PERANCANGAN PENGAMANAN DATA BERBASIS TEKS MENGGUNAKAN TRIPLE DES

Jurusan Teknik Telekomunikasi

Ade Nurhayati, ST[1] , Fitria Heryanti, ST[2], Rahman Hakim[3]

Akademi Teknik Telekomunikasi Shandy Putra Jakarta

Sade_icad@yahoo.com, alcaalexble@rocketmail.com

ABSTRAK

Triple DES (*Triple Data Encryption Standard*) merupakan salah satu algoritma simetris pada kriptografi yang digunakan untuk mengamankan data dengan cara menyandikan data. Proses yang dilakukan dalam penyandian datanya, yaitu proses enkripsi dan proses dekripsi. Algoritma Triple DES adalah suatu algoritma pengembangan dari algoritma DES (*Data Encryption Standard*). Perbedaan DES dengan Triple DES terletak pada panjangnya kunci yang digunakan. Pada DES menggunakan satu kunci yang panjangnya 56-bit, sedangkan pada Triple DES menggunakan tiga kunci yang panjangnya 168-bit (masing-masing panjangnya 56 bit). Pada Triple DES, tiga kunci yang digunakan bisa bersifat saling bebas (K1 ≠ K2 ≠ K3) atau hanya dua buah kunci yang saling bebas dan satu kunci lainnya sama dengan kunci pertama (K1 ≠ K2 dan K3 = K1). Karena tingkat kerahasiaan algoritma Triple DES terletak pada panjangnya kunci yang digunakan, maka penggunaan algoritma Triple DES dianggap lebih aman dibandingkan dengan algoritma DES.

Untuk memudahkan penggunaan algoritma Triple DES, maka dibuat suatu program algoritma Triple DES dengan alat Bantu bahasa pemrograman yaitu Visual Basic 2005, bahasa tersebut digunakan untuk membuat program yang dapat mengenkripsi dan mendekripsi file yang berekstensi .txt.

Kata kunci : Triple DES (*Triple Data Encryption Standard*), DES (*Data Encryption Standard*), kriptografi, enkripsi, dekripsi, kunci.

ABSTRACT

Triple DES (Triple Data Encryption Standard) is one of the symmetrical algorithm of cryptography used to protect data by encoding data. Process in encoding data is encryption and decryption process. Triple DES Algorithm is a development algorithm of DES algorithm (Data Encryption Standard). DES different with Triple DES because of length keys that used. DES used one key with length 56-bits while Triple DES used three keys with length 168-bits (each length 56 bits). Three keys that used in Triple DES may independent (K1 ≠ K2 ≠ K3) or two keys independent which one key equal to first key (K1 ≠ K2 dan K3 = K1). Because of level secret of Triple DES algorithm laying in used length keys, the usage of Triple DES assumed more peaceful compared to DES algorithm.

Triple DES algorithm was arranged in Visual Basic 2005, the Ianguage used to make program in order to make easy in encryption and decryption process with file extension .txt.

***Keywords** : Triple DES (Triple Data Encryption Standard), DES (Data Encryption Standard), cryptography, encryption, decryption, key.*

1. Pendahuluan

1.1 Latar Belakang

Berbagai macam layanan komunikasi tersedia di Internet diantaranya adalah web, e-mail, milis, newsgroups, dan sebagainya. Dengan semakin maraknya orang memanfaatkan layanan komunikasi di Internet tersebut, maka permasalahan pun bermunculan apalagi ditambah dengan munculnya para peretas. Masalah yang pertama yaitu tentang kerahasiaan *(confidentiality)*, yaitu bagaimana agar pesan atau file yang ingin dikirimkan tidak dapat dibaca oleh orang lain yang tidak berhak. Masalah yang kedua yaitu tentang keaslian pesan *(authentication)*, yaitu pesan yang dikirimkan

benar berasal dari seseorang dan bukan dari orang lain yang sedang menyamar.

Masalah keamanan data sangatlah penting jika ingin berkomunikasi melalui internet yang terpenting adalah bagaimana seseorang dapat mengamankan data tersebut agar tidak mudah dilihat atau dibajak oleh orang lain yang tidak berhak atau berwenang. Jika hal tersebut terjadi maka data-data yang dikirimkan rusak bahkan bisa saja hilang serta dapat menimbulkan kerugian bagi seseorang yang telah melakukan komunikasi melalui dunia maya tersebut.

Banyak orang menyiasati bagaimana cara mengamankan informasi yang dikomunikasikannya atau menyiasati bagaimana mendeteksi keaslian dari informasi yang diterimanya. Salah satunya dengan menggunakan penyandian pesan atau sering disebut kriptografi, dengan adanya kriptografi ini bertujuan agar seseorang dapat merasa aman jika berkomunikasi dengan orang lain.

Oleh karena itu dibuatlah sebuah aplikasi yang dapat menyandikan sebuah pesan agar pesan tersebut dapat dirahasiakan oleh pemiliknya. Aplikasi yang dibuat ini merupakan program enkripsi dan dekripsi pesan teks dengan metode triple DES menggunakan Visual Basic 2005, hal ini dimaksudkan agar program tersebut dapat digunakan untuk merahasiakan sebuah pesan dari pihak yang tidak berwenag.

