak yang telah memberikan bantuan dan dorongan baik dalam bentuk moral maupun material sehingga Laporan Proyek Ilmiah ini dapat terselesaikan dengan baik. Dalam kesempatan ini, ucapan terima kasih dan rasa hormat penulis sampaikan kepada:

1. Kedua Orang Tua yang tercinta sebagai motivasi untuk maju dan semangat berkreasi.
2. Bapak Ir. H. Sukarno Budi Utomo, MT selaku Dekan Fakultas Teknologi Industri Universitas Islam Sultan Agung Semarang.
3. Bapak M. Khosyi'in ST., MT. selaku Ketua Program Studi D3 Teknik Komputer Fakultas Teknologi Industri Universitas Islam Sultan Agung Semarang.
4. Bapak Moch.Taufik ST., MT. selaku Dosen Pembimbing Proyek Ilmiah.
5. Teman-teman TIKOM angkatan 2006 dan sahabat yang telah membantu memberikan saran, kritik, semangat serta tenaga yang sangat berharga kepada penulis.
6. Semua pihak yang tidak dapat penulis sebutkan satu per satu yang telah membantu dalam menyelesaikan Proyek Ilmiah ini dengan baik.

Upaya maksimal dalam penyusunan Laporan Proyek Ilmiah ini telah penulis lakukan, namun tidak menutup kemungkinan adanya kekurangan baik tata tulis, bahasa, maupun penyajiannya. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan. Penulis berharap, semoga Laporan Proyek Akhir ini dapat bermanfaat bagi semua pihak.

Semarang, Maret 2010

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

ABSTRAK

Sistem pendidikan dewasa ini telah mengalami kemajuan yang sangat pesat. Berbagai cara telah dikenalkan serta digunakan dalam proses belajar mengajar (PBM) dengan harapan pengajaran guru akan lebih berkesan dan pembelajaran bagi murid akan lebih bermakna. Sejak beberapa tahun belakangan ini teknologi informasi dan komunikasi telah banyak digunakan dalam proses belajar mengajar, dengan satu tujuan mutu pendidikan akan selangkah lebih maju seiring dengan kemajuan teknologi.

Beberapa jenis buku yang mencakup materi kriptografi mungkin sudah banyak kita jumpai. Namun sebagian kurang menarik dan membosankan terutama untuk pemula. Buku memang sangat praktis digunakan, tetapi buku juga memiliki kelemahan, yaitu pembelajaran dengan menggunakan media buku ini nampaknya sulit dipahami dan membosankan. Penelitian De Porter mengungkapkan manusia dapat menyerap suatu materi sebanyak 70% dari apa yang dikerjakan, 30% dari apa yang didengar dan dilihat (audio visual), sedangkan dari yang dilihatnya hanya 20%, dari yang didengarnya hanya 20%, dan dari yang dibaca hanya 10%.

Untuk menghindari masalah-masalah tersebut, maka perlu dibuat metode pembelajaran baru yang lebih menarik dan menyenangkan. Oleh karena itu, muncul suatu ide penulis untuk membuat pembelajaran pada kriptografi yang khusus menjelaskan tentang algoritma RSA dan algoritma Knapsack yang ditampilkan dalam multimedia interaktif. Dengan adanya pembelajaran ini diharapkan para pemula dalam belajar kriptografi khususnya pada algoritma RSA dan algoritma Knapsack akan lebih tertarik dan senang mempelajarinya.

Kata kunci : pembelajaran, algoritma RSA, algoritma knapsack

BAB I
PENDAHULUAN

1.1. Latar Belakang

Sistem pendidikan dewasa ini telah mengalami kemajuan yang sangat pesat. Berbagai cara telah dikenalkan serta digunakan dalam proses belajar mengajar (PBM) dengan harapan pengajaran guru akan lebih berkesan dan pembelajaran bagi murid akan lebih bermakna. Sejak beberapa tahun belakangan ini teknologi informasi dan komunikasi telah banyak digunakan dalam proses belajar mengajar, dengan satu tujuan mutu pendidikan akan selangkah lebih maju seiring dengan kemajuan teknologi.

Perkembangan teknologi multimedia telah menjanjikan potensi besar dalam merubah cara seseorang untuk belajar, untuk memperoleh informasi, menyesuaikan informasi dan sebagainya. Multimedia juga menyediakan peluang bagi pendidik untuk mengembangkan teknik pembelajaran sehingga menghasilkan hasil yang maksimal. Demikian juga bagi pelajar, dengan multimedia diharapkan mereka akan lebih mudah untuk menentukan dengan apa dan bagaimana siswa untuk menyerap informasi secara cepat dan efisien.

Salah satu hal yang penting dalam komunikasi menggunakan komputer untuk menjamin kerahasiaan data adalah enkripsi. Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau chipper. Sebuah sistem pengkodean menggunakan suatu tabel atau kamus yang telah didefinisikan untuk mengganti kata dari informasi atau yang merupakan bagian dari informasi yang dikirim.

Beberapa jenis buku yang mencakup materi kriptografi mungkin sudah banyak kita jumpai. Namun sebagian kurang menarik dan membosankan terutama untuk pemula. Buku memang sangat praktis digunakan, tetapi buku juga memiliki kelemahan, yaitu pembelajaran dengan menggunakan media buku ini nampaknya sulit dipahami dan membosankan. Penelitian De Porter mengungkapkan manusia dapat menyerap suatu materi sebanyak 70% dari apa yang dikerjakan, 50% dari

apa yang didengar dan dilihat (audio visual), sedangkan dari yang dilihatnya hanya 30%, dari yang didengarnya hanya 20%, dan dari yang dibaca hanya 10%.

Untuk menghindari masalah-masalah tersebut, maka perlu dibuat metode pembelajaran baru yang lebih menarik dan menyenangkan. Oleh karena itu, muncul suatu ide penulis untuk membuat pembelajaran pada kriptografi yang khusus menjelaskan tentang algoritma RSA dan algoritma Knapsack yang dituangkan dalam macromedia flash 8. Dengan adanya pembelajaran ini diharapkan para pemula dalam belajar kriptografi khususnya pada algoritma RSA dan algoritma Knapsack akan lebih tertarik dan senang mempelajarinya.

1.2. Perumusan Masalah

Sebagaimana telah dijelaskan pada latar belakang permasalahan, bahwa media pembelajaran kriptografi juga penting untuk dipelajari karena berkenaan masalah keamanan dan kerahasiaan suatu data, maka yang menjadi permasalahan pada Proyek Ilmiah ini adalah " bagaimana agar perancangan pembelajaran ini sebagai alat bantu pembelajaran kriptografi yang mudah dipahami dan menarik bagi pengguna (mahasiswa) khususnya pada algoritma RSA dan algoritma Knapsack".

1.3. Pembatasan Masalah

Batasan masalah pada proyek ilmiah ini hanya difokuskan pada pembelajaran kriptografi khususnya algoritma RSA dan algoritma Knapsack dengan materi yaitu sejarah, konsep dasar, dan simulasi pada algoritma RSA dan algoritma Knapsack dengan media pembelajaran yang ditujukan untuk mahasiswa.

1.4. Tujuan Perancangan

1. Untuk menciptakan media pembelajaran pada kriptografi yang memiliki daya tarik terhadap pengguna (mahasiswa).
2. Memberikan solusi kepada mahasiswa atau masyarakat luas tentang proses enkripsi maupun dekripsi terhadap suatu pesan dengan menggunakan kunci

publik maupun kunci privat khususnya pada algoritma RSA dan algoritma Knapsack melalui bentuk pembelajaran agar lebih mudah dipahami dan menarik untuk dipelajari.

I.5. Metodologi Penelitian

Agar proyek ilmiah ini dapat memberikan hasil yang baik maka dalam penyusunan laporan ini penulis menggunakan data, informasi dan beberapa metode penelitian dalam pencarian sumber informasi yang dibutuhkan supaya penganalisaan berjalan secara terorganisasi, terencana dan tepat pada sasaran yang ditentukan.

1. *Interview*

   Cara mengumpulkan data dengan menggunakan wawancara secara langsung dengan tujuan mendapatkan informasi dari pihak yang bersangkutan. Wawancara dilakukan terhadap dosen mata kuliah kriptografi atau sistem keamanan.

2. Literatur dan Studi Pustaka

   Merupakan teknik pengumpulan data yang mendasar pada sumber-sumber terdahulu sebagai referensi dan penelitian selanjutnya. Alasan menggunakan literatur sebagai alat pengumpulan data adalah supaya dapat diperoleh data-data tertulis yang berupa referensi dari berbagai sumber seperti buku-buku atau internet.

4. Kebutuhan Software

   Software yang digunakan pada perancangan pembelajaran ini adalah menggunakan Macromedia Flash Professional 8 untuk pembuatan animasi dan audio untuk musik dan dubbing agar tidak membosankan.

5. Hasil Karya

   Dengan beberapa metode yang dilakukan, maka diperoleh hasil karya pembelajaran kriptografi khususnya algoritma RSA dan algoritma knapsack berbasis multimedia. Data yang dikumpulkan adalah data-data yang relevan dengan permasalahan, sehingga dalam hal ini data-data tersebut dapat dibagi dalam dua jenis yaitu:

a. Data Primer

Data primer yaitu data yang diperoleh secara langsung oleh penyusun melalui wawancara atau interview pada dosen mata kuliah kriptografi atau keamanan data.

b. Data Sekunder

Data sekunder adalah data yang dikumpulkan melalui jurnal-jurnal, internet dan buku-buku yang berkaitan dengan proyek ilmiah ini.

1.6. Sistematika Penulisan

Secara garis besar penyusunan laporan Proyek Ilmiah ini dibagi menjadi 5 (lima) bah, dengan rinciannya sebagai berikut:

BAB I PENDAHULUAN

Dalam bab ini menguraikan atau menjelaskan latar belakang masalah, perumusan masalah, pembatasan masalah, tujuan proyek ilmiah, metodologi penelitian, dan sistematika penulisan Laporan Proyek Ilmiah.

BAB II LANDASAN TEORI

Bab ini membahas tentang landasan teori dan definisi-definisi serta materi yang digunakan sebagai acuan dalam proses pembuatan media pembelajaran multimedia.

BAB III PERANCANGAN DAN PEMBUATAN SISTEM

Pada bab ini menjelaskan tentang perancangan sistem, teknik dan pembuatan sistem.

BAB IV HASIL DAN ANALISIS

Bab ini menjelaskan dan menguraikan hasil pengujian dan analisa.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan hasil penelitian dan saran-saran sehubungan dengan permasalahan yang telah dibahas.

BAB II
LANDASAN TEORI

2.1. Media Pembelajaran

2.1.1. Pengertian Media Pembelajaran

Menurut Depdiknas (2003) istilah media berasal dari bahasa latin yang merupakan bentuk jamak dari "medium"yang secara harfiah berarti perantara atau pengantar. Makna umumnya adalah segala seguatu yang dapat menyalurkan informasi dari sumber informasi kepada penerima informasi. Proses belajar mengajar pada dasarnya juga merupakan proses komunikasi, sehingga media yang digunakan dalam pembelajaran disebut media pembelajaran. Media pembelajaran merupakan bagian dari sumber belajar yang merupakan kombinasi antara perangkat lunak (bahan belajar) dan perangkat keras (alat belajar).

Secara umum media pembelajaran dapat dipilah menjadi istilah-istilah sebagai berikut:

- Alat peraga adalah alat (benda) yang digunakan untuk memperagakan fakta, konsep, atau prosedur tertentu agar tampak lebih nyata atau konkrit
- Alat bantu adalah alat atau benda yang digunakan oleh guru untuk mempermudah tugas dalam mengajar
- Ausio-Visual Aids (AVA) mempunyai pengertian dan tujuan yang sama hanya saja penekanannya pada peralatan audio dan visual
- Alat bantu belajar yang penekanannya pada pihak yang belajar.

