PROGRAM STUDI TEKNIK INFORMATIKA

ANALISIS DAN PERANCANGAN KEAMANAN DATA MENGGUNAKAN ALGORITMA KRIPTOGRAFI *DES (DATA ENCYPTION STANDARD)*

Febriansyah

08 142 349

Skripsi ini diajukan sebagai syarat memperoleh

gelar sarjana komputer di Universitas Bina Darma

FAKULTAS ILMU KOMPUTER

UNIVERSITAS BINA DARMA

PALEMBANG

2012

ANALISIS DAN PERANCANGAN KEAMANAN DATA MENGGUNAKAN ALGORITMA KRIPTOGRAFI *DES* (*Data encryption Standard*)

SKRIPSI

Disusun sebagai syarat memperoleh gelar Sarjana Komputer

OLEH :

FEBRIANSYAH
08.142.349

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BINA DARMA
PALEMBANG

TAHUN 2012

LEMBAR PENGESAHAN SKRIPSI

ANALISIS DAN PERANCANGAN KEAMANAN DATA MENGGUNAKAN ALGORITMA KRIPTOGRAFI *DE*S *(DATA ENCYPTION STANDARD)*

Oleh:

FEBRIANSYAH
08.142.349

Telah diterima sebagai salah satu syarat memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika

Palembang, September 2012
Program Studi Teknik Informatika
Fakultas Ilmu Komputer
Universitas Bina Darma

Pembimbing I **Dekan,**

Emigawaty, M.Kom **M. Izman Herdiansyah, Ph.D.**

Pembimbing II

Ria Andryani, M.Kom

HALAMAN PERSETUJUAN UJIAN

Skripsi berjudul "ANALISIS DAN PERANCANGAN KEAMANAN DATA MENGGUNAKAN ALGORITMA KRIPTOGRAFI DES (*DATA ENCRYPTION STANDARD*)" Oleh "FEBRIANSYAH NIM 08142349" telah dipertahankan didepan komisi penguji pada hari Selasa tanggal 14 Agustus 2012.

Komisi Penguji

1.	**Emigawaty, M.Kom**	**(ketua)**	**(**	**)**
2.	**Ria Andryani, M.Kom**	**(Sekretaris)**	**(**	**)**
3.	**Fatmasari, M.Kom**	**(Anggota)**	**(**	**)**
4.	**Susan Dian, M.Kom**	**(Anggota)**	**(**	**)**

Mengetahui.
Program Studi Teknik Informatika
Fakultas Ilmu Komputer
Universitas Bina Darma

Ketua,

Syahril Rizal, S.T., M.M., M.Kom

PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan dengan sesungguhnya bahwa seluruh data dan informasi yang disajikan dalam skripsi ini, kecuali yang disebutkan dengan jelas sumbernya, adalah hasil investigasi saya sendiri dan belum pelum pernah atau tidak sedang disajikan sebagai syarat memperoleh sebutan propessional lain atau sebutan yang sama ditempat lain. Apabila pernyataan ini tidak benar, saya bersedia menenrima sanksi kecuali yang disebutkan dengan jelas subernya.

Palembang, Agustus 2012
Yang membuat pernyataan,

Febriansayah
08.142.349

MOTTO DAN PERSEMBAHAN

MOTTO

" Kejujuran Dan Semangat Adalah Kunci Mencapai Keberhasilan"

PERSEMBAHAN

Kupersembahkan kepada :

- *Ayah dan Ibu Tercinta yang selalu mendoakan dan mengorbankansegalanya untuk keberhasilan ku*
- *Para pendidikku*
- *Saudara-saudaraku yang tercinta*
- *Untuk sahabatku yang telah memberikan semangat dan membantu*
- *Kepada Dosen pembimbing skripsi ini.*
- *Untuk yang tersayang*
- *Almamater*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

KATA PENGANTAR

بسم الله الرحمن الرحيم

Puji syukur kehadirat Allah SWT yang mana berkat rahmat dan hidayah-Nya jualah, skripsi ini dapat terselesaikan guna memenuhi salah satuu syarat untuk diteruskan menjadi skripsi sebagai proses akhir dalam menyelesaikan pendidikan dibangku kuliah.

Dalam penulisan skripsi ini, tentunya masih jauh dari sempurna. Hal ini dikarenakan keterbatasan pengetahuan yang dimiliki. Oleh karena itu dalam rangka melengkapi kesempurnaan dari penulisan skripsi ini diharapkan adanya saran dan kritik yang diberikan bersifat membangun.