1.4 Pembatasan Masalah

1. Membuat aplikasi pengamanan data berbasis teks menggunakan Triple DES dan lebih difokuskan lagi pada proses enkripsi dan dekripsi file teks saja.
2. Program menggunakan visual basic 2005.
3. Diagram *Unified Modeling Language* (UML) yang digunakan hanya dua buah diagram yaitu diagram use case dan diagram konteks.

1.5 Metodologi dan Penelitian

Metode yang digunakan untuk penyusunan laporan tugas akhir ini adalah sebagai berikut:

1. Studi literatur, merupakan metode pengumpulan data dengan cara mengumpulkan bahan-bahan yang didapat dari buku-buku, modul ataupun sampel program yang berkaitan dengan tema penulisan.
2. Metode Rekayasa Perangkat Lunak menggunakan Waterfall Model, yang terdiri dari 6 tahapan: definisi, pendahuluan, teori dasar, perancangan, analisis, dan pengujian.

1.6 Sistematika Penulisan

BAB I : PENDAHULUAN

Bab ini membahas mengenai latar belakang, maksud dan tujuan, metode penulisan, batasan masalah, dan sistematika penulisan.

BAB II : TEORI DASAR TRIPLE DES

Bab ini berisi tentang materi yang mendukung laporan tugas akhir juga sebagai dasar acuan agar penelitian yang dilakukan tidak menyimpang dari latar belakang masalah yang ada dan sesuai dengan tujuan yang dicapai.

BAB III : ANALISA DAN PERANCANGAN

Bab ini berisi tentang perancangan terhadap program aplikasinya, diantaranya perancangan aplikasi Aplikasi pengamanan data berbasis teks menggunakan triple DES.

BAB IV : PERANCANGAN PENGAMANAN DATA BERBASIS TEKS MENGGUNAKAN TRIPLE DES

Bab ini berisi tentang perancangan terhadap program aplikasinya, diantaranya perancangan aplikasi Perancangan pengamanan data berbasis teks menggunakan triple DES.

BAB V : PENUTUP

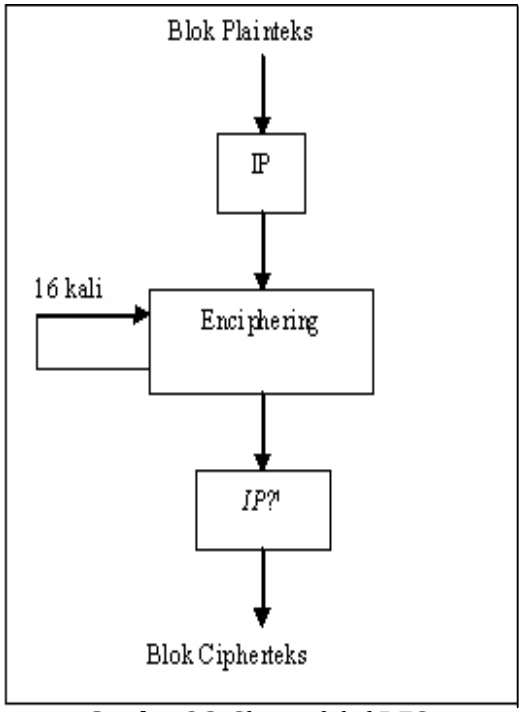
Pada bab ini merupakan kesimpulan dan pembahasan pada penulis proyek akhir ini beserta saran-saran untuk kesempurnaan program aplikasi ini secara keseluruhan

2. Teori Triple DES

2.1 DES (*Data Encryption Standard*)

DES adalah salah satu algoritma cipher blok yang populer karena dijadikan standar algoritma enkripsi kunci-simetri, meski pun saat ini standard tersebut sudah diganti dengan algoritma yang baru, AES, karena DES sudah dianggap tidak aman lagi. Algoritma DES Dikembangkan di IBM pada tahun 1972 dibawah kepemimpinan W. L.Tuchman. Algorima ini didasarkan pada algoritma Lucifer yang dibuat oleh Horst Feistel. Algorima ini telah disetujui oleh National Bureau of Standard (NBS) setelah penilaian kekuatannya oleh *National Security Agency (NSA)* Amerika Serikat.

DES beroperasi pada ukuran blok 64 bit. DES mengenkripsinya 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (*internal key*) atau upda-kunci(*subkey*). Kunci internal dibangkitkan dari kunci eksternal (*external key*) yang panjangnya 64 bit. Skema global dari algoritma DES dapat dilihat pada Gambar 2.3.



Gambar 2.3. Skema global DES.