2.1.2. Manfaat Media Pembelajaran

Secara umum manfaat media pembelajaran adalah memperlancar interaksi antara guru dan siswa sehingga kegiatan pembelajaran akan lebih efektif dan efisien. Tetapi secara khusus ada beberapa manfaat media yang lebih rinci. Kemp dan Dayton (dalam Depdiknas, 2003) mengidentifikasikan beberapa manfaat media dalam pembelajaran yaitu:

- Penyampaian materi pelajaran dapat diseragamkan
- Proses pembelajaran akan lebih jelas dan menarik

- Proses pembelajaran menjadi lebih interaktif
- Efisiensi dalam waktu dan tenaga
- Meningkatkan kualitas hasil belajar
- Memungkinkan proses belajar dapat dilakukan di mana saja dan kapan saja
- Media dapat menumbuhkan sikap positif siswa terhadap materi dan proses belajar
- Merubah peran guru ke arah yang lebih positif dan produktif.

Selain beberapa manfaat media seperti yang dikemukakan di atas, masih terdapat beberapa manfaat praktis. Manfaat praktis tersebut adalah :

- Media dapat membuat materi pelajaran yang abstrak menjadi lebih konkrit
- Media juga dapat membantu mengatasi keterbatasan ruang dan waktu
- Media dapat membantu mengatasi keterbatasan indra manusia
- Media dapat menyajikan obyek pelajaran berupa benda atau peristiwa langka dan berbahaya
- Informasi pelajaran yang disajikan dengan media yang tepat akan memberikan kesan mendalam dan lebih lama tersimpan pada diri siswa.

2.1.3. Jenis Media Pembelajaran

Anderson (dalam Depdiknas,2003) mengelompokkan media pembelajaran menjadi 10 golongan sebagai berikut:

- Audio : kaset audio, siaran radio, CD, telepon
- Cetak : buku pelajaran, modul, brosur, leaflet, gambar
- Ausi-cetak : kaset audio yang dilengkapi bahan tertulis
- Proyeksi visual diam: Overhead Transparansi (OHT), film bingkai (slide)
- Visual gerak : film bisu
- Proyeksi ausio visual diam : film bingkai (slide bersuara)
- Audio visual gerak : film gerak bersuara, video/ VCD, televisi
- Obyek fisik : benda nyata, model, spesimen
- Manusia dan lingkungan : guru, pustakawan, laboran

- Komputer : CAI (pembelajaran berbantuan komputer), CBI (pembelajaran berbasis komputer).

2.2. Multimedia

2.1.1. Pengertian Multimedia

Multimedia adalah kombinasi dari komputer dan video, atau secara umum merupakan kombinasi tiga elemen, yaitu suara, gambar dan teks. Atau kombinasi dari paling sedikit dua media input atau output dari data yang berupa audio (suara, musik), animasi, video, teks, grafik dan gambar. Atau multimedia merupakan alat yang dapat menciptakan presentasi yang dinamis dan interaktif yang mengkombinasikan teks, grafik, animasi, audio dan gambar video. Multimedia adalah suatu media yang terdiri dari beberapa media pendukung dan secara keseluruhan membentuk satu kesatuan media yang saling terkait untuk menambah arti dan manfaat terhadap user dari kegunaan media tersebut. Beberapa stimulus yang dapat dihasilkan dan digunakan diantaranya adalah audio, gambar, grafik, animasi gerak, dan interaksi. Kelima bentuk stimulus ini akan membantu proses pembelajaran, namun demikian tidaklah mudah mendapatkan kelima bentuk itu dalam satu kesatuan.

2.2.2. Multimedia Interaktif

Multimedia interaktif yaitu sistem yang menggunakan lebih dari satu media presentasi untuk memberikan perintah, mengendalikan dan memanipulasi suatu obyek sehingga terlihat lebih menarik.

2.2.3. Sejarah Perkembangan Multimedia

Multimedia adalah gabungan dari berbagai media penyampai informasi dengan menggunakan komputer. Contoh media penyampai informasi yang dimaksud adalah teks, gambar, foto, video, musik, bahkan animasi. Tetapi definisi tersebut masih belum lengkap. Masih ada satu karakterisik yang merupakan salah satu karakteristik dari mutimedia yang merupakan satu alasan terpenting mengapa kita perlu menggunakan teknologi multimedia, yaitu adalah interaktifitas. Kalau

kita perhatikan sebetulnya pada era awal penggunaan komputer, kita berinteraksi dengan komputer menggunakan *"Low Level Language"* atau "Bahasa Tingkat Rendah" yang berupa kode-kode atau symbol yang sulit untuk dihafal baik oleh seorang penggemar komputer sekalipun, yang menyebabkan orang awam kurang tertarik untuk menggunakan komputer. Era berikutnya adalah penggunaan *"High Level Language"* atau "Bahasa Tingkat Tinggi", dimana perintah yang digunakan untuk berinteraksi dengan komputer adalah semakin mirip dengan bahasa manusia, dalam hal ini Bahasa Inggris, sesuai dengan bahasa pembuatnya. Namun, dengan perkembangan pesat di perangkat keras komputer, baik dari segi prosessor, monitor, dan perangkat lainnya, munculah era grafi yang dimotori oleh Apple, yang kemudia diikuti oleh Microsoft dengan *"windows"*-nya. Disini ditawarkan penggunaan komputer yang betul-betul mudah, karena pemakai komputer tinggal menekan tombol – tombol yang tersedia. Namun dalam perkembangannya pemakai komputer masih belum puas hanya melihat komputer, sehingga diciptakanlah perangkat lunak dan perangkat keras untuk pemakaian audio, video pada komputer sehingga munculah era "Multimedia".

Multimedia merupakan teknologi komputer yang sedang berkembang pesat, selain internet, seiring dengan perkembangan komputer pribadi (*personal computer*). Ribuan perusahaan di seluruh dunia telah memanfaatkan teknologi multimedia untuk memasarkan produk perusahaan mereka, jutaan *programmer* (pembuat program) mereka perangkat lunak multimedia berupa permainan. Juga untuk CAL/CAI (*Computer Aided Learning / Computer Aided Instruction*) program untuk belajar dengan bantuan program komputer baik matematika, fisika, merakit komputer, mempelajari jalan sebuah kota. Atau sekedar sebagai media penyampai informasi seperti perumahan yang telah dijadikan contoh permasalahan diatas, atau mungkin hotel, pertokoan dan sebagainya.

2.2.4. Obyek – Obyek Multimedia

Terdapat lima elemen atau obyek yang utama dalam multimedia, yaitu teks, grafik, audio, video dan animasi. Selain dari itu, interaktifitas juga merupakan sebagian dai obyek yang diperlukan bagi kelengkapan proses

komunikasi interaktif menerusi penggunaan multimedia. Setiap obyek ini mempunyai peranannya sendiri dalam mewujudkan satu persembahan informasi yang lebih menarik dan berkesan. Berikut merupakan penerangan ringkas setiap objek tersebut dan hubungannya dengan era digital.

1. **Teks**

   Teks secara umum merupakan huruf-huruf yang tersusun untuk membentuk suatu makna yang akan dipahami dan memberikan pengertian tertentu. Teks sendiri terdiri dari jenis symbol, huruf abjad, nomor dan sebagainya. Teks dapat membentuk kata, surat atau narasi dalam mutimedia yang menyajikan bahasa. Kebutuhan teks bergantung pada kegunaan aplikasi multimedia.

   Dalam suatu system multimedia interaktif, teks menjalankan peranan yang sangat penting dalam menyalurkan suatu informasi kepada pengguna. Apabila penggunaan elemen-elemen lain gagal dalam menyampaikan keterangan yang diberikan kepada pengguna, maka dengan adanya teks akan membantu dalam penyampaian keterangan atau informasi yang ada. Dan penggunaan teks juga akan lebih menarik apabila digabungkan dengan elemen-elemen multimedia yang lain. Dan penggunaan elemen ini akan menjadikan keterangan yang akan dipaparkan lebih menarik, tepat dan menyeluruh.

2. **Grafik**

   Grafik dapat diartikan sebagai suatu gambar yang melambangkan sesuatu keadaan. Alasan untuk menggunakan gambar dalam presentasi atau publikasi multimedia adalah lebih menarik perhatian dan dapat mengurangi kebosanan dibanding dengan teks. Gambar dapat meringkas dan menyajikan data kompleks. Multimedia dapat membantu untuk melakukan hal tersebut yakni ketika gambar grafis menjadi obyek sesuatu. Grafis dapat digunakan sebagai latar belakang suatu teks untuk menghadirkan kerangka yang memperindah teks. Gambar juga bisa bertungsi sebagaia ikon yang bisa dipandu dengan teks, menunjukkan berbagai opsi yang bisa dipilih.

3. **Audio / Suara**

Animasi yang baik biasanya dilengkapi dengan suara. Macromedia Flash dapat memberikan latar musik atau musik yang dijalankan seiring dengan animasi. Dalam Macromedia Flash ada dua macam suara, yaitu:

1. *Event Sound* yang harus didowload semua, kemudian baru dijalankan secara terus menerus sampai ada perintah berhenti.
2. *Steram Sound* yang akan dijalankan setelah ada beberapa paket data yang telah diperoleh dan ini cocok sekali untuk membuat sinkronisasi suara dengan *time line*.

Untuk memasukkan suara dilakukan dengan mengkonversi teks suara, kemudian memilih berbagai macam format suara seperti WAV (untuk Window), AIFF (untuk Macintosh), atau MP3 (untuk window atau Macintosh). Flash secara otomatis akan menyimpan suara tersebut ke dalam pustaka bersama dengan gambar *bitmap* dan symbol. Kualitas suara dapat ditentukan dengan berbagai macam format kompresi suara yang ada sehingga ukuran besar *Flash* menjadi lebih kecil.

4. **Animasi**

Animasi dapat berupa simulasi pergerakan yang diciptakan dengan memperlunjukkan rangakaian gambar. Adapun perbedaan antara animasi dengan video adalah video mengambil gambar gerak secara langsung dan menjadikannya dalam bentuk *frame-frame* yang di-skrit, sedangkan animasi dimulai dengan gambar-gambar yang bebas dan menempatkan mereka bersama-sama ke bentuk ilusi gerak langsung. Animasi yang sering kita lihat dihasilkan dari sederetan gambar diam yang berurutan. Gerak gambar animasi dihasilkan dari suatu rangkaian gambar diam yang tersusun dalam suatu urutan perbedaan gerak yang minim. Dengan demikian model animasi diartikan sebagai cara "menghidupkan" benda atau konsep yang mati atau abstrak sehingga mudah dipahami. Animasi dibuat dari gambar yang dimasukkan melalui *scanner*, gambar tangan maupun dari program-program aplikasi untuk menggambar seperti *freehand*, *Corel Draw*, *Adobe Photoshop*, *Adobe Illustrator* dan lain-lain. Dalam multimedia, animasi merupakan penggunaan komputer untuk menciptakan gerak pada layar.

Beberapa jenis animasi yang sering dipakai adalah sebagai berikut :

1. **Animasi Sel** ***(Cell Animation)***

   Sel animasi biasanya merupakan lembaran-lembaran yang membentuk sebuah frame animasi tunggal. Sel animasi merupakan sel yang terpisah dari lembaran latar belakang dan sebuah sel untuk masing-masing obyek yag bergerak secara mandiri di atas latar belakang. Lembaran-lembaran ini memungkinkan untuk memisahkan dan menggambar kembali bagian-bagian gambar yang berubah antara frame yang berurutan. Sebuah frame terdiri dari sel latar belakang dan sel di atasnya. Misalnya ingin membuat karakter yang berjalan, pertama-tama menggambar lembaran latar belakang, kemudian membuat karakter akan berjalan pada lembaran berikutnya, selanjutnya membuat karakter ketika kaki diangkat dan akhirnya membuat karakter kaki dilangkahkan. Diantara lembaran – lembaran *(frame – frame)* dapat disisipi efek animasi agar karakter berjalan mulus. *Frame – frame* yang digunakan untuk menyisipi celah-celah tersebut disebut *key frame*. Selain dengan *key frame*, proses dan terminologi animasi sel dengan *layering* dan *tweening* dibuat dengan animasi komputer.