Pada kesempatan ini, tidak lupa penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan bimbingan, pengarahan, nasihat dan pemikiran dalam menyelesaikan proposal skripsi ini, terutama kepada :

1. Prof. Ir. H. Bochari Rachman, M.Sc., selaku Rektor Universitas Bina Darma Palembang.

2. M. Izman Herdiansyah, ST, M.M.,Ph.D., selaku Dekan Fakultas Ilmu Komputer.

3. Syahril Rizal, S.T.,M.M., M.Kom., selaku Ketua Program Studi Teknik Informatika.

4. Emigawaty, M.Kom selaku pembimbing I dalam Penulisan Laporan.

5. Ria Andryani, M.M., M.Kom Selaku pembimbing II dalam Penulisan Laporan.

6. Bapak dan Ibu Dosen Universitas Bina Darma Palembang.

7. Ibu dan Ayah tercinta yang selalu memberikan dorongan baik dalam bentuk materi maupun moral, serta kakak dan adik-adikku yang selalu memberikan semangat.

8. Teman-teman di Program Studi Teknik Informatika yang telah banyak membantu dalam menyelesaikan proposal skripsi ini.

Palembang, Juli 2012

Penulis

ABSTRAK

Kriptografi merupakan bidang pengetahuan yang menggunkan persamaan matematis untuk melakukan proses enkripsi maupun deskripsi. Teknik ini digunakan untuk mengkonversi data kedalam bentuk kode-kode tertentu, untuk tujuan agar informasi yang tersimpan tidak dapat terbaca oleh siapa pun kecuali orang-orang yang berhak. Oleh karena itu sangat diperlukan sebuah sistem keamana data untuk menjaga kerahasiaan informasi agar tetap terjaga, salah satunya adalah metode algoritma simetris, karena algoritma ini menggunakan kunci yang sama pada saat melakukan proses enkripsi dan deskripsi sehinggan data yang kita miliki akan sulit untuk dimengerti maknanya dan untuk proses enkripsi data yang sangat besar akan sangat cepat. Algoritma kriptografi (*cipher*) yang digunakan adalah *DES.*

Kata kunci : *kriptografi, Enkripsi, Deskripsi, Cipher Blok*

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi sangat cepat dan pesat, hal ini yang menyebabkan munculnya kemajuan teknologi informasi. Secara langsung atau tidak, teknologi informasi telah menjadi bagian penting dari berbagai bidang kehidupan. Karna banyak kemudahan yang di tawarkan, teknologi informasi tidak dapat lepas dari berbagai aspek kehidupan manusia, yang memungkinkan dapat berkomunikasi dan saling bertukar informasi atau data. Seiring dengan kemajuan teknologi informasi maka sangat di perlukan sebuah keamanan data terhadap kerahasiaan informasi yang saling di pertukarkan, apa lagi jika data tersebut dalam suatu jaringan komputer yang terhubung/terkoneksi dengan jaringan lain. Hal tersebut tentu saja menimbulkan resiko bila informasi yang sensitif dan berharga tersebut di akses oleh orang yang tidak bertangung jawab. Yang mana jika hal tersebut sampai terjadi, kemungkinan besar akan merugikan bahkan membahayakan orang yang akan mengirim pesan, maupun organisasinya. Informasi yang terkandung di dalamnya pun bisa saja berubah sehingga menyebabkan salah penafsiran oleh penerima pesan. Selain itu

data yang di bajak tersebut kemungkinan rusak atau hilang yang menimbulkan kerugian material yang besar.

Oleh karena itu untuk menghindari agar hal tersebut tidak terjadi, penulis menggunakan algoritma kriptografi *DES* untuk proses enkripsi dan deskripsi data. Kriptografi telah menjadi suatu bagian yang tidak dapat di pisahkan dari sistem keamanan jaringan, Salah satu metode enkripsi data adalah *Data Encryption Standard* (*DES*). *Data Encryption Standard* (*DES*) merupakan algoritma *cipher* blok yang popular karena dijadikan standar algoritma enkripsi kunci-simetri. Sebenarnya *DES* adalah nama standar enkripsi simetri, nama algoritma enkripsinya sendiri adalah *DEA* (*Data Encryption Algorithm*), namun nama *DES* lebih popular dari pada *DEA*. Dari latar belakang di atas penulis mencoba untuk membuat *rancangan* keamanan data dengan menggunakan algoritma kriptografi *DES*, dengan mengambil judul **"Analisis dan Perancangan Keamanan Data Menggunakan *Data Encryption Standar* (*DES*)".**

1.2 Perumusan Masalah

Berdasarkan penjelasan dari latar belakang diatas maka perumusan masalah yang akan di bahas adalah "Bagaimana menganalisis dan merancang keamanan data menggunakan *Data Encryption Standard (DES)*".