Penjelasan:

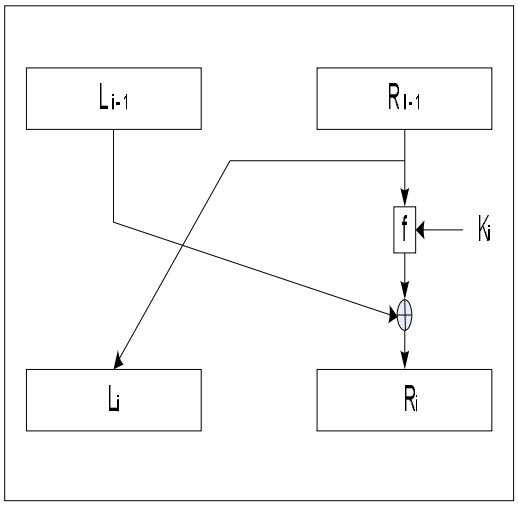
1. Blok plainteks dipermutasi dengan matriks permutasi awal (initial permutation atau IP).
2. Hasil permutasi awal kemudian di enciphering sebanyak 16 kali (16 putaran).
3. Setiap putaran menggunakan kunci internal yang berbeda. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (invers initial permutation atau IP-1) menjadi blok cipherteks.

Di dalam proses *enciphering*, blok plainteks terbagi menjadi dua bagian, kiri (*L*) dan kanan (*R*), yang masing-masing panjangnya 32 bit. Kedua bagian ini masuk ke dalam 16 putaran DES. Pada setiap putaran *i*, blok *R* merupakan masukan untuk fungsi transformasi yang disebut *f*. Pada fungsi *f*, blok *R* dikombinasikan dengan kunci internal *Ki*. Keluaran dari fungsi *f* di-*XOR*-kan dengan blok *L* untuk mendapatkan blok *R* yang baru. Sedangkan blok *L* yang baru langsung diambil dari blok *R* sebelumnya. Ini adalah satu putaran DES. Secara matematis, satu putaran DES dinyatakan sebagai berikut:

$$Li = Ri - 1$$

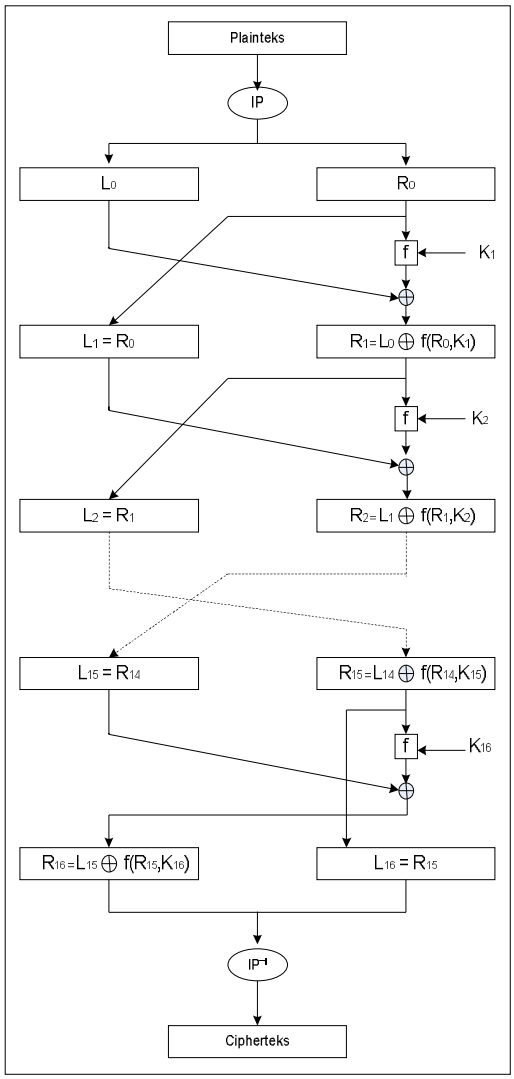
$$Ri = Li - 1 \text{ Å } f(Ri - 1, Ki)$$

Satu putaran DES merupakan model jaringan *Feistel* (lihat Gambar 2.4).



Gambar 2.4. Jaringan Feistel untuk satu putaran DES.

Gambar 2.5 memperlihatkan skema algoritma DES yang lebih rinci.



Gambar 2.5. Algoritma Enkripsi dengan DES.

Perlu dicatat dari Gambar diatas bahwa jika (*L*16, *R*16) merupakan keluaran dari putaran ke-16, maka (*R*16, *L*16) merupakan pra-cipherteks (*pre-ciphertext*) dari *enciphering* ini. Cipherteks yang sebenarnya diperoleh dengan melakukan permutasi awal balikan, IP-1, terhadap blok pra-cipherteks.

DES saat ini sudah dianggap tidak aman lagi karena panjang kuncinya yang pendek. Panjang kunci eksternal DES hanya 64 bit atau 8 karakter, itupun yang dipakai hanya 56 bit. Pada rancangan awal, panjang kunci yang diusulkan IBM adalah 128 bit, tetapi atas permintaan NSA, panjang kunci diperkecil menjadi 56 bit. Karena kunci DES yang sebanyak 56 bit dianggap sangat rawan terhadap serangan brute force, maka digunakanlah tiga buah DES secara berurutan untuk mengenkrip suatu pesan dengan kunci yang berlainan. Teknik tersebut dikenal dengan Triple DES yang akan meningkatkan keamanan dengan peningkatan kunci yang tadinya 56 bit menjadi 56 x 3 = 168 bit.