2. **Animasi Frame** ***(Frame Animation)***

   Animasi frame adalah bentuk animasi yang paling sederhana. Diumpamakan sebuah buku yang mempunyai gamabr berseri di tepi halaman berurutan. Bila jempol membuka buku dengan cepat, maka gambar kelihatan bergerak. Pada komputer multimedia, animasi buku tersebut menampilkan sebuah gambar yang berurutan.

3. **Animasi Sprite** ***(Sprite Animation)***

   Animasi sprite serupa dengan teknik animasi tradisional, yaitu objek yang diletakkan dan dianimasikan pada bagian puncak grafik dengan latar belakang diam. Sprite adalah setiap bagian dari animasi yang bergerak secara mandiri, misalnya burung terbang, planet berotasi, bola memantul-mantul atau logo berputar. Sprite beranimasi dan bergerak sebagai obyek yang mandiri.

   Dalam animasi sprite, sebuah gambar tunggal atau berurutan dapat ditempelkan dalam sprite. Sprite dianimasikan dalam suatu tempat, seperti halnya pelnet berputar atau burung bergerak sepanjang garis lurus. Animasi sprite berbeda

dengan animasi frame. Dalam urutan masing-masing frame, hanya dapat memperbaiki dari layar yang mengandung sprite tidak dapat memperbaiki bagian dalam yang ditampilkan layar untuk masing-masing frame, seperti yang dapat dikerjakan pada animasi frame.

4. Animasi Karakter (*Character Animation*)

Animasi karakter merupakan sebuah cabang khusus animasi. Animasi ini berbeda dengan animasi lainnya, misalnya grafik bergerak animasi logo yang melibatkan bentuk organik yang komleks dengan penggandaan yang banyak, gerakan yang hirarkis. Tidak hanya mulut, mata, muka dan tangan yang bergerak tetapi semua gerakan pada waktu yang sama.

5. Action Script

Action script merupakan bahasa pemrOgraman yang modular. Maksudnya, script-script merupakan modul-modul kecil untuk melakukan hal yang luar biasa, seperti memainkan atau menghentikan suatu film. Setiap modul berdiri sendiri tetapi digabungkan bersama-sama menjadi animasi film flash. Pada *Action Script*, script dapat bersifat tidak sederhana dan kompleks. *Action Script* menggunakan pemrograman *Object Oriented (Object Oriented Programming/ OOP)*. Pendekatan yang dilakukan pada action script adalah menganggap elemen dalam suatu program sebagai objek.

2.3 Perangkat Lunak Pendukung

Dengan perkembangan perangkat lunak atau software seperti sekarang ini. Khususnya perangkat lunak yang menunjang untuk membuat aplikasi mutimedia sudah banyak dijumpai. Dengan adanya alasan tersebut maka sebuah perangkat lunak dituntut untuk dapat berinteraksi dengan pemakai, yang mempunyai tingkat kesulitan dan kesalahan yang sedikit dan dapat membantu pemakai dalam suatu persoalan dengan hasil yang diinginkan, dapat menimbulkan rasa puas, tertarik dan rasa ingin mengetahui dan mempelajari perangkat lunak aplikasi tersebut.

Masalah yang sering muncul adalah kesulitan menjalankan perangkat lunak tersebut bagi pemakai pemula, hal itu akan menimbulkan rasa kurang

tertarik atau kurang berminat terhadap perangkat lunak tersebut. Untuk itu, dikembangkan perangkat lunak aplikasi dengan antarmuka yang dikenal dengan GUI (graphical user interface). GUI adalah suatu media antarmuka yang memungkinkan seorang pengguna dapat melakukan komunikasi atau dapat berinteraksi dengan komputer, dengan fasilitas GUI user dapat mudah merasakan berbagai kemudahan dalam mengoperasikannya, serta dapat menimbulkan rasa ingin tahu dan ingin mempelajarinya lebih dalam tentang perangkat dengan aplikasi multimedia.

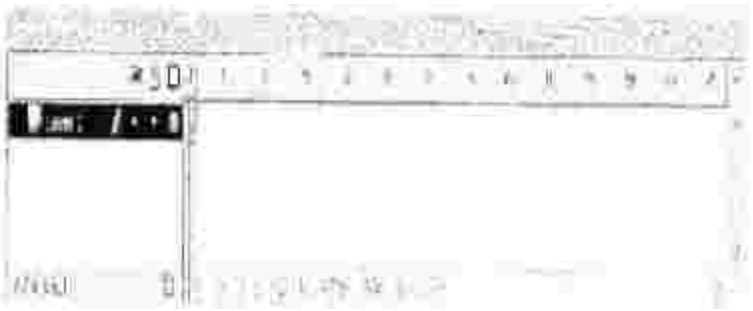
Untuk pembangunan aplikasi dalam peta digital berbasis multimedia ini digunakan aplikasi animasi developer Macromedia Flash Professional 2008. Macromedia Flash merupakan salah satu produk dari Macromedia yang merupakan program pembuatan animasi yang terintegrasi. Dewasa ini program Macromedia menjadi salah satu program populer untuk pengembangan aplikasi animasi. Satu hal yang menjadikan Macromedia Flash program yang populer adalah kemudahan pengoperasiannya dengan hasil yang sangat optimal dan lingkungan kerja yang terintegrasi dengan fitur yang lengkap.

2.3.1. Macromedia Flash Professional 8

Macromedia Flash Professional 8 adalah salah satu produk dari macromedia, yang merupakan program pembuatan animasi. Macromedia Flash Professional 8 menjadi salah satu program populer dalam pembuatan animasi, baik untuk keperluan Web, ataupun yang lainnya. Animasi bisa didefinisikan sebagai proses perubahan bentuk atau properti objek yang ditampilkan dalam suatu pergerakan transisi dalam suatu kurun waktu. (*A. Zaenaul Fanani. 2006)* Sedangkan lembar kerja yang akan ditemui dalam software ini diantaranya, yaitu:

1. Jendela kotak – kotak yang mempresentasikan frame.

   Jendela *Timeline* digunakan untuk mengorganisasi dan mengontrol pemutaran movie Flash. *Frame – frame* di dalam jendela *Time line* merupakan tempat objek movie ditampilkan.



Gambar 21 : Tampilan Timeline pada Macromedia Flash Professional 8

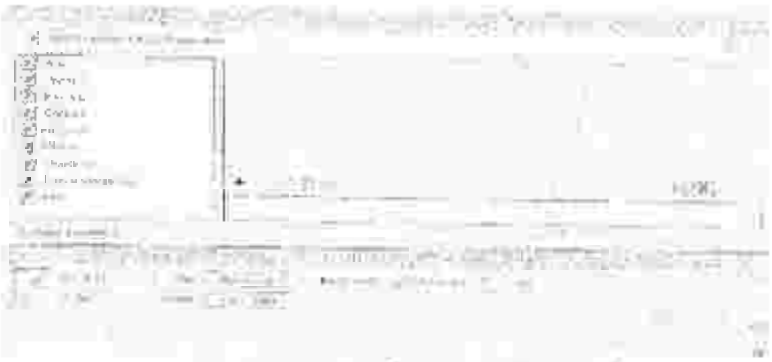
2. Jendela pengaturan opsi tool.

Di dalam movie Flash, terdapat berbagai tipe objek yang masing-masing mempunyai karakteristik pengeditan yang berbeda, dengan itu bisa memanfaatkan beberapa macam di dalam tool.

Gambar 22: Tampilan pengaturan opsi tool

3. Jendela – Jendela Panel Actions

Panel Actions digunakan untuk menulis dan mengelola actions. Actions dapat diterapkan pada frame, button, atau movie clip.



Gambar 2.3: Tampilan Jendela Panel Actions

2.3.2. Cool Edit Pro

Sedangkan untuk pengeditan audionya sendiri penulis menggunakan software utama *Cool Edit Pro*. *Cool Edit Pro* adalah software yang digunakan untuk mengedit file –file yang berekstensi mp3, wav, cda, dan sebagainya yang mendukung format suara. Dengan software ini penulis dapat menggabungkan suara dalam hal ini lagu yang satu dengan lagu yang lainnya, dan berbagai efek yang bisa digunakan dalam cool edit pro (www. ilmukomputer. com/*penggabunga-dua-lagu-dengan-cool-edit-pro*).

Sedangkan lembar kerja yang akan ditemui dalam software Cool Edit Pro 2.0 ini diantaranya yaitu:

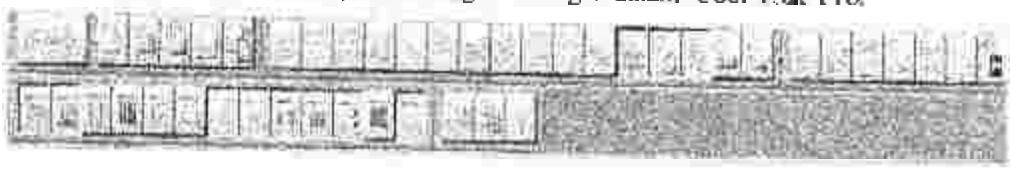
1. Jendela Organizer Windows

   Berfungsi untuk menampilkan file – file yang digunakan dalam proses pengeditan.

Gambar 2.4: Tampilan Jendela Organizer Windows

2. Jendela Multitrack

Berfungsi untuk menampilkan fungsi – fungsi dalam Cool Edit Pro.



Gambar 25: Tampilan Jendela Multitrack

3. Jendela Playback

Berfungsi untuk memainkan atau seperti fungsi playback pada umumnya.

Gambar 26: Tampilan Jendela Play back

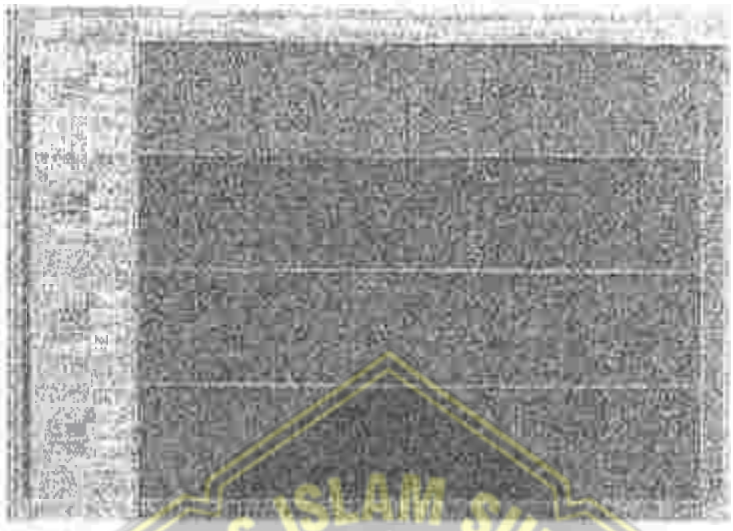
4. Jendela Effect Control

Berfungsi untuk menampilkan effect – effect yang dapat digunakan dalam proses pengeditan.

Gambar 27: Tampilan Jendela Effect Control

5. Jendela Kerja Multitrack

Berfungsi untuk menampilkan file – file yang diedit.