1.3 Batasan Masalah

Agar penelitian ini lebih terarah dan tidak menyimpang dari rumusan masalah yang ada, maka batasan masalah dari penelitian ini hanya membahas mengenai proses penyandian data yang meliputi proses enkripsi dan deskripsi data

menggunakan algoritma kriptografi *DES* (*Data Encryption Standard*) pada blok mode ECB file yang berekstensi *.doc, *.txt dan hanya menggunakan kurang dari 64 bit.

1.4 Tujuan Penelitian

Sesuai dengan konsep yang ada, untuk menyelesaikan penelitian maka Tujuan dari penelitian ini adalah menganalisis dan merancang keamanan data menggunakan algoritma kriptografi *Data Encryption Standard (DES)*

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah dapat menambah pengetahuan dan wawasan penulis tentang kriptografi khususnya dalam hal proses enkripsi dan deskripsi didalam pengamanan dan kerahasiaan keamanan data menggunakan kriptografi *Data Encryption Standard (DES).*

1.6 METODOLOGI PENELITIAN

1.6.1 Waktu Penelitian

Penelitian ini dilakukan mulai dari bulan April sampai dengan Agustus 2012.

1.6.2 Metode penelitian

Metode penelitian yang di gunakan dalam penulisan proposal penelitian ini adalah metode penelitian deskriptif (Arikuno, 2012) mendefinisikan penelitian deskriptif ini adalah penelitian yang dimaksudkan untuk menyelidiki keadaan,

kondisi, situasi, peristiwa dan hal hal lain, yang hasilnya dipaparkan dalam bentuk laporan penelitian ini.

1.6.3 Metode Pengumpulan Data

Dalam kegiatan pengumpulan data untuk penelitian ini digunakan metode pengumpulan Studi Pustaka yang mana pada metode ini kegiatan yang dilakukan adalah mempelajari, mencari dan menggumpulkan data yang berhubungan dengan penelitian ini, seperti buku dan internet.

1.6.4 Metode pengembangan sistem

Dalam perancangan perangkat lunak ini penulis menggunakan metode *prototyping*/pemodelan (Pressman, 2002) sebagai metode pengembangan sistemnya yang terdiri atas empat langkah :

1. *Requirements*

Merupakan analisis terhadap kebutuhan calon pemakai dimana terlebih dahulu harus melakukan pengumpulan data yang berkaitan dengan system yang akan dibangun, kemudian menganalisis data-data yang sudah terkumpul agar dapat dilihat kebutuhan yang diinginkan pemakai.

2. *Design*

Yaitu pembuatan desain global untuk membentuk *prototype* perangkat lunak dengan terlebih dahulu membuat desain/rancangan secara keseluruhan yang akan digunakan oleh calon pemakai. Desain yang dibuat masih berupa *prototype* yang masih dalam bentuk rancangan.

3. *Build Prototype*

Yaitu pembuatan *prototype* perangkat lunak, termasuk didalamnya adalah pengujian dan penyempurnaan *prototype*. Desain yang sudah dipilih akan dibuat perangkat lunak *prototype*-nya dengan aplikasi yang sesuai keinginan calon pemakai. Kemudian perangkat lunak yang sudah dibuat *prototype*-nya akan diuji kebenarannya dan kehandalannya, sehingga nantinya akan dibuat *prototype* yang sebenarnya.

4. *Evaluate and Refine Requirements*

Merupakan kegiatan mengevaluasi *prototype* dan memperhalus analisis kebutuhan calon pengguna. *Prototype* yang sudah diuji dan disempurnakan kemudian dievaluasi kebenaran dan kemampuannya terhadap sistem. Kemudian kebutuhan calon pengguna yang dianalisis dilihat kesesuaiannya terhadap perangkat lunak yang akan dibangun.

BAB II

TINJAUAN PUSTAKA

2.1 Analisis

Pengertian analisis diartikan sebagai penguraian suatu pokok atas berbagai penelahan bagian itu sendiri, serta hubungan antar bagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan (Prastowo dan Julianty, 2002). Lain pula menurut (Komaruddin, 2001), analisis kegiatan berfikir untuk menguraikan suatu keseluruhan menjadi komponen sehingga dapat mengenal tanda-tanda komponen, hubungannya satu sama lain dan fungsi masing-masing dalam satu keseluruhan yang terpadu.

Dari pendapat data diatas dapat disimpulkan bahwa analisis atau analisa adalah kegiatan berfikir untuk menguraikan suatu pokok hal menjadi bagian-bagian atau komponen sehingga dapat diketahui ciri atau tanda tiap bagian, kemudian hubungan satu sama lain serta fungsi masing-masing bagian dari keseluruhan.