2.2 Triple DES

Triple Des atau TDES atau 3DES menggunakan DES tiga kali. Penggunaan tiga langkah ini penting untuk mencegah meet-in-the-middle attack sebagaimana pada Double DES. Bentuk sederhana dari Triple DES adalah:

Enkripsi: C = Ek3(Ek2(Ek1(P)))

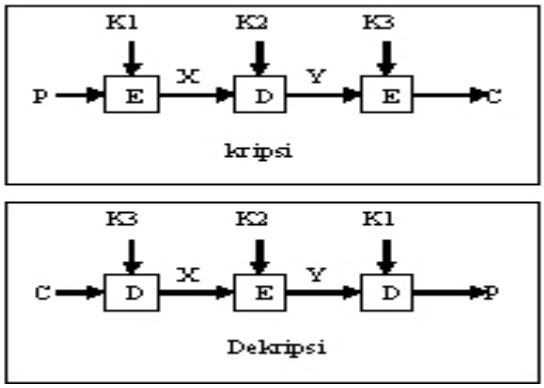
Dekripsi: P = Dk1(Dk2(Dk3(C)))

Varian ini umum dikenal sebagai mode EEE (untuk enkripsi) karena pada proses enkripsi semuanya menggunakan enkripsi. Untuk meyederhanakan interoperability antara DES dan Triple DES, maka langkah ditengah (pada proses enkripsi TDES) diganti dengan dekripsi (mode EDE). Dengan pengubahan ini, maka dibuat beberapa versi TDES. Versi pertama Triple DES menggunakan dua buah kunci, k1 dan k2:

Enkripsi: C = Ek1(Dk2(Ek1(P)))

Dekripsi: P = Dk1(Ek2(Dk1(C)))

Enkripsi DES tunggal dengan kunci K dapat dinyatakan sebagai TDES-EDE with K1 = K2 = K. Gambar dibawah ini memperlihatkan versi TDES yang menggunakan dua buah kunci. Penggunaan enkripsi pada langkah ditengah tidak mempengaruhi keamanan algoritma. Untuk lebih jelas lihat Gambar 2.6.



Gambar 2.6. Diagram enkripsi dan dekripsi

TDES dengan 3 buah kunci Secara umum, Triple DES dengan dua buah kunci mempunyai panjang kunci 2 x 56 = 112 bit, jauh lebih pendek daripada Triple DES dengan tiga buah kunci yang mempunyai panjang kunci 3 x 56 = 168 bit.

3. Analisa dan Perancangan

3.1 Analisis

Pada tahap ini, semua kebutuhan perangkat lunak didefinisikan sesuai dengan sasaran yanga ingin dicapai. Adapaun analisis tersebut menyangkut tentang masukan (*input*) dan keluaran (*output*) dari perangkat lunak, serta mendefinisikan bagaimana proses yang berjalan pada perangkat lunak unutk menjadi masukan yang ada menjadi keluaran yang diharapkan.

Analisis dari kebutuhan aplikasi yang akan dibangun adalah sebagai berikut:

1. Aplikasi yang akan dibuat harus mampu megenkripsi data yaitu berupa teks dari teks asli ke teks yang telah disandikan sebaliknya aplikasi tersebut dapat mendekripsi data berupa teks yang telah disandikan menjadi teks semula atau aslinya.
2. Aplikasi yang dibuat harus mampu mencari teks yang ingin di enkripsi atau di dekripsi serta dapat menyimpan hasil enkripsi dan dekripsi teks tersebut

3.2 Pembahasan Algoritma

Algoritma enkripsi atau dekripsi Triple DES seperti algoritma kriptografi lainnya yaitu memiliki algoritma umum. Pada pembahasan ini akan diberikan gambaran secara umum tentang algoritma Triple DES dan merancang prosedur tentang pembuatan aplikasi enkripsi atau dekripsinya serta memberikan penjelasan dari prosedur-prosedur yang digunakan.

3.2.1.1 Algoritma Triple DES

Triple DES (*Triple Data Encryption Standard*) merupakan suatu algoritma pengembangan dari algoritma DES (*Data Encryption Standard*). Pada dasarnya algoritma yang digunakan sama, hanya pada Triple DES dikembangkan dengan melakukan enkripsi dengan implementasi algoritma DES sebanyak tiga kali. Triple DES memiliki tiga buah kunci yang berukuran 168-bit (tiga kali kunci 56 bit dari DES). Pada algoritma Triple DES dibagi menjadi tiga tahap, setiap tahapnya merupakan implementasi dari algoritma DES. Gambar 3.1 menjelaskan tentang tahapan algoritma Triple DES.

Tahap pertama, plainteks yang diinputkan dioperasikan dengan kunci eksternal pertama (K1) dan melakukan proses enkripsi dengan menggunakan algoritma DES. Sehingga menghasilkan pra-cipherteks pertama. Tahap kedua, pra-cipherteks pertama yang dihasilkan pada tahap pertama, kemudian dioperasikan dengan kunci eksternal kedua (K_2) dan melakukan proses enkripsi atau proses dekripsi (tergantung cara pengenkripsian yang **Proses Enkripsi**

Proses enkripsi algoritma Triple DES dapat dicapai dengan beberapa cara, yaitu dengan menggunakan dua buah kunci atau tiga buah kunci:

1. Dengan dua buah kunci

   Enkripsi: C = Ek1(Dk2(Ek1(P)))

Penjelasan:

Enkripsi pesan *P* mula-mula dengan kunci K1, lalu hasilnya didekripsi lagi dengan kunci K2 kemudian dienkripsi lagi dengan kunci K1 dan hasil enkripsi terakhir adalah cipherteks (*C*).