Gambar 28: Tampilan Jendela Multitrack

2.4. Sekilas Penjelasan Algoritma RSA dan Algoritma Knapsack

2.4.1. Algoritma RSA

A. Sejarah

Algoritma ini dikembangkan oleh Rivest, Adi Shamir, dan Len Adleman pada tahun 1977. Algoritma ini sekaligus menjawab tantangan dari sebuah paper yang dibuat oleh Diffe dan Hellman tentang pendekatan baru mengenai algoritma kriptografi yang dapat memenuhi kebutuhan untuk metode kunci publik. Algoritma Rivest Shamir (RSA) ini adalah metode kunci yang paling banyak dipakai sampai saat ini.

B. Konsep Dasar Algoritma RSA

1. Pengertian

Algoritma RSA merupakan algoritma kriptografi kunci publik (asimetris). Dimana salah satu dari kriptografi kunci publik yang sering digunakan untuk memberikan pengamanan data sehingga data tidak bisa dibaca oleh pihak yang tidak berhak. **Keamanan enkripsi / dekripsi data model ini** terletak pada kesulitan untuk memfaktorkan modulus n yang sangat besar, sehingga ketika

kriptografi kunci publik dengan algoritma RSA mau dipecahkan oleh pihak yang tidak berhak, maka mereka akan kesulitan dalam mencari faktor- faktor primanya dalam nilai yang besar. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. Kunci publik boleh diketahui oleh siapa saja, dan digunakan untuk proses enkripsi. Sedangkan kunci rahasia hanya pihak-pihak tertentu saja yang boleh mengetahuinya, dan digunakan untuk proses dekripsi. Sandi RSA terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Sebelumnya diberikan terlebih dahulu beberapa konsep perhitungan matematis yang digunakan RSA.

2. Proses Pembentukan Kunci

Berikut ini adalah proses pembentukan kunci. Proses ini dilakukan oleh pihak penerima, dalam hal ini adalah B.

a. Pilih bilangan prima p dan q
b. Hitung $\phi(n) = (p-1)(q-1)$
c. Pilih sembarang bilangan e, $1<e< \phi(n)$. Dimana $gcd(e,\phi(n))= 1$
d. Hitung invers dari e yaitu d, $de = 1 \bmod n$
e. e adalah kunci publik dan d adalah kunci private

3. Proses Enkripsi dan Dekripsi

a. Enkripsi

- Mengambil kunci publik penerima pesan, e, dan modulus n
- Menyatakan plainteks m menjadi blok-blok m1, m2, ..., sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang [0, n- 1]
- Setiap blok m1 dienkripsi menjadi blok ci dengan rumus $ci = ml^e \bmod n$.

b. Dekripsi

Setiap blok cipherteks m_i dienkripsi menjadi blok c_i dengan rumus $c_i = m_i^e \bmod n$.

2.4.2. Algoritma Knapsack

A. Sejarah Merkle-Hellman Knapsack Kriptosistem

Merkle-Hellman Knapsack merupakan Kriptosistem yang dibuat oleh Merkle dan Hellman pada tahun 1980 Walaupun sistem ini, dan beberapa variannya, telah dipecahkan sekitar awal tahun 1980, tetapi masih layak untuk dipelajari dengan berbagai alasan. Masalah yang mendasari matematika adalah masalah penjumlahan himpunan bagian dimana sangat berhubungan dengan masalah knapsack dari operasi pencarian (dengan demikian, "Knapsack" dalam nama dari system ini merupakan misnomer). Suatu masalah bisa didekripsikan sebagai berikut. Jika setiap elemen dari himpunan S adalah suatu bilangan integer positif. Diberikan suatu himpunan bagian dari S, penjumlah dari elemen terdekat dari bagian himpunan bilangan menghasilkan bilangan integer yang berkoresponden dengan himpunan bagiannya. Masalah penjumlahan himpunan bagian adalah kebalikannya, untuk itu, diberikan bilangan integer T, apakah ada himpunan bagian dari S yang dijumlahkan sama dengan T? Penyelesaian masalah ini (hanya membutuhkan respon ya atau tidak) apakah NP merupakan masalah yang lengkap. Selanjutnya adalah hubungan dengan pencarian masaluh, diberikan suatu T yang mana jawabannya adalah Ya, cari suatu himpunan bagian (atau himpunan-himpunan bagian, jawabannya tidak mungkin unik) yang merupakan hasil jumlah. Seperti dengan masalah NP apapun, meskipun itu adalah bukan algoritma polynomial untuk penyelesaian masalah secara umum. Beberapa soal mungkin bisa terselesaikan dengan mudah. ini adalah soal dengan masalah himpunan penjumlahan. Dan memperolehkan pencarian dari suatu trapdoor. Disini akan merumuskan suatu masalah. sebagai contoh : diberikan $s1,s2,,sn$ adalah himpunan bilangan positif (ukuran pemanggilan) dan T adalah bilangan positif, penyelesaian masalah adalah dengan mencari suatu vector0-1 $(x_1,x_2,..,xn)$ yang dapat dinyatakan sebagai berikut:

$$x1s1 + x2s2 + .. + xnsn = T. \qquad (2.1)$$

B. Konsep Dasar Algoritma Knapsack

1. Pengertian

Algoritma knapsack adalah algoritma kriptografi kunci publik. Knapsack artinya karung/kantung, karung mempunyai kapasitas muat terbatas. Barang-barang dimasukkan ke dalam karung hanya sampai batas kapasitas muat maksimum karung saja.

Keamanannya terletak pada sulitnya memecahkan persoalan knapsack (knapsack problem).

2. Knapsack problem

Bobot knapsack adalah M. Diketahui n buah objek yang masing-masing bobotnya adalah $s_1, s_2, ..., s_n$. Jadi rumusnya sebagai berikut :

$$T = x_1 s_1 + x_2 s_2 + ... + x_n s_n \qquad (2.2)$$

Setiap bobot s_i di dalam persoalan *knapsack* merupakan kunci privat, sedangkan bit-bit plainteks menyatakan x_i. Dimana dalam hal ini, x_i bernilai 0 atau 1. Jika $x_i = 1$, berarti objek i dimasukkan ke dalam *knapsack*, sebaliknya jika $x_i = 0$, objek i tidak dimasukkan.

3. Algoritma Knapsack Kunci-Publik

Algoritma *superincreasing knapsack* adalah algoritma yang lemah, karena cipherteks dapat didekripsi menjadi plainteksnya secara mudah di dalam waktu lanjar (0(n)). Algoritma *non-superincreasing knapsack* atau *normal knapsack* adalah algoritma knapsack yang sulit karena membutuhkan waktu dalam orde eksponensial untuk memecahkannya. Namun, *superincreasing knapsack* dapat dimodifikasi menjadi *non-superincreasing knapsack* dengan menggunakan kunci publik (untuk enkripsi) dan kunci privat (untuk dekripsi). Kunci publik merupakan barisan *non-superincreasing knapsack* sedangkan kunci privat merupakan barisan *superincreasing knapsack*.

Algoritma untuk membangkitkan kunci publik dan kunci privat:

- Menentukan barisan superincreasing
- Mengalikan setiap elemen di dalam barisan tersebut dengan n modulo m. Modulus m seharusnya angka yang lebih besar daripada jumlah

semua elemen di dalam barisan, sedangkan pengali n seharusnya tidak mempunyai vaktor persekutuan dengan m.

- Hasil perkalian akan menjadi kunci publik sedangkan barisan superincreasing semula menjadi kunci privat.

4. Proses Enkripsi Knapsack
   a. Pesan plaintext *P* bisa dituliskan dalam bentuk: *P* = [p1, p2,..., p*k*].
   b. Membagi pesan ke dalam blok bit-bit *m*, P0 = [p1, p2,..., p*m*], P1 = [p*m*+1,..., p2*m*], dan selanjutnya. (*m* adalah bilangan pembatas dalam knapsack)
   c. Mengalikan setiap bit di dalam blok dengan elemen yang berkoresponden di dalam kunci publik.
   d. Nilai ciphertext merupakan: *P i**t, target menggunakan blok *Pi* untuk memilih vector.
5. Proses Dekripsi Knapsack
   a. Dekripsi dilakukan dengan menggunakan kunci privat. Mula-mula penerima pesan menghitung nilai n-1, yaitu inversi n modulo m, sedemikian sehingga *n.n*-1 = 1 (mod m).
   b. Mengalikan setiap kriptogram dengan n-1 mod m, lalu menyatakan hasil kalinya sehingga penjumlahan elemen-elemen kunci privat untuk memperoleh plainteks dengan menggunakan algoritma pencarian solusi supercreasing knapsack.

2.5. Kurikulum Kriptografi Teknik Informatika

Dalam perancangan pembelajaran ini, materi yang disajikan berdasarkan Kurikulum Jurusan Teknik Informatika tahun 2008, agar dalam pembahasannya tidak menyimpang dan lebih terstruktur. Berikut penjabaran dari kurikulum Keamanan Data :

Standar Kompetensi: Menggunakan Kurikulum Algoritma RSA dan Algoritma Knapsack

Tabel2.1 Kurikulum Algoritma RSA dan Algoritma Knapsack

Kompetensi Dasar	Indikator	Pengalaman Pembelajaran	Materi Ajar	Sumber alat/bahan ajar	Penilaian
Memahami dan memiliki wawasan tentang konsep dan sejarah kriptografi kunci publik, serta beberapa jenis kriptografinya	- menjelaskan konsep dan sejarah kriptografi kunci publik - menjelaskan beberapa kriptografi kunci publik	- Menjelaskan konsep, dan sejarah kriptografi kunci publik - Menjelaskan RSA - Menjelaskan Algoritma Knapsack	- Konsep kripografi Kunci Publik - Sejarah Kriptografi Kunci Publik - Algoritma RSA - Algoritma Knapsack	OHP, Projector In Focus, Laptop. "Kriptografi" karangan Rinaldi Munir, Penerbit Informatika Bandung.	Partisipasi kelas, dan presentasi

Berdasarkan kurikulum yang telah dipaparkan diatas, maka materi dalam perancangan pembelajaran ini mengacu pada kurikulum tersebut.

2.6. Desain Sistem

2.6.1. Ide Cerita

Seperti yang kita ketahui sebelum membuat suatu aplikasi system keamanan dengan menggunakan kriptografi, haruslah mengerti benar konsep dan langkah-langkah di dalam algoritma yang digunakan, terutama proses enkripsinya. Mempelajari sebuah proses enkripsi pada sebuah algoritma tidaklah mudah, media yang sering digunakan adalah buku. Akan tetapi untuk membaca dan memahami sebuah algoritma di dalam sebuah buku tidaklah cukup menyenangkan dan seringkali membosankan. Karena itulah muncul gagasan perancangan pembelajaran sebagai alat bantu untuk mempelajari algoritma pada kriptografi.

2.6.2. Alur Cerita (Narasi)

Alur cerita pada media pembelajaran ini sebagai berikut :

1. Pembukaan atau Opening

Pada pembukaan atau opening, pertama kali ditampilkan loadig complete yang tujuannya adalah agar lebih menarik yang kemudian dilanjutkan dengan tampilan beberapa gambar animasi yang berkaitan dengan kriptografi.

2. Menu Utama

Pada bagian menu Utama, terdapat beberapa tombol pilihan untuk masuk pada bagian materi yang akan dipelajari. Tombol – tombol tersebut yaitu:

a. Tombol RSA

Pada tombol RSA ini menjelaskan tentang algoritma RSA, diantaranya sejarah konsep dasar algoritma RSA dan simulasi algoritma RSA dimana simulasi tersebut menjelaskan alur proses enkripsi dan dekripsi pada algoritma RSA .

b. Tombol Knapsack

Begitu halnya seperti pada tombol Knapsack menjelaskan tentang algoritma Knapsack, diantaranya sejarah,konsep dasar algoritma Knapsack dan simulasi algoritma Knapsack dimana simulasi tersebut menjelaskan alur proses enkripsi dan dekripsi pada algoritma Knapsack.

c. Tombol Replay (Ulangi)

Pada tombol replay ini yang terdapat pada simulasi algoritma RSA dan algoritma knapsack yang digunakan jika ingin mengulang simulasi tersebut.

d. Tombol Intro

Pada tombol Intro untuk kembali ke menu pembukaan atau opening.

e. Tombol Exit (Keluar)

Pada tobol Exit untuk keluar dari pembelajaran, dimana pada tombol Exit ini apakah anda yakin akan keluar atau tidak? jika "Ya" maka akan keluar dan jika "Tidak" maka akan kembali pada menu utama.