2.2 Perancangan

Menurut (whitte, 2004) Perancangan didefinisikan sebagai tugas yang fokus pada spesifikasi solusi detail berbasis komputer. Terhadap beberapa strategi perancangan dasain *system* yaitu :

1. Desain stuktur modern
2. Teknik informasi
3. Prototyping
4. *Join Application Development* (JAD)
5. *Rapid Application Development (RAD)*

6 Desain Berorientasi Objek

Kadang – kadang teknik tersebut dianggap sebagai teknik yang saling bersaing, tetapi seringkali untuk beberapa jenis proyek tertentu diperlukan kombinasi dari beberapa diantaranya sehingga saling melengkapi satu sama lain.

2.3 Keamanan Data

Secara umum data dikategorikan menjadi dua, yaitu data yang bersifat rahasia dan data yang tidak bersifat rahasia. Data yang tidak bersifat rahasia biasanya tidak akan terlalu diperhatikan. Yang sangat perlu diperhatikan adalah data yang bersifat rahasia, dimana setiap informasi yang ada didalamnya akan sangat berharga bagi pihak yang membutuhkan karena data tersebut dapat dengan mudah digandakan. Untuk mendapatkan informasi didalamnya, biasanya dilakukan berbagai cara yang tidak sah (Herryawan, 2010)

Keamanan data biasanya terkait hal-hal berikut:

a. Fisik**,** dalam hal ini pihak yang tidak berwenang terhadap data berusaha mendapatkan data dengan melakukan kegiatan sabotase atau penghancuran tempat penyimpanan data.
b. Organisasi, dalam hal ini pihak yang tidak berwenang untuk mendapatkan data melalui kelalaian atau kebocoran anggota yang menangani data tersebut.
c. Ancaman dari luar, dalam hal ini pihak yang tidak berwenang berusaha untuk mendapatkan data melalui media komunikasi dan juga melakukan pencurian data yang tersimpan di dalam komputer.

Fungsi keamanan komputer adalah menjaga tiga karakteristik, yaitu:

a. *Secrecy*, adalah isi dari program komputer hanya dapat diakses oleh orang yang berhak. Tipe yang termasuk di sini adalah *reading, viewing, printing*, atau hanya yang mengetahui keberadaan sebuah objek.
b. *Integrity*, adalah isi dari komputer yang dapat dimodifikasi oleh orang yang berhak, yang termasuk disini adalah *writing, changing status, deleting*, dan *creating*.
c. *Availability*, adalah isi dari komputer yang tersedia untuk beberapa kelompok yang diberi hak. Data yang aman adalah data yang memenuhi ketiga karakteristik keamanan data tersebut.

2.4 Algoritma

Ditinjau dari asal usul katanya, kata algoritma sendiri mempunyai sejarah yang aneh. Orang hanya menemukan kata *algorism* yang berarti proses menghitung dengan angka arab. Anda dikatakan *algorist* jika anda menggunakan. dengan angka arab. Para ahli bahasa berusaha menemukan asal kata ini namun

hasilnya kurang memuaskan. Akhirnya para ahli sejarah matematika menemukan asal kata tersebut yang berasal dari penulis buku arab yang terkenal yaitu Abu Ja'far Muhammad Ibnu Musa Al-Khuwarizmi menulis buku yang berjudul Kitab Aljabar Walmuqabala yang artinya "buku pemugaran dan pengurangan"(*The book off restoration and reduction*).

Dari judul buku itu kita juga memperoleh akar kata "Aljabar" (*Algebro*) perubahan dari kata *algorism* menjadi *algorithm* muncul karena kata algorism sering dikelirukan dengan arithmetic, sehingga akhiran-sm berubah menjadi thm. Karena perhitungan dengan angka arab sudah menjadi ha yang bisa, maka lambat laut kata *algorithm* berangsur-angsur dipakai sebagai metode perhitungan (komputasi) secara umum, sehingga kehilangan makna kata aslinya. Dalam bahasa Indonesia, kata *algorithm* diserap menjadi algoritma.

"Algoritma adalah urutan langka-langka logis penyelesaian masalah yang disusun secara sistematik dan logis". Kata logis merupakan kata kunci dalam algoritma. Langka-langka dalam algoritma harus logis dan harus dapat ditentukan bernilai salah atau benar (Munir, 2002).