2. Dengan tiga buah kunci

   Enkripsi: C = Ek3(Dk2(Ek1(P)))

Penjelasan:

Enkripsi pesan *P* mula-mula dengan kunci K1, lalu hasilnya didekripsi lagi dengan kunci K2 kemudian dienkripsi lagi dengan kunci K3 dan hasil enkripsi terakhir adalah cipherteks (*C*).

3.2.1.2 Proses Dekripsi

Proses dekripsi algoritma Triple DES dapat dicapai dengan beberapa cara, yaitu dengan menggunakan dua buah kunci atau tiga buah kunci:

1. Dengan dua buah kunci

   Dekripsi: P = Dk1(Ek2(Dk1(C)))

Penjelasan:

Mula-mula kunci K1 digunakan untuk mendekripsi *C*, lalu hasilnya dienkripsi lagi dengan kunci K2 kemudian didekripsi lagi dengan kunci K1dan hasil dekripsi terakhir adalah pesan semula (*P*).

2. Dengan tiga buah kunci

   Dekripsi: P = Dk1(Ek2(Dk3(C)))

Mula-mula kunci K3 digunakan untuk mendekripsi *C*, lalu hasilnya dienkripsi lagi dengan kunci K2 kemudian didekripsi lagi dengan kunci K1dan hasil dekripsi terakhir adalah pesan semula (*P*).

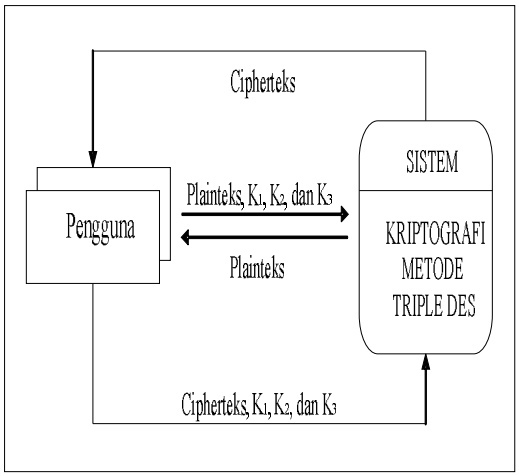
3.3 Perancangan Sistem

Pada rancangan sistem ini terdapat rancangan diagram blok berupa gambaran sistem penerapan algoritma Triple DES secara garis besar, flowchart yang menggambarkan prosedur dari sebuah aplikasi, serta struktur menu yang merupakan struktur hirarki menu dan rancangan tampilan aplikasi.

3.3.1 Perancangan Diagram Blok

Diagram blok dipergunakan untuk menggambarkan rancangan sistem secara umum yang hanya mengandung satu dan hanya proses saja dimana proses ini mewakili seluruh proses dari seluruh sistem.

Gambar 3.2 merupakan diagram blok yang menggambarkan sistem penerapan algoritma Triple DES secara garis besar.



Gambar 3.2. Diagram blok Triple DES.

Dari gambar diagram blok tersebut dapat dijelaskan bahwa terdapat satu terminator yang berhubungan dengan sistem tersebut yaitu pengguna. Adapun penjelasan dari aliran data yang digambarkan dalam diagram konteks tersebut diatas adalah sebagai berikut:

1. Pengguna melakukan enkripsi menggunakan teks asli (*plainteks*) dengan tiga buah kunci yaitu K1, K2, K3 kemudian sistem memprosesnya sehingga mengeluarkan hasil berupa teks terenkripsi (*cipherteks*) yang didapat oleh pengguna.
2. Pengguna melalukan dekripsi menggunakan teks terenkripsi (*cipherteks*) dengan tiga buah kunci yaitu K1, K2, K3 kemudian system memprosesnya sehingga mengeluarkan hasil berupa teks asli (*plainteks*) yang didapat oleh pengguna.

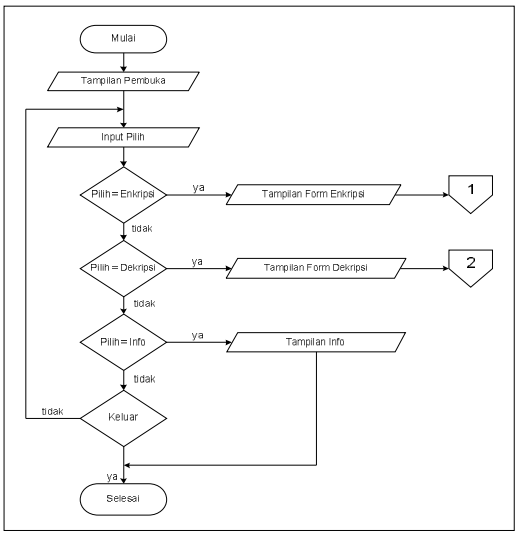
3.3.2 Perancangan Flowchart

Flowchart adalah penyajian yang sistematis tentang proses dan logika dari kegiatan penanganan informasi atau penggambaran secara grafik dari langkah langkah dan urut-urutan prosedur dari suatu program. Flowchart menolong analis dan programmer untuk memecahkan masalah kedalam segmen-segmen yang lebih kecil dan menolong dalam menganalisis alternatif-alternatif lain dalam pengoperasian.