BAB III
PERANCANGAN DAN PEMBUATAN SISTEM

3.1. Perancangan Sistem

3.1.1. Analisa Kebutuhan Sistem

Sebelum membuat program, perlu dilakukan beberapa tahapan pembuatan program supaya hasil program yang dibuat akan lebih berhasil dan bermanfaat. Adapun tujuan tahap – tahap dalam penyusunan suatu program adalah untuk mempermudah penyusunan program dan pengembangan program selanjutnya.

Sumber informasi tidak lagi berfokus pada teks dari buku semata tetapi lebih luas dari itu. Buku memang sangat praktis digunakan, tetapi buku juga memilki kelemahan, yaitu pembelajaran dengan menggunakan media buku ini nampaknya sulit dipahami dan membosankan. Penelitian De Porter mengungkapkan manusia dapat menyerap suatu materi sebanyak 70% dari apa yang dikerjakan, 50% dari apa yang didengar dan dilihat (audio visual), sedangkan dari yang dilihatnya hanya 30%, dari yang didengarnya hanya 20%, dan dari yang dibaca hanya 10%.

Untuk menghindari masalah-masalah tersebut, maka perlu dibuat metode pembelajaran baru yang lebih menarik dan menyenangkan. Karena itulah, timbul suatu gagasan penulis untuk membuat perancangan pembelajaran kriptografi yang menjelaskan materi algoritma RSA dan algoritma Knapsack. Dengan adanyapembelajaran ini diharapkan pengguna khususnya mahasiswa dapat diajak untuk berinteraksi sambil belajar sehingga mereka tidak cepat bosan dan merasa *fun* saat belajar Kriptografi di rumah.

3.1.2. Analisa Kebutuhan Pengguna

Kebutuhan pengguna perlu diperhatikan supaya aplikasi ini dapat memberikan kemudahan dan kenyamanan bagi pengguna, yaitu :

1. Tampilan program dibuat semenarik mungkin
2. Navigasi menu yang sederhana dan tidak rumit
3. Adanya audio yang dalam bentuk musik ini agar *user* tidak membosankan.

3.2. Pemilihan Alat dan Bahan

3.2.1. Spesifikasi Kebutuhan Sistem

Tahap awal sebelum perancangan suatu program aplikasi ini adalah menentukan spesifikasi kebutuhan system. Spesifikasi kebutuhan system yang akan dibangun yaitu:

1. Program aplikasi pembelajaran interaktif berisi tentang materi algoritma RSA yang mempelajari tentang sejarah, konsep dasar, dan simulasi algoritma RSA, dan algoritma Knapsack yang terdiri dari sejarah, konsep dasar, dan simulasi algoritma Knapsack.
2. Aplikasi pembelajaran interaktif membantu mahasiswa yang mengalami kesulitan dalam memahami pembelajaran kriptografi khususnya pada algoritma RSA dan algoritma Knapsack.
3. Aplikasi ini disertai dengan user interface atau antarmuka yang diharapkan sangat mudah digunakan dari sudut pandang pengguna (mahasiswa).

3.2.2. Spesifikasi Kebutuhan Alat

1. Komputer

Spesifikasi komputer yang akan digunakan penulis untuk proses aplikasi ini adalah :

a. Sistem Operasi Windows XP
b. Processor Intel Pentium Dual-Core T4200 (2.0 GHz, 800 MHz FSB, 1 MB L2 cache)
c. Memory DDR2 1 GB
d. Hard Disk 250GB
e. Mobile Intel Graphics Media Accelerator 4500MHD
f. Monitor 14.1'' WXGA Acer CrystalBrite.
g. Headset Quenn

Spesifikasi minimal untuk pengguna dalam proses pembuatan aplikasi ini dengan cara memasukkan CD – ROOM yaitu :

a. Sistem Operasi Windows XP
b. Processor Intel Pentium III

c. CD–ROOM

d. Memory 128 Mb RAM

e. Sound Card on Board

f. VGA Card

g. Mouse

h. Keyboard

i. Monitor

Perancangan perangkat lunak (*software*) pembuatan media pembelajaran berbasis multimedia ini menggunakan platform system operasi Windows dengan konfigurasi minimal Microsoft XP. Untuk pengembangan elemen – elemen multimedia lainnya digunakan program aplikasi pengolahan gambar, video, dan suara serta penggunaan efek yaitu Macromedia Flash Professional 8 untuk pembuatan animasi.

2.Video Animasi

Dalam pembuatan animasi diperlukan imajinasi yang tinggi yaitu menggunakan *software* untuk pembuatan animasi yaitu penulis menggunakan Macromedia Flash Professional 8, karena *software* ini menjadi salah satu program popular dalam pembuatan animasi, baik untuk keperluan Web, presentasi, game, ataupun yang lainnya.

3.2.3. Spesifikasi Kebutuhan Bahan

1. Animasi

   Animasi merupakan hal yang pokok dalam pembuatan media pembelajaran ini. Karena produk yang dihasilkan bisa dinikmati oleh para mahasiswa dan para pengajar (dosen).

2. Audio

   Audio merupakan bagian yang menunjang dalam sebuah film atau jenis video lainnya. Pemakaian audio dalam media pembelajaran ini berupa musik agar pembelajaran tersebut tidak membosankan.

3.3. Sistematika Perancangan

Dalam perancangan sistem diperlukan struktur program yang bertujuan untuk mendokumentasikan menjelaskan struktur aplikasi yang dibuat. Pirani bantu yang yang akan dibuat berupa navigasi. Sebuah peta navigasi atau *site map* biasanya merupakan daftar isi dengan hierarki yang sederhana dengan masing-masing *heading* terhubung ke sebuah halaman. Ada berbagai macam kombinasi dalam peta navigasi ini, diantaranya:

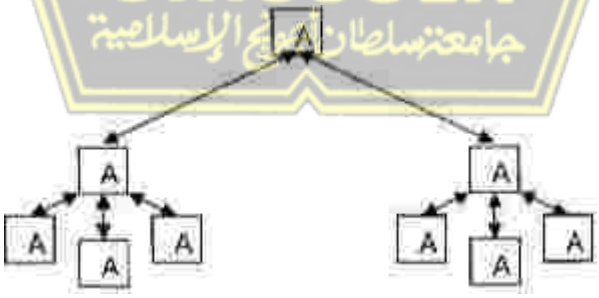
1. linier

   Pengguna melakukan navigasi secara berurutan, dari frame atau bite informasi satu ke yang lainnya.

Gambar 3.1 gambar navigasi linear

2. Hierarkis

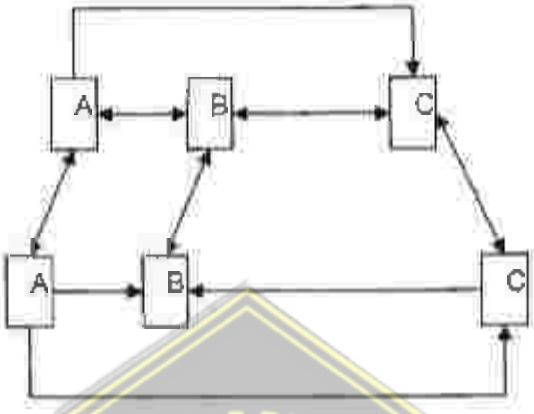
   Disebut juga "linier dengan percabangan", karena pengguna melakukan navigasi di sepanjang cabang pohin instrukter yang terbentuk oleh natural logic dari isi.



Gambar 3.2 gambar navigasi hierarchies

3. Nonlinier

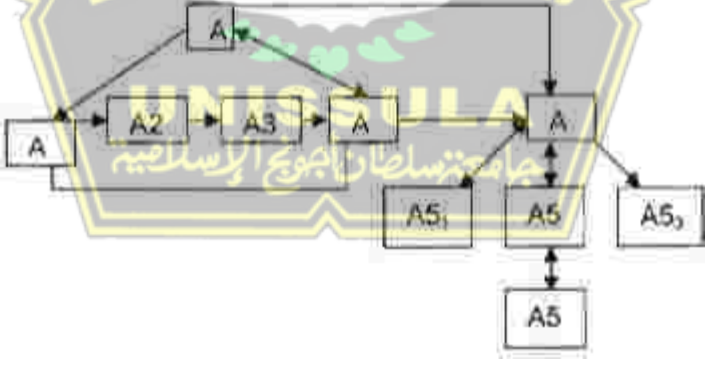
Pengguna melakukan navigasi dengan bebas melalui isi proyek, tidak terkait dengan rute yang telah ditetapkan sebelumnya.



Gambar 3.3 gambar navigasi nonlinier

4. Komposit

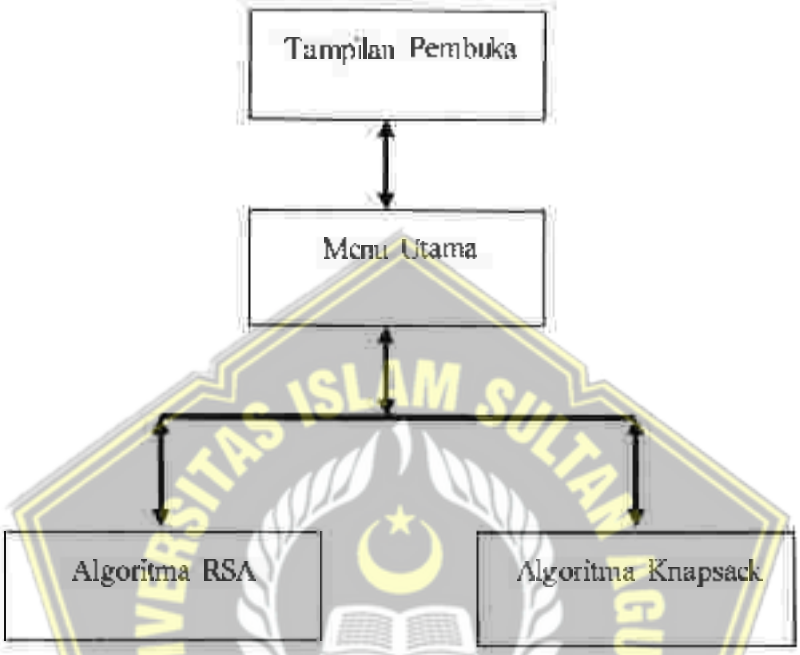
Pengguna melakukan navigasi dengan bebas (secara nonlinier), tetapi terkadang dibatasi oleh presentasi linier film atau informasi kritis dan atau pada data yang paling terorganisasi secara logis dalam suatu hierarki.