2.5 Definisi Kriptografi

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan (*Cryptography is the art and science of keeping messages secure*) selain itu ada pengertian tentang kriptografi yaitu kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Kata "seni" di dalam definisi di atas maksudnya adalah mempunyai cara yang unik

untuk merahasiakan pesan. Kata "*graphy*" di dalam "*cryptography*" itu sendiri sudah menyiratkan sebuah seni (Munir, 2006).

2.6 Sejarah Kriptografi

Kriptografi mempunyai sejarah yang panjang. Informasi yang lengkap mengenai sejarah kriptografi dapat di temukan di dalam buku David Kahn yang berjudul *The Codebreakers.* Buku yang tebalnya 1000 halaman ini menulis secara rinci sejarah kriptografi mulai dari penggunakaan kriptografi oleh bangsa Mesir 4000 tahun yang lalu (berupa *hieroglyph* yang tidak standar pada piramid) hingga penggunaan kriptografi pada abat ke-20.secara historis ada empat kelompok orang yang berkontribusi terhadap perkembangan kriptografi, dimana mereka menggunakan kriptografi untuk menjamin kerahasiaan dalam komunikasi pesan penting, yaitu kalangan militer (termasuk intelejen dan mata-mata), kalangan *diplomatic*, penulis buku harian, dan pencinta (*lovers*). Diantara ke-empat kelompok ini, kalangan militer yang memberikan kontribusi paling penting karena pengiriman pesan didalam suasana perang membutuhkan teknik enkripsi dan deskripsi yang rumit. Kriptografi juga digunakan Untuk tujuan keamanan. Kalangan gereja pada masa awal agama Kristen menggunakan kriptografi untuk menjaga tulisan *religious* dan gangguan otoritas politik atau budaya yang dominan saat itu. Mungkin yang sangat terkenal adalah "Angka si Buruk Rupa" (*Number of the beast*) di dalam kitab perjanjian baru. Angka "666" menyatakan cara kriptografi (yaitu dienskripsi) untuk menyembunyikan pesan berbahaya; para ahli percaya bahwa pesan tersebut mengacu pada kerajaan Romawi.

Kriptografi modern dipicu oleh perkembangan peralatan komputer digital. Dengan komputer *digital*, *cipher* yg lebih kompleks menjadi sangat mungkin untuk dapat dihasilkan. Tidak seperti kriptografi klasik yang mengenskripsi karakter per karakter (dengan menggunakan *alphabet* tradisionil), kriptografi *modern* beroperasi pada *string biner*. *Cipher* yang kompleks seperti *DES* (*Data Encryption Standard*) dan penemuan algoritma *RSA* adalah algoritma kriptografi *modern* yang paling dikenal di dalam sejarah kriptografi *modern*. Kriptografi *modern* tidak hanya berkaitan dengan teknik menjaga kerahasiaan pesan, tetapi juga melahirkan konsep seperti tanda –tangan *digital* dan sertifikasi *digital*. Dengan kata lain, kriptografi modern tidak hanya memberikan aspek keamanan *confidentiality*, tetapi juga aspek keamanan lain seperti otentikasi, integritas data, dan penyangkalan (Munir, 2006).

2.7 Tujuan Kriptografi

Menurut (Munir, 2006) Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi, yaitu:

1. *Convidentiality* (kerahasiaan), yaitu memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan data dengan menyembunyikan informasi lewat teknik-teknik enkripsi.
2. *Message intergrity* (integritas data), yaitu memberikan jaminan bahwa dari setiap bagian tidak mengalami perubahan dari saat data dibuat/ dikirim sampai dengan saat data tersebut di buka.

3. *Non-repudiation* (nirpenyangkalan), yang memberikan cara untuk membuktikan bahwa suatu dokumen dating dari setiap seseorang apabila ia mencoba menyangkal memiliki dokumen tersebut.
4. *Auntentication* (autentikasi), yang memberikan dua layanan. Yang pertama mengidentifikasi keaslian dari suatu pesan dan memberikan jaminan keotentikannya. Kedua, untuk meguji identitas seseorang apabila ia akan memasuki sebuah sistem.

2.8 Kriptografi Klasik Dan Kriptografi *Modern*

a. Kriptografi Klasik

Sebelum komputer ada kriptografi dilakukan dengan algoritma berbasis karakter. Algoritma yang digunakan termasuk ke dalam sistem kriptografi simetri dan digunakan jauh sebelum sistem kriptografi kunci *public* ditemukan. Terdapat sejumlah algoritma yang tercatat dalam sejarah kriptografi (sehingga dinamakan algoritma kriptografi klasik), namun sekarang algoritma tersebut sudah usang karena sangat mudah dipecahkan (Munir, 2006).