Beberapa flowchart dibawah ini merupakan prosedur dari program enkripsi/dekripsi Triple DES yaitu flowchart layar utama, layar proses enkripsi, dan layar proses dekripsi.

3.3.2.1 Flowchart Layar Utama

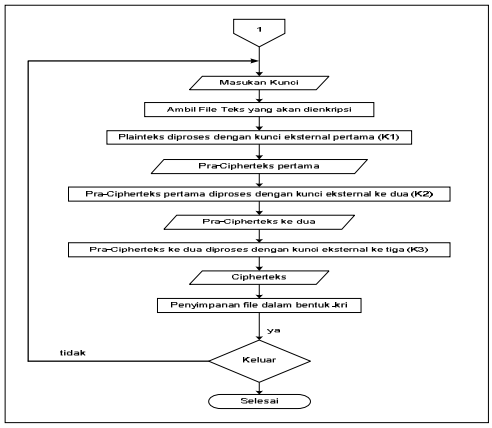
Flowchart layar utama merupakan aliran proses tahap pertama dalam menjalankan sebuah aplikasi yang digunakan untuk memudahkan interaksi antara pengguna dengan aplikasi. Pada tampilan layar utama ini, pengguna dapat memilih salah satu proses yang diinginkan yaitu memilih proses enkripsi, proses dekripsi, dan melihat informasi tentang pembuatan aplikasi. Untuk lebih jelasnya lihat Gambar 3.3.



Gambar 3.3. Flowchart tampilan layar utama.

3.3.2.2 Flowchart Proses Enkripsi

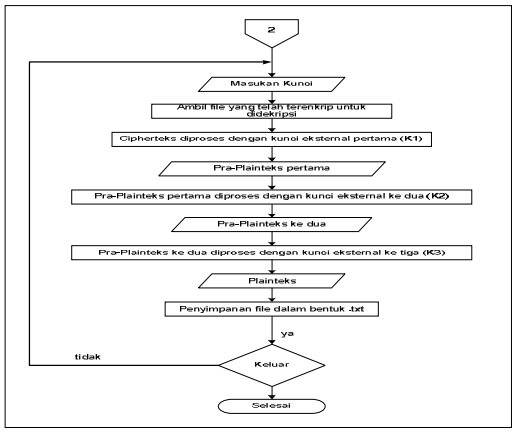
Flowchart proses enkripsi merupakan aliran proses untuk menjalankan program enkripsi yang digunakan untuk mengenkripsi file berupa teks. Pada tampilan program enkripsi ini, pengguna dapat mencari file untuk dienkripsi dengan menggunakan tombol pencari dan tombol penyimpan untuk menyimpan hasil enkripsi tersebut. Untuk lebih jelasnya lihat Gambar 3.4.



Gambar 3.4. Flowchart tampilan layar proses enkripsi.

3.3.2.3 Flowchart Proses Dekripsi

Flowchart proses dekripsi merupakan aliran proses untuk menjalankan program dekripsi yang digunakan untuk mendekripsi file yang telah dienkripsi. Pada tampilan program dekripsi ini, pengguna dapat mencari file untuk didekripsi dengan menggunakan tombol pencari dan tombol penyimpan untuk menyimpan hasil dekripsi tersebut. Untuk lebih jelasnya lihat Gambar 3.5.

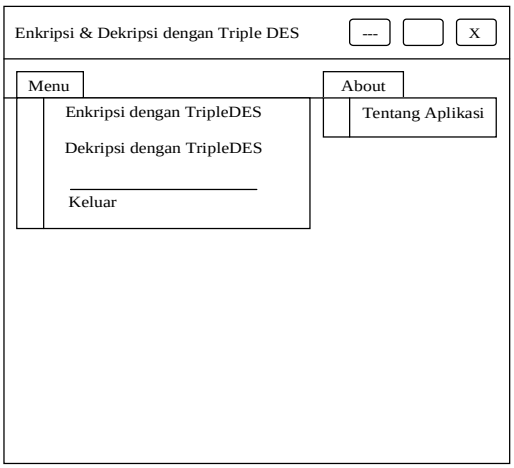


Gambar 3.5. Flowchart tampilan layar proses enkripsi.

3.4 Perancangan Aplikasi

3.4.1 Rancangan Halaman Utama

Halaman utama aplikasi adalah halaman yang memiliki sub yaitu ”Menu” dan ”About”. Menu terdiri atas sub menu proses enkripsi, proses dekripsi, dan keluar. Struktur rancangannya dapat dilihat pada Gambar 3.6.