Gambar 3.4 gambar navigasi komposit

3.3.1 Sistematika Perancangan Menu Utama

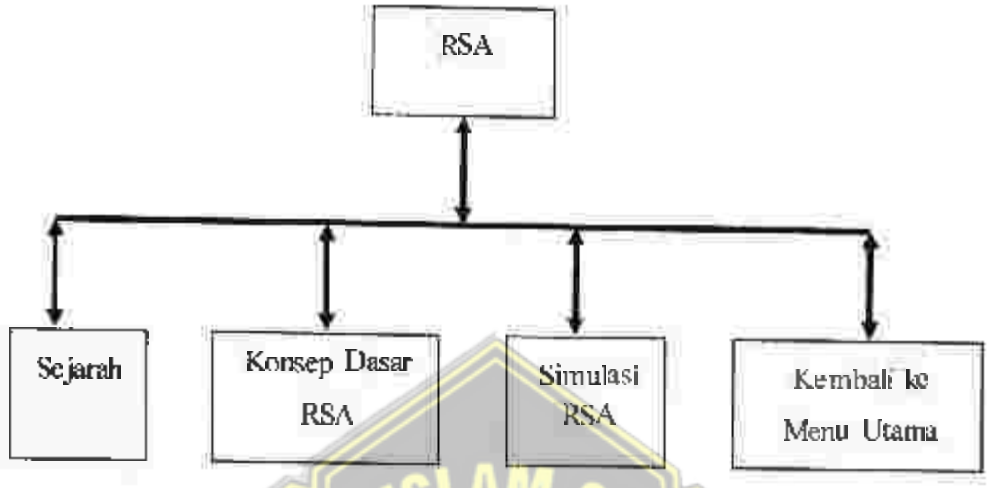
Berdasarkan dari penjelasan mengenai system navigasi diatas, maka dalam pembuatan media pembelajaran ini digunakan navigasi yang berbentuk Hierarkis. Gambaran rinciannya adalah sebagai berikut:



Gambar 3.5 : Struktur Menu Utama Sistem Pembelajaran Kriptografi

Diskripsi untuk Menu Utama adalah pada saat program dijalankan maka yang pertama kali ditampilkan adalah tampilan pembuka kemudian masuk pada menu utama dengan tombol Enter. Pada menu utama terdapat sub menu RSA, sub menu Knapsack, sub menu Intro untuk kembali ke menu utama, dan tombol Exit untuk mengakhiri program.

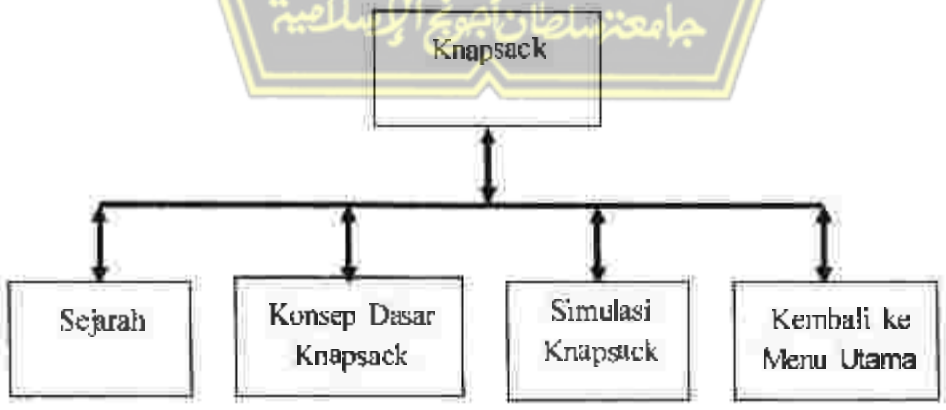
3.3.2. Sistematika Perancangan Sub Menu RSA



Gambar 3.6. Sub Menu Algoritma RSA

Dekripsi untuk Sub Menu RSA adalah mempelajari tentang sejarah, konsep dasar RSA, dan simulasi RSA (proses enkripsi dan dekripsi algoritma RSA). Disediakan tombol Replay pada tombol simulasi RSA untuk mengulangi simulasi tersebut. Untuk kembali pada halaman menu utama pilih tombol Intro.

3.3.3. Sistematika Perancangan Sub Menu Knapsack



Gambar 3.7: Sub Menu Algoritma Knapsack

Dekripsi untuk Sub Menu Knapsack adalah mempelajari tentang sejarah, konsep dasar Knapsack, dan simulasi Knapsack (proses enkripsi dan dekripsi algoritma Knapsack). Disediakan tombol Replay pada tombol simulasi Knapsack untuk mengulangi simulasi tersebut. Untuk kembali pada halaman menu utama pilih tombol Intro.

3.4. Naskah Dan Story Board

3.4.1. Skenario

Judul : "Media Pembelajaran Kriptografi (Algoritma RSA dan Algoritma Knapsack) Berbasis Multimedia"

Jenis Produk : Media Pembelajaran

Bila program dijalankan, maka pertama kali yang muncul adalah tampilan loading time tujuannya sebelum masuk pada menu pembuka diberi jangka waktu agar lebih menarik. Sebelum masuk pada Menu Utama, akan ditampilkan terlebih dahulu gambar-gambar yang berkaitan dengan kriptografi. Tekan tombol Enter untuk masuk pada Menu Utama. Pada Menu Utama di latar belakangi instrument lagu dan gambar Logo UNISSULA kemudian ditampilkan judul dari media pembelajaran dan diikuti oleh nama penyusun yang menarik dengan berbagai macam tombol di bawahnya. Tombol tersebut digunakan untuk masuk pada pokok bahasan materi. Tombol-tombol tersebut diantaranya:

1. Tombol RSA berisi materi tentang sejarah algoritma RSA, konsep dasar algoritma RSA, dan simulasi algoritma RSA yaitu dimana simulasi tersebut menjelaskan proses enkripsi dan dekripsi pada algoritma RSA. Dan pada simulasi terdapat tombol Replay tujuannya untuk mengulangi simulasi tersebut.
2. Begitu pula dengan tombol Knapsack berisi materi tentang sejarah algoritma Knapsack, konsep dasar algoritma Knapsack, dan simulasi algoritma Knapsack yaitu dimana simulasi tersebut menjelaskan proses enkripsi dan dekripsi pada algoritma Knapsack. Dan pada simulasi terdapat tombol Replay tujuannya untuk mengulangi simulasi tersebut.

3. Tombol INTRO untuk kembali ke halaman menu pembuka.
4. Tombol KELUAR untuk keluar dari pembelajaran. Diakhiri dengan peringatan "Anda yakin akan keluar?" jika Ya maka akan keluar dari pembelajaran dan jika Tidak maka akan kembali pada halaman menu utama.

Berikut tabel naskah pembelajaran Algoritma RSA dan Algoritma Knapsack:

Tabel 3.1 Naskah pembelajaran Algoritma RSA dan Algoritma Knapsack

DUBBING	" PEMBELAJARAN ALGORITMA RSA DAN ALGORITMA KNAPSACK "
	NEXT
	" Selamat datang di media pembelajaran kriptografi. Kali ini kita akan belajar algoritma RSA dan algoritma Knapsack. Apa kamu sudah siap? jika kamu sudah siap maka tekan tombol ENTER!"
	NEXT
	" Sekarang kamu berada pada menu utama. Kamu bisa pilih salah satu tombol yang ingin kamu pelajari. Pilih tombol RSA untuk belajar Algoritma RSA dan pilih tombol Knapsack untuk belajar Algoritma Knapsck."
	NEXT
	Algoritma RSA " Jika kamu ingin mengetahui sejarah pada algoritma RSA maka tekan tombol sejarah, jika ingin belajar konsep dasar pada algoritma RSA maka tekan tombol konsep dasar RSA, dan jika ingin belajar proses enkripsi dan dekripsi algoritma RSA maka tekan tombol simulasi RSA. "
	NEXT

Tabel 3.2(Lanjutan) Naskah pembulajaran Algoritma RSA dan Algoritma Knapsack

	Simulasi Algoritma RSA " Alice mengirimkan pesan atau plainteks berupa angka desimal kepada Roby dengan ketentuan plainteks dibagi menjadi blok-blok yang kemudian setiap blok-blok pada plainteks akan dienkripsi dengan rumus sebagai berikut.., atau yang biasa disebut cipherteks. kemudian sebelum melakukan proses dekripsi, Roby membangkitkan kunci publik dan kunci privat dengan rumus sebagai berikut.., baru kemudian menuju ke proses dekripsi dengan menggunakan kunci privat sehingga memperoleh kembali plainteks semula. Dan pesan atau plainteks dapat dibaca oleh Roby."
	NEXT
	Algoritma Knapsack " Jika kamu ingin mengetahui sejarah pada algoritma Knapsack maka tekan tombol sejarah, jika ingin belajar konsep dasar pada algoritma Knapsack maka tekan tombol konsep dasar Knapsack, dan jika ingin belajar proses enkripsi dan dekripsi algoritma Knapsack maka tekan tombol simulasi Knapsack.""
	NEXT
	Simulasi Algoritma Knapsack " Alice mengirimkan pesan atau plainteks dalam bentuk bit-bit kepada Roby dengan ketentuan plainteks dibagi menjadi blok-blok kemudian setiap bit di dalam blok dienkripsi yaitu dikalikan dengan elemen yang berkoresponden di dalam kunci publik atau hasil enkripsi tadi disebut cipherteks kemudian sebelum cipherteks tersebut didekripsi Roby membangkitkan kunci publik dan kunci privat dengan rumus sebagai berikut.., baru kemudian menuju ke proses dekripsi dengan menggunakan kunci privat sehingga memperoleh kembali plainteks semula. Dan pesan atau plainteks dapat dibaca oleh Roby."

3.4.2. Story Board

I. Perancangan Tampilan Pembuka Menu Utama

Sebelum masuk pada halaman menu utama, akan ditampilkan terlebih dahulu tampilan pembuka. Halaman menu utama adalah halaman yang terdapat seluruh tombol-tombol dimana jika tombol-tombol tersebut di pilih mempunyai sub-sub menu. Untuk masuk pada halaman menu utama maka harus menekan tombol ENTER.

Gambar 3.8: Halaman Pembuka

Script yang diberikan pada tombol ENTER adalah:

```
on (release){
gotoAndPlay(9);
}
```

Dimaksudkan untuk masuk ke dalam menu utama.

Agar pembahasan materi dan dubbing dapat bergantian secara teratur, maka scrip yang digunakan adalah:

```
loadMovieNum("utamasound.swf", 1);
stop();
stopAllSounds();
```

2. Perancangan Halaman Menu Utama

Halaman ini ditampilkan setelah halaman judul, di dalam menu utama ini terdapat tombol-tombol yang terdapat sub-sub menu. Disertai dengan sound effect dan juga dubbing agar lebih jelas.

Untuk masuk ke menu utama, harus menekan tombol ENTER yang ada pada tampilan pembuka. Scrip yang diberikan pada tombol ENTER adalah

```
on (release) {
gotoAndPlay(91);
}
```

Dimaksudkan untuk masuk ke dalam menu utama.

Gambar 39 : Halaman Menu Utama

Pada halaman menu utama terdapat empat tombol yang menunjukkan isi dari pembelajaran tersebut. Tombol-tombol tersebut adalah :

1. Tombol RSA berisi materi tentang sejarah algoritma RSA, konsep dasar algoritma RSA, dan simulasi algoritma RSA yaitu dimana simulasi tersebut menjelaskan proses enkripsi dan dekripsi pada algoritma RSA. Dan pada simulasi terdapat tombol Replay tujuannya untuk mengulangi simulasi tersebut.

2. Begitu pula dengan tombol Knapsack berisi materi tentang sejarah algoritma Knapsack, konsep dasar algoritma Knapsack, dan simulasi algoritma Knapsack yaitu dimana simulasi tersebut menjelaskan proses enkripsi dan dekripsi pada algoritma Knapsack. Dan pada simulasi terdapat tombol Replay tujuannya untuk mengulangi simulasi tersebut.
3. Tombol INTRO untuk kembali ke halaman menu pembuka.
4. Tombol KELUAR untuk keluar dari pembelajaran. Diakhiri dengan peringatan "Anda yakin akan keluar?" jika "Ya" maka akan keluar dari pembelajaran dan jika "Tidak" maka akan kembali pada halaman menu utama.

3. Perancangan Halaman Sub Menu RSA

Untuk bisa mempelajari materi algoritma RSA, pada halaman menu utama menampilkan tombol sub menu RSA yang akan mempelajari tentang sejarah algoritma RSA, konsep dasar algoritma RSA, dan simulasi algoritma RSA.