Tiga alasan mempelajari algoritma kriptografi klasik, yaitu:

1. Untuk memberikan pemahaman konsep dasar kriptografi.
2. Dasar dari algoritma kriptografi *modern*. 14
3. Dapat memahami potensi-potensi kelemahan sistem *chiper*.

b. Kriptografi Modern

Algoritma kriptografi *modern* umumnya beroperasi dalam *mode bit* ketimbang *mode* karakter (seperti yang dilakukan pada *cipher* substitusi atau *cipher* transposisi dari algoritma kriptografi klasik) (Munir, 2006). Operasi dalam

mode bit berarti semua data dan informasi (baik kunci, *plainteks*, maupun *cipherteks*) dinyatakan dalam rangkaian (*string*) *bit biner*, 0 dan 1. Algoritma enkripsi dan dekripsi memproses semua data dan informasi dalam bentuk rangkaian *bit*. Rangkaian *bit* yang menyatakan *plainteks* dienkripsi menjadi *cipherteks* dalam bentuk rangkaian *bit*, demikian sebaliknya

Enkripsi *modern* berbeda dengan enkripsi konvensional. Karena enkripsi *modern* sudah menggunkan komputer untuk pengoperasiannya. Berfungsi untuk mengamankan data baik yang di *transfer* melalui jaringan komputer maupun yang bukan. Hal ini sangat berguna untuk melindungi *privacy data*, *integrity*, *authentication* dan *non-repudiation*. Perkembangan algoritma kriptografi *modern* berbasis *bit* didorong oleh penggunaan komputer *digital* yang merepresentasikan data dalam bentuk *biner*

Kriptografi *modern* merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Pada kriptogarfi *modern* terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer.

Algoritma kriptografi *modern* terdiri dari dua jenis

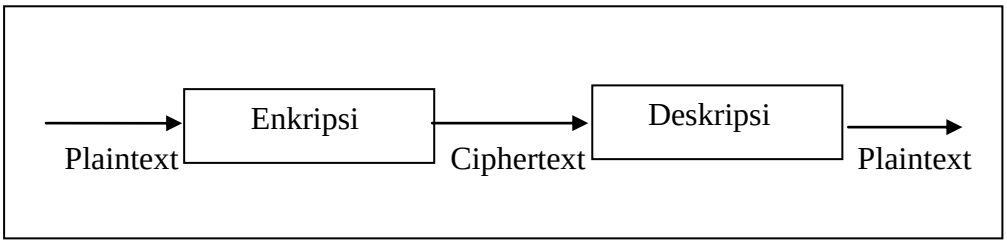
1. Algoritma Simetris

   Algoritma simetris adalah yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Algoritma kriprografi simetris sering disebut algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci, dan mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu. Kelebihan dari algoritma kriprografi simetris adalah waktu proses untuk enkripsi dan dekripsi relatif cepat. Hal ini disebabkan efesiensi yang terjadi pada pembangkit kunci.

Karena prosesnya relatif cepat maka algoritma ini tepat untuk digunakan pada sistem komunikasi *digital* secara *real time* seperti *GSM.*

2. Algoritma Asimetris

Algoritma Asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi deskripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia itu, yang dalam hal ini kunci rahasia, untuk melakukan pembongkaran terhadap kode yang dikirim untuknya. Contoh algoritma terkenal yang menggunakan kunci Asimetris adalah *RSA* (merupakan singkatan dari nama penemunya, yakni *Rivest, Shamir* dan *Adleman*).



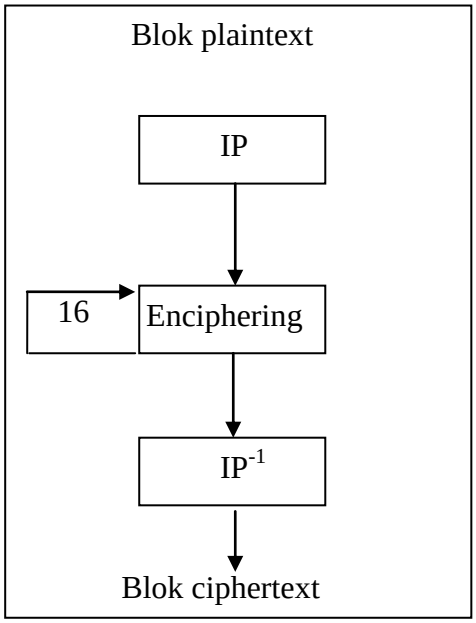
Gambar 2.1 Urutan Proses Kriptografi

2.9 *Data Encryption Standar* (*DES*)