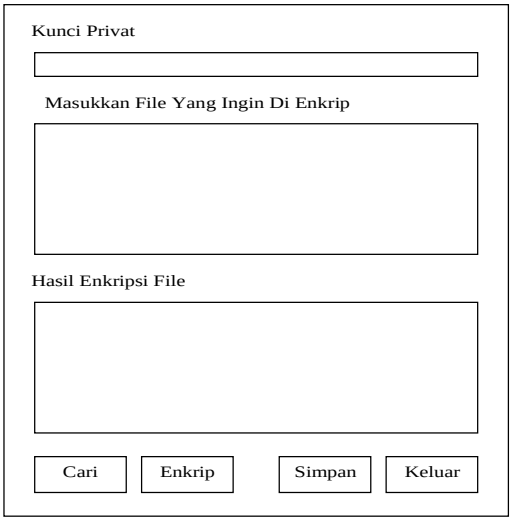


Gambar 3.6. Desain antar muka halaman utama

Rancangan ini adalah tampilan yang akan muncul pertama kali jika Perancangan Pengamanan Data Berbasis Teks Menggunakan Triple DES. dijalankan.

3.4.2 Rancangan Halaman Proses Enkripsi

Halaman proses enkripsi adalah halaman yang digunakan untuk melakukan proses enkripsi file teks. Lihat Gambar 3.7.

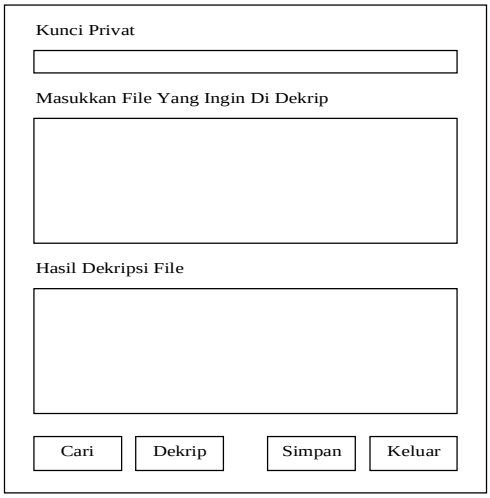


Gambar 3.7. Desain antar muka halaman proses enkripsi.

Rancangan ini digunakan untuk merubah file teks biasa menjadi teks yang tidak dapat dibaca oleh orang lain.

3.4.3 Rancangan Halaman Proses Dekripsi

Halaman proses dekripsi adalah halaman yang digunakan untuk melakukan proses dekripsi file teks. Struktur rancangannya dapat dilihat pada Gambar 3.8.

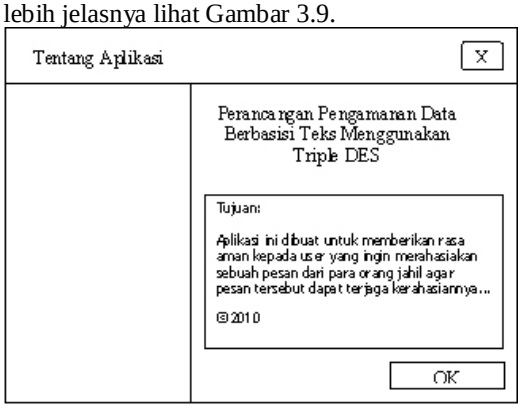


Gambar 3.8. Desain antar muka halaman proses dekripsi.

Rancangan ini digunakan untuk merubah file teks terenkripsi menjadi teks semula yang dapat dibaca oleh orang lain.

3.4.4 Rancangan Halaman About

Halaman about adalah halaman yang digunakan untuk mengetahui profil tentang aplikasi. Pada halaman ini ditampilkan informasi tentang aplikasi dan tujuan membuat aplikasi enkripsi dekripsi dengan Triple DES. Untuk lebih jelasnya lihat Gambar 3.9.



Gambar 3.9. Desain antar muka halaman about.

3 Perancangan Pengamanan Data Berbasis Teks Menggunakan Triple DES

4.1.2. mplementasi Kode Program

4.1.2.1. Kode Program Untuk Membuka Form Enkripsi

```
Private Sub
enkrip_Click(ByVal sender As
System.Object, ByVal e As
System.EventArgs) Handles
enkrip.Click
  Dim formSatu As Form1 =
New Form1
  formSatu.MdiParent = Me
  formSatu.Show()
  Label1.Hide()
End Sub
```

4.1.2.2. Implementasi Kode Program Membuka Form Dekripsi

```
Private Sub
Dekrip_Click(ByVal sender As
System.Object, ByVal e As
System.EventArgs) Handles
Dekrip.Click
 Dim formDua As Form2 = New
Form2
  formDua.MdiParent = Me
  formDua.Show()
  Label1.Hide()
End Sub
```

4.1.2.3. Kode Program Untuk Membuka Form About

```
Private Sub
Tentang_Click(ByVal sender
As System.Object, ByVal e As
System.EventArgs) Handles
Tentang.Click
  Dim about As AboutBox =
New AboutBox
  about.MdiParent = Me
  AboutBox.Show()
End Sub
```

4.2 Spesefikasi Kebutuhan Pengujian Sistem

4.2.1 Pengujian Sistem

Pada lingkungan pengujian ini, implementasi dari sistem yang akan dibangun didukung oleh berbagai elemen pendukung, seperti perangkat keras dan perangkat lunak. Pada sub bab berikut akan dijelaskan spesifikasi kebutuhan sistem untuk mendukung aplikasi enkripsi dan dekripsi. Lihat Tabel 4.1 dan 4.2.