Berikut ini gambar tombol menu dan sub menu pada algoritma RSA:

Gambar 3.10: Tombol Menu RSA

Script yang diberikan untuk tombol RSA adalah:

```
on (release) {
gotoAndPlay(117);
}
```

Gambar 3.11 Tombol Sub Menu RSA

Pada halaman sub menu RSA ini ditampilkan beberapa tombol diantaranya sejarah, konsep dasar, simulasi algoritma RSA dan tombol Kembali. Untuk mempelajarinya, dapat memilih salah satu tombol yang berada dibawah maka akan masuk pada sejarah, konsep dasar, simulasi algoritma RSA. Berikut script yang diberikan untuk masing-masing pembahasan algoritmaRSA:

1. Sejarah Algoritma RSA

```
on (release) {
gotoAndStop(146);
}
```

Dimaksudkan untuk masuk pada materi sejarah RSA

Tombol Kembali untuk kembali pada halaman menu utama. *Script* yang diberikan :

```
on (release) {
gotoAndStop(116);
}
```

2. Konsep Dasar Algoritma RSA

```
on (release) {
  gotoAndStop(147);
}
```

Dimaksudkan untuk masuk pada materi Konsep Dasar Algoritma RSA

Tombol Kembali untuk kembali pada halaman menu utama. *Script* yang diberikan :

```
on (release) {
  gotoAndStop(116);
}
```

3. Simulasi Algoritma RSA

```
on (release) {
gotoAndStop(148);
}
```

Dimaksudkan untuk masuk pada materi Simulasi Algoritma RSA

Tombol Kembali untuk kembali pada halaman menu utama. *Script* yang diberikan

```
on (release) {
  gotoAndStop(116);
}
```

4. Perancangan Halaman Sub Menu Knapsack

Untuk bisa mempelajari materi algoritma Knapsack, pada halaman menu utama menampilkan tombol sub menu Knapsack yang akan mempelajari tentang sejarah algoritma Knapsack, konsep dasar algoritma Knapsack, dan simulasi algoritma Knapsack. Berikut ini gambar tombol menu dan sub menu pada algoritma Knapsack:

Gambar 3.12: Tombol Menu Knapsack

Script yang diberikan untuk tombol Knapsack adalah:

```
on (release) {
gotoAndPlay(150);
}
```

Ini dimaksudkan untuk masuk ke dalam tombol Knapsack

Gambar 3.13: Tombol Sub Menu Knapsack

Pada halaman sub menu Knapsack ini ditampilkan lebih sederhana dengan adanya beberapa tombol di bawahnya, diantaranya sejarah, konsep dasar algoritma Knapsack, simulasi algoritma Knapsack dan tombol Kembali. Untuk mempelajarinya, dapat memilih salah satu tombol yang berada dibawah maka

akan masuk pada sejarah, konsep dasar, simulasi algoritma Knapsack. Berikut script yang diberikan untuk masing-masing pembahasan algoritma Knapsack:

1. Sejarah Algoritma Knapsack

Script yang diberikan untuk tombol Sejarah Knapsack adalah:

```
on (release) {
gotoAndStop(179);
}
```

2. Konsep Dasar Knapsack

Script yang diberikan untuk tombol konsep dasar Knapsack adalah:

```
on (release) {
gotoAndStop(180);
}
```

3. Simulasi Knapsack

Script yang diberikan untuk tombol simulasi Knapsack adalah:

```
on (release) {
gotoAndStop(181);
}
```

5. Perancangan Tampilan Penutup

Pada halaman menu utama menampilkan tombol keluar untuk keluar dari program. Sebelum keluar dari program, akan ada pertanyaan yakin akan keluar dari program yang sedang dijalankan. Jika memilih "ya" maka akan keluar dari program, Jika "tidak" yang dipilih maka akan kembali pada halaman menu pembuka.

Gambar 3.14: Tombol Exit (Keluar)

Gambar 3.15: Tombol Yakin Keluar Atau Tidak

Script yang diberikan untuk tombol keluar adalah :

```
on (release) {
    //fscommand("quit",true);
    _root.gotoAndStop(2);
}
on (release) {
    exit.enabled=false;
    reset.enabled=false;
    knapsack.enabled=false;
    intro.enabled=false;
}
```

BAB IV
HASIL DAN ANALISIS

4.1 Desain Implementasi Aplikasi Media Pembelajaran Kriptografi Untuk Algoritma RSA dan Algoritma Knapsack

4.1.1. Halaman Tampilan Pembuka

Gambar 4.1 Loading Complete

Gambar 4.2, Halaman Menu Pembuka

1. Diskripsi Karya

Load complete pertama kali muncul pada pembelajaran ini yang menunjukkan loading sebelum menuju ke halaman menu pembuka. Kemudian ditampilkan halaman menu pembuka yaitu dengan tampilan gambar-gambar yang berkaitan dengan pembelajaran kriptografi.

2. Analisis Karya

Tampilan pada saat pertama kali program pembelajaran dijalankan berupa load komplete. Hal ini dimaksudkan untuk menunjukkan loading menuju halaman menu pembuka. Selanjutnya masuk pada tampilan halaman pembuka. Untuk masuk pada halaman menu utama diharuskan untuk memilih tombol ENTER yang berada di kiri gambar pengarang dan gambar yang berkaitan dengan kriptografi. Pada tombol ENTER diberikan script agar dapat masuk pada halaman menu utama.

4.1.2. Halaman Menu Utama

1. Tampilan Menu Utama

Gambar 43. Menu Utama

Gambar 4.4. Tombol Menu RSA

Gambar 4.5. Tombol Menu Knapsack

Gambar 4.6. Tombol Menu INTRO

Gambar 4.7. Tombol Menu EXIT

1. Diskripsi Karya

Halaman menu utama ditampilkan logo UNISSULA. Hal ini dimaksudkan untuk menunjukkan penyusun sebagai mahasiswi UNISSULA yang menyusun proyek ilmiah membuat media pembelajaran kriptografi algoritma RSA dan algoritma Knapsack. Selain itu ditampilkan judul proyek ilmiyah ini yang disertai nama penyusun proyek ilmiah ini. Pada halaman menu utama dibuat animasi semenarik mungkin agar mahasiswa menjadi lebih tertarik, yaitu dengan ditampilkannya berbagai macam tombol untuk masuk pada materi yang akan dipelajari. Terdapat tombol dengan tulisan RSA dan tombol dengan tulisan Knapsack. Dan terakhir terdapat tombol exit dan tombol intro. Tombol exit untuk mengakhiri progam pembelajaran dan tombol intro untuk kembali ke menu pembuka yang ditampilkan pertama kali.

2.Analisis Karya

Setelah menekan tombol ENTER, maka masuk pada halaman menu utama. Pada halaman menu utama terdapat dua tombol untuk masuk pada materi pembelajaran dan dua tombol yang lain untuk mengakhiri program yaitu Exit atau untuk kembali ke menu tampilan awal yaitu Intro. Kedua tombol tersebut memiliki sub menu-sub menu lagi.

Tombol pertama untuk masuk pada sub menu RSA. Masuk pada sub menu RSA akan ditampilkan beberapa tombol yang mempelajari tentang sejarah RSA, konsep dasar RSA, dan simulasi RSA. Pada tombol simulasi terdapat tombol Replay yaitu untuk mengulangi simulasi tersebut apabila kurang paham. Dengan script yang telah diberikan pada tombol RSA, maka akan masuk pada pembahasan RSA.

Tombol kedua adalah tombol untuk masuk pada sub menu Knapsack. Dengan script yang diberikan pada tombol Knapsack maka akan masuk pada pembahasan materi Knapsack. Pada sub menu ini akan mempelajari tentang sejarah RSA, konsep dasar RSA, dan simulasi RSA. Pada sub menu Knapsack ini akan diberikan empat tombol, yaitu tombol sejarah RSA untuk mengetahui sejarah algoritma RSA, tombol konsep dasar RSA untuk mempelajari algoritma RSA, tombol simulasi RSA untuk mempelajari simulasi atau proses enkripsi dan dekripsi pada algoritma RSA, dan tombol Kembali untuk kembali pada program awal atau halaman menu utama.

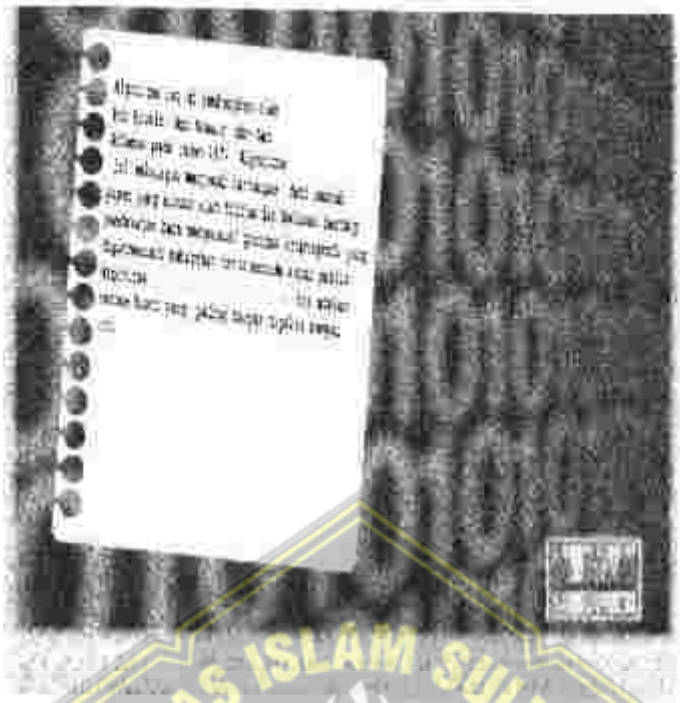
Tombol ketiga adalah tombol Intro yang fungsinya untuk kembali pada halaman menu pembuka. Tombol terakhir yang terdapat pada menu utama adalah tombol keluar. Apabila tombol ini dipilih, maka akan mengakhiri program. Tetapi sebelum keluar, akan ditanyakan apakah benar-benar akan keluar dari program. Jika "ya" yang dipilih, maka program akan selesai. Jika "tidak" dipilih, maka akan kembali pada program awal atau tampilan menu utama. Pada tombol keluar juga diberikan script agar program yang dikehendaki dapat berjalan.

4.1.3. Halaman Sub Menu Algoritma RSA

1. Tampilan Sub Menu RSA

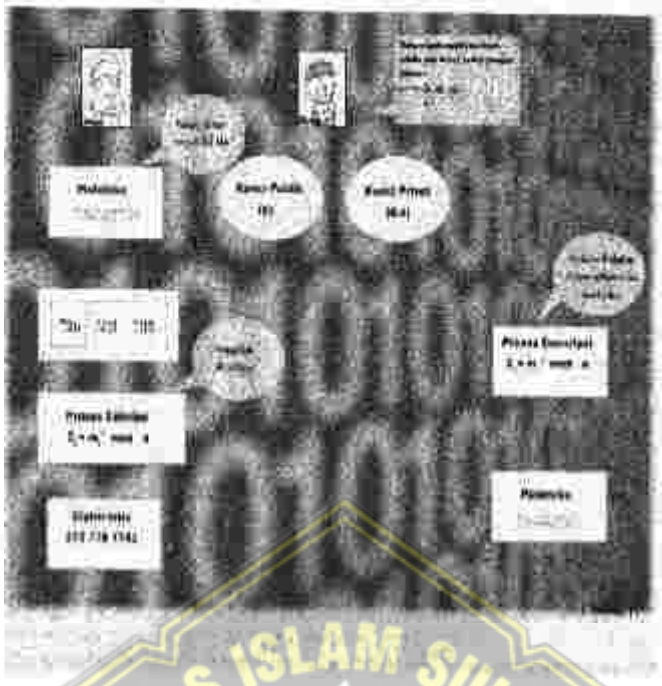
Gambar 48. Tombol Sub Menu RSA

Gambar 49. Tampilan Halaman Sub Menu RSA



Gambar 4.10. Halaman Materi Sejarah Algoritma RSA

Gambar 4.11. Halaman Materi Konsep Dasar Algoritma RSA



Gambar 4.12. Halaman Materi Simulasi Algoritma RSA

1. Diskripsi Karya

   Jika pada menu utama memilih tombol RSA, maka akan masuk pada halaman sub menu RSA dan jika memilih tombol.