Data Encrytion Standar (*DES*) adalah algoritma cipher blok yang popular karena dijadikan standar algoritma enkripsi kunci-simetri, meskipun saat ini standar tersebut telah digantikan dengan algoritma yang baru, *AES,* karena *DES* sudah di anggap tidak aman lagi. Sebenarnya *DES* adalah nama standar enkripsi simetri, nama algoritma enkripsinya sendiri adalah *DEA* (*Data Encryption Algorithm*),namun nama *DES* lebih popular dari pada *DEA*. Algoritma

DES dikembangkan di IBM dibawah kepemimpinan W.L. Tuchman pada Feistel. Algoritma ini telah disetujuin oleh *National Bureau of standar* (*NBS*) Amerika Serikat (Munir, 2006)

DES termasuk ke dalam *system* kriptografi simetri dan tergolong jenis *cipher* blok. *DES* peroperasi pada ukuran blok 64 bit. *DES* mengenkripsikan 64 bit plainteks menjadi 64 bit chipherteks dengan menggunkan 56 kunci internal atau upa-kunci. Kunci internal di bangkitkan dari kunci eksternal yang panjangnya 64 bit



Gambar 2.2 Global Algoritma *DES*

Skema global dari algoritma *DES* adalah sebagai berikut

1. Blok plainteks di permutasikan dengan metric permutasi awal (*initial permutation atau IP*).
2. Hasil permutasian awal kemudian di-*enciphering*- sebanyak 16 kali (16 putaran) setiap putaran menggunkan kunci *internal* yang berbeda.

3. Hasil enciphering kemudian di permutasikan dengan matriks permutasi balikan (*invers initial permutation* atau ip^{-1}) menjadi blok cipherteks.

2.10 K**eamanan *DES***

Isu-isu yang menjadi perdebatan kontroversi menyangkut keamanan *DES*

1. Panjang kunci

   Panjang kunci eksternal *DES* hanya 64 bit atau 8 karakter , itupun yang dipakai hanya 56 bit. Pada rancangan awal, panjang kunci yang di usulkan IBM adalah 128 bit,tetapi atas permintaan NSA, panjang kunci diperkecil menjadi 56 bit. Alasan pengurangan tidak diumumkan. Serangan yang palik praktis terhadap *DES* adalah *exhaustive key search*. Dengan panjang kunci 56 bit akan terdapat 2^{56} atau 72.057.594.037.927.936 kemungkinan kunci. Jika di asumsikan serangan *exhaustive key search* dengan menggunkan prosesor paraler mencoba setengah dari jumlah kemungkinan kunci itu , maka dalam satu detik dapat dikerjakan satu juta serangan. Jadi seluruhnya diperlukan 1142 tahun untuk menemukan kunci yang benar. Namun tahun, pada tahun 1998 *electronic frontier foundation* (*EFE*) merancang dan membuat perangkan keras khusus untuk menemukan kunci *DES* secara *exhaustive search key* dengan biaya $250.000 dan dapat diharapkan dapat menemukan kunci selama 5 hari. Tahun 1990, kombinasi perangkat keras *EFE* dengan kolaborasi internet yang melibatkan lebih dari 100.000 komputer dapat menemukan kunci *DES* kurang dari 1 hari.

2. Jumlah Putaran

Sebenarnya delapan putaran sudah cukup untuk membuat *cipherteks* sebagai fungsi acac dari setiap bit *plainteks* dan setiap bit *chiperteks*. Jadi,mengapa harus 16 x putaran? Dari penelitian, *DES* dengan jumlah putaran yang kurang dari 16 ternyata dapat di pecahkan dengan *known-plaintexk attack* bagus dari pada dengan *brute force attack* [SCH96].

3. Kotak-S

   Pengisian kota-S *DES* masih menjadi misteri tanpa ada alasan mengapa memilih konstanta-konstanta di dalam kota itu.

2.11 Mode *DES*

DES dapat di operasikan dengan *mode*, *ECB, CBC, OFB,* dan *CFB.* Namun karena kesederhanaannya, *mode ECB* lebih sering di gunakan pada paket program komersil meskipun sangat rentan terhadap serangan *Mode CBC* lebih *kompleks* dari pada *ECB* namu memberikan tingkat keamanan yang lebih bagus dari mode *ECB.* mode *CBC* hanya kadang-kadang saja digunakan.

2.12 *Flowchart*

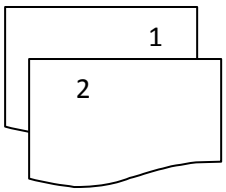
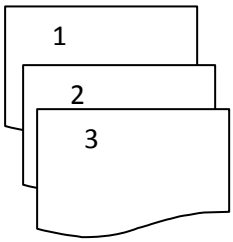
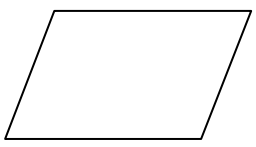
Flowchart adalah suatu metode untuk menggambarkan tahap-tahap pemecahan masalah dengan mempresentasikan simbol-simbol tertentu yang mudah dimengerti, mudah digunakan dan standar (sutedjo, 2004).