Tabel 4.1. Spesifikasi Perangkat Keras.

Spesifikasi Perangkat Keras	
Prosesor	Intel Pentium IV 3.00 GHz
Memori	1 GB
Kapasitas Harddisk	80 GB
Kartu VGA	ATI Radeon 9200

Perangkat keras tersebut dilengkapi dengan monitor dengan resolusi layar 1024 x 768 sebagai sarana menampilkan aplikasi yang dibuat serta alat-alat input seperti keyboard dan mouse untuk mengoperasikannya.

Selain perangkat keras untuk menjalankan aplikasi, diperlukan juga perangkat lunak yang sesuai agar Perancangan Pengamanan Data Berbasi Teks Menggunakan Triple DES. dapat berjalan dengan baik serta optimal. Spesifikasi perangkat lunak yang digunakan dapat dilihat pada Tabel 4.2.

Tabel 4.2. Spesifikasi Perangkat Lunak.

Spesifikasi Perangkat Lunak	
Sistem Operasi	Microsoft Windows XP professional Service Pack 2
Bahasa Pemrograman	Visual Basic 2005

Aplikasi ini akan bekerja lebih cepat jika sedikit program lainnya yang sedang berjalan serta memori komputer yang tidak terpakai cukup besar. Kecepatan proses kerja suatu perangkat keras dan perangkat lunak menentukan kecepatan waktu proses aplikasi tersebut.

5. Penutup

5.1 Kesimpulan

Beberapa kesimpulan yang dapat diambil melalui pembahasan-pembahasan pada bab-bab sebelumnya dalam hal pembuatan aplikasi yang dilakukan oleh penulis adalah sebagai berikut:

1. Proses enkripsi dan dekripsi suatu data dengan algoritma 3DES dilakukan dengan cara mengimplementasikan algoritma DES sebanyak tiga kali, sesuai dengan pemilihan kuncinya dan urutan proses yang dipilih.
2. Kecepatan antara proses enkripsi dengan proses dekripsi pada setiap pemprosesan file teks adalah sama dan waktu yang di butuhkan oleh enkripsi dan dekripsi juga sama.
3. Plainteks yang diproses dengan kunci 1, kunci 2, dan kunci 3 menghasilkan cipherteks dengan jumlah karakter yang lebih besar, karena adanya proses padding dan disimpan dalam bentuk heksadesimal. Jika salah satu kunci atau ketiga kunci dirubah, maka cipherteks juga akan berubah.
4. Kecepatan untuk proses enkripsi dan dekripsi pada setiap pertambahan ukuran file input sebesar 1 KB, kecepatannya adalah sama. Untuk algoritma 3DES, pada proses enkripsi kecepatan rata-ratanya adalah 0.03024 KB/detik dan pada proses dekripsi kecepatan rata-ratanya adalah 0.05908 KB/detik. Sedangkan untuk algoritma DES, pada proses enkripsi kecepatan rata-ratanya adalah 0.08828 KB/detik dan pada proses dekripsi kecepatan rata-ratanya adalah 0.16667 KB/detik.
5. Untuk mendapatkan plainteks tanpa mengetahui kuncinya, jumlah kombinasi kemungkinan kunci yang harus dicoba adalah sebanyak 3,741 10^{50} kali.
6. Waktu yang diperlukan untuk mencoba seluruh kemungkinan kunci oleh serangan *brute force* adalah 1,183 10^{43} tahun.

5.2 Saran

Disamping kesimpulan, penulis juga memiliki beberapa saran yang mengarah pada pengembangan perancangan aplikasi yang dibuat, yaitu sebagai berikut:

1. Pengamanan data yang di buat masih banyak kekurangannya mulai dari desain, program, koding, dan lain-lain terkait dengan penggunaan program.
2. Pengamanan data ini hanya sebatas enkrip file berbasis teks, maka disarankan untuk mengembangkan ke tahap selanjutnya seperti dapat mengenkrip file-file yang lainnya yaitu file berbasis dokumen atau lainnya.
3. Penyimpanan hasil enkripsi terkadang tidak sama dengan proses enkripsi jika di buka dalam form dekripsi oleh karna itu di ajurkan untuk memperbaiki agar pengamanan data ini dapat berjalan dengan baik dan normal.
4. Pengembangan system dilengkapi dengan format file-file lain yang digunakan untuk membuka atau menyimpan file.

DAFTAR PUSTAKA

1 http://en.wikipedia.org/wiki/Triple_des

2 Hasan, Rusydi. 2003. **Mengenal Algoritma DES.** www.ilmukomputer.org

3 Komputer, Wahana Semarang. 2005. **Pemprograman Visual Basic. Net 2005.**

4 Munir, Rinaldi. 2006. **Kriptografi.** Bandung : Informatika

5 Rickyanto, Isak. 2003. **Tip dan Trik Visual Basic .Net.** Jakarta: Elex Media Komputindo.

6 Wardana. 2005. **Membuat 5 Program Dahsyat Di Visual Basic 2005.** Jakarta : Elex Media Komputindo

7 Whitten, Jeffery L. 2005. **Metode Desain dan Analisis edisi 6.** Yogyakarta: Penerbit Andi.