2. Analisa Karya

   Pada menu utama, terdapat tombol RSA yang menjelaskan Algoritma RSA. Tampilan halaman sub menu RSA ini adalah akan ditampilkan beberapa tombol yang mempelajari tentang sejarah RSA, konsep dasar algoritma RSA, dan simulasi algoritma RSA. Pada tombol simulasi terdapat tombol Replay yaitu untuk mengulangi simulasi tersebut apabila kurang paham.

   Pada tombol RSA diberikan script agar dapat masuk pada materi RSA. Masing-masing tombol pada sub menu RSA yang dibahas diberikan script agar dapat masuk pada pembahasan materi.

   Pada tombol kembali diberikan script agar setelah pembahasan materi RSA dapat masuk pada sub menu lainnya atau akan masuk pada halaman menu utama.

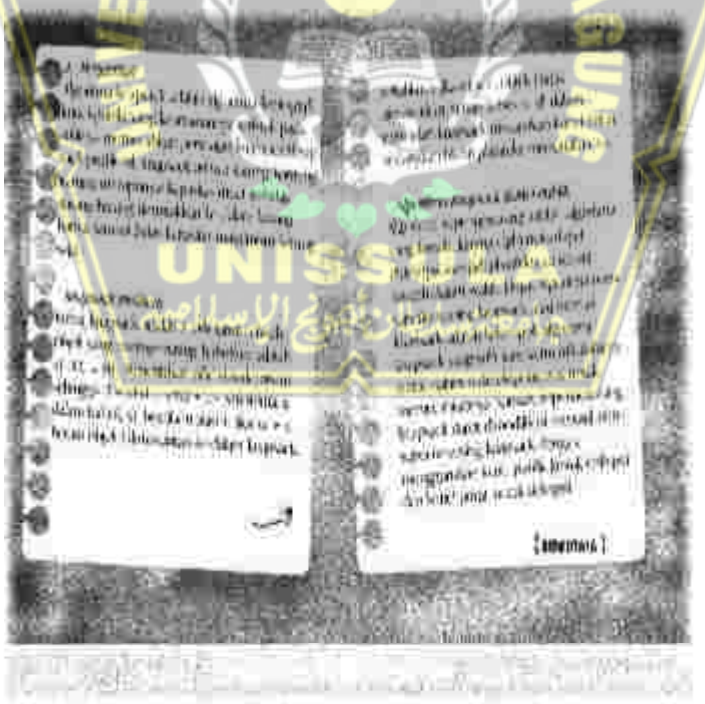
4.1.4. Halaman Sub Menu Algoritma Knapsack

1. Tampilan Sub Menu Knapsack

Gambar 4.13. Sub Menu Knapsack

Gambar 4.14. Halaman Sub Menu Knapsack

Gambar 4.15. Halaman Materi Sejarah Knapsack



Gambar 4.16. Halaman Materi Konsep Dasar Knapsack

Gambar 4.17. Halaman Simulasi Algoritma Knapsack

Gambar 4.18. Tombol Kembali

2. Diskripsi Karya

Jika pada menu utama memilih tombol Knapsack, maka akan masuk pada halaman sub menu Knapsack

3. Analisa Karya

Pada menu utama, terdapat tombol Knapsack yang menjelaskan Algoritma Knapsack. Tampilan halaman sub menu Knapsack ini adalah akan ditampilkan beberapa tombol yang mempelajari tentang sejarah Knapsack, konsep dasar algoritma Knapsack, dan simulasi algoritma Knapsack. Pada tombol simulasi terdapat tombol Replay yaitu untuk mengulangi simulasi tersebut apabila kurang paham.

Pada tombol Knapsack diberikan script agar dapat masuk pada materi Knapsack. Masing-masing tombol pada sub menu Knapsack yang dibahas diberikan script agar dapat masuk pada pembahasan materi.

Pada tombol kembali diberikan script agar setelah pembahasan materi RSA dapat masuk pada sub menu lainnya atau akan masuk pada halaman menu utama.

4.3.4 Halaman Tampilan Penutup

1. Tampilan Penutup

Gambar 4.19. Tombol EXIT

Gambar 4.20 Tampilan Keluar

2. Diskripsi Karya

Setelah semua program dalam media pembelajaran ini telah dijalankan, maka ada tombol keluar yang berfungsi untuk mengakhiri jalannya program. Sebelum benar-benar akan keluar dari program tersebut, terlebih dahulu akan ditampilkan pesan singkat berupa pertanyaan yakin akan keluar dari program. Apabila "ya" yang dipilih, maka akan keluar dari program.

3. Analisis Karya

Tombol keluar merupakan tombol untuk mengakhiri jalannya program media pembelajaran. Dengan script yang telah diberikan pada tombol keluar, Sebelum program benar-benar ditutup akan tampil peringatan keluar. Dengan script yang telah diberikan pada tombol "ya", maka apabila tombol "ya" yang dipilih, program pembelajaran ini berhenti dan ditutup dengan tampilan ucapan terima kasih penulis. Begitu juga dengan script yang diberikan pada tombol "tidak". Apabila tombol "tidak" yang dipilih, maka program akan kembali pada halaman menu utama.

BAB V
PENUTUP

5.1 Kesimpulan

Dari pembuatan Media Pembelajaran Algoritma RSA dan Algoritma Knapsack Berbasis Multimedia ini dapat disimpulkan sebagai berikut:

1. Metode pembelajaran multimedia ini merupakan salah satu alternatif untuk belajar Kriptografi, khususnya materi Algoritma RSA dan Algoritma Knapsack, selain menggunakan media buku.
2. Dengan media pembelajaran ini mahasiswa diharapkan dapat belajar dengan *fun*, karena gambar animasi yang menarik membuat mereka tidak mudah bosan.

5.2 Saran

1. Perkembangan teknologi berkembang pesat. Hal ini berpengaruh pada sistem belajar mahasiswa yang tidak hanya menggunakan buku melainkan media lainnya seperti komputer. Oleh karena itu media pembelajaran seperti pembelajaran multimedia ini perlu dikembangkan.
2. Interface yang mudah dan menarik membuat pengguna khususnya mahasiswa menjadi lebih mudah dalam memahami materi yang disajikan.

DAFTAR PUSTAKA

http://lmucomputer.org/2008/11/25/Penggabungan-dua-lagu-dengan-cool-Edit-Pro

http://makalah IF 3058-2009-b004pdf

Munir, Rinaldi2006.*Kriptografi*. Penerbit Informatika, Bandung

Madcoms, Andi 2007. *Mahir dalam 7 hari : Macromedia Flash Pro 8, Andi, Yogjakarta*

LAMPIRAN

```
on (release) {
        gotoAndPlay(91);
}

loadMovieNum("utamasound.swf",1);
stop();
stopAllSounds();

on (release) {
        gotoAndPlay(117);
}

on (release) {
        gotoAndStop(116);
}

on (release) {
        gotoAndStop(146);
}

on (release) {
        gotoAndStop(147);
}

on (release) {
        gotoAndStop(179);
}
```

```
on (release) {
        gotoAndPlay(150);
}

on (release) {
        gotoAndStop(181);
}

on (release) {
        //fscommand "quit",true;
        _root.att.gotoAndStop(2);
        exit.enabled=false;
        rss.enabled=false;
        knapsack.enabled=false;
        intro.enabled=false;

on (release) {
        gotoAndStop(180);
}

on (release) {
        gotoAndStop(148);
}
```

```
on (release) {
        gotoAndStop(116);
}
```

FAKULTAS TEKNOLOGI INDUSTRI
Universitas Islam Sultan Agung (UNISSULA)
Jl. Raya Kaligawe Km4 Telp. 024-6583584 Psw. 340 Faks. 024-6582455
Semarang 50112 http://www.unissula.ac.id

LEMBAR REVISI SIDANG PROYEK ILMIAH

Berdasarkan Rapat Tim Penguji Sidang Proyek Ilmiah

Hari	:	Jum'at
Tanggal	:	12 Maret 2010
Tempat	:	Ruang Seminar Lt. 1

Memutuskan bahwa mahasiswa :

Nama	:	Tri Mustikaningtyas
NIM	:	86.206.0060
Judul Proyek Ilmiah	:	Media Pembelajaran Kriptografi (Algoritma RSA dan Algoritma Knapsack) Berbasis Multimedia

wajib melakukan perbaikan seperti tercantum dibawah ini:

NO	REVISI	BATAS REVISI
-	penulisan	2 minggu
-	hal ana.	
-	bawa laporan u/ ditengs.	

Semarang, 12 Maret 2010

Penguji,

M. Khosyi'in ST, MT
NIK/NIP : 210.603.026

Acc 26/3

FAKULTAS TEKNOLOGI INDUSTRI
Universitas Islam Sultan Agung (UNISSULA)
Jl. Raya Kaligawe Km 4 Telp. 024-6583584 Psw. 340 Fax. 024-6582455
Semarang 50112 http://www.unissula.ac.id

LEMBAR PERTANYAAN

Dosen Penguji	:	Moch. Taufik, ST. MIT
Nama Mahasiswa	:	Tri Mustikaningtyas
NIM	:	86.206.0060
Judul Proyek Ilmiah	:	Media Pembelajaran Kriptografi (Algoritma RSA dan Algoritma Knapsack) Berbasis Multimedia

NO	PERTANYAAN

Semarang, 12 Maret 2010

Penguji,

Moch. Taufik, ST. MIT

210.206.026

FAKULTAS TEKNOLOGI INDUSTRI
Universitas Islam Sultan Agung (UNISSULA)
Jl. Raya Kaligawe Km4 Telp. 024-6583584 Psw. 340 Faks. 024-6582455
Semarang 50112 http://www.unissula.ac.id

LEMBAR REVISI SIDANG PROYEK ILMIAH

Berdasarkan Rapat Tim Penguji Sidang Proyek Ilmiah

Hari	:	Jum'at
Tanggal	:	12 Maret 2010
Tempat	:	Ruang Seminar Lt. 1

Memutuskan bahwa mahasiswa:

Nama	:	Tri Mustikaningtyas
NIM	:	86.2060060
Judul Proyek Ilmiah	:	Media Pembelajaran Kriptografi (Algoritma RSA dan Algoritma Knapsack) Berbasis Multimedia

wajib melakukan perbaikan seperti tercantum dibawah ini:

NO	REVISI	BATAS REVISI

Semarang, 12 Maret 2010

Penguji,

Moch. Taufik, ST. MIT
NIK/NIP.: 210.604.034

FAKULTAS TEKNOLOGI INDUSTRI
Universitas Islam Sultan Agung (UNISSULA)
Jl. Raya Kaligawe Km.4 Telp. 024-6583584 Psw. 340 Faks. 024-6562455
Semarang 50112 http://www.unissula.ac.id

LEMBAR PERTANYAAN

Dosen Penguji	:	M. Khosyi'in ST, MT
Nama Mahasiswa	:	Tri Mustikaningtyas
NIM	:	86.206.0060
Judul Proyek Ilmiah	:	Media Pembelajaran Kriptografi (Algoritma RSA dan Algoritma Knapsack) Berbasis Multimedia

NO	PERTANYAAN

Semarang, 12 Maret 2010

Penguji,

M. Khosyi'in ST, MT