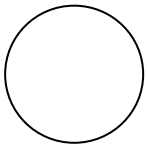
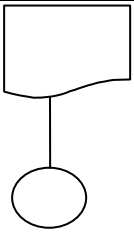
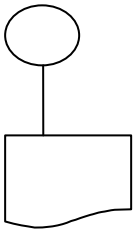
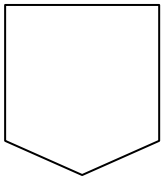
1. *System Flowchart*

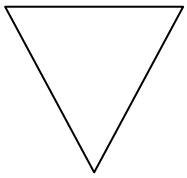
   System flowchart adalah urutan proses dalam *system* dengan menunjukkan alat. Media *input, output,* serta jenis media penyimpanan dalam proses pengolahan

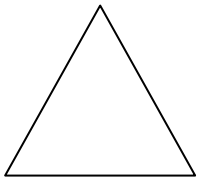
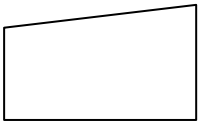
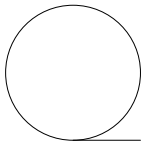
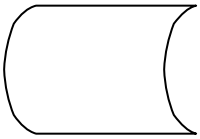
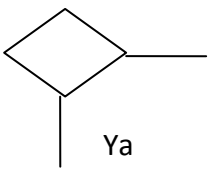
data. *System flowchar* ini tidak digunakan untuk menggambar urutan langka untuk memecahkan masalah, tetapi hanya untuk menggambarkan prosedur dalam system yang di bentuk.berikut ini adlah gambar dari simbol-simbol standar yang telah banyak digunakan pada penggunaan penggambaran *system flowchart.*

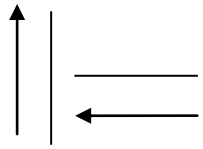
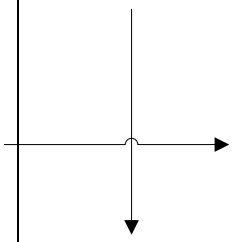
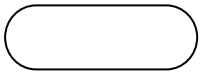
Tabel. 2.1 Simbol-simbol *System Flowchart*

No	Simbol	Keterangan
		**Dokumen**. Simbol ini di gunakan untuk menggambarkan semua jenis dokumen, yang merupakan formulir yang digunakan untuk merekam data terjadi suatu transaksi.
		**Dokumen dan Tembusannya.** Simbol ini digunakan untuk menggambarkan dokumen asli dan tembusannya. Nomor lembar dokumen dicantumkan di sudut kanan atas.
		**Berbagai Dokumen.** Simbol ini digunakan untuk menggambarkan berbagai jenis dokumen yang digabungkan bersama di dalam satu paket.
		**Catatan.** Simbol ini digunakan untuk menggambarkan catatan akuntansi yang digunakan untuk mencatat data yang direkam

		sebelumnya di dalam dokumen atau formulir.
		**Penghubung pada halaman yang sama.** *(on-page connector)*. Dalam menggambarkan bagan alir, arus dokumen dapat dibuat mengalir dari atas ke bawah dari kiri ke kanan.
		**Akhir arus dokumen dan** mengarahkan pembaca ke simbol penghubung halaman yang sama bernomor seperti yang tercantum di dalam simbol tersebut.
		**Akhir arus dokumen dan** mengarahkan pembaca ke simbol penghubung halaman yang sama bernomor seperti yang tercantum di dalam simbol tersebut.
		**Penghubung pada halaman yang berbeda.** *(off-page connector)* Jika untuk menggambarkan bagan alir suatu suatu sistem akuntansi diperlukan lebih dari satu halaman , simbol ini harus digunakan untuk menununjukkan kemana dan bagamana bagan alir terkait satu dengan yang lainnya.
		**Kegitan Manual.** Simbol ini digunakan untuk menggambarkan kegiatan *manual* seperti mengisi formulir, membandingkan, memeriksa dan

		berbagai jenis kegiatan klerikal yang lain.
		**Keterangan Komentar.** Simbol ini memungkinkan ahli sistem menambahkan keterangan untuk memperjelas pesan yang disampaikan dalam bagan alir.
		**Arsip Sementara.** Simbol ini digunakan untuk menunjukkan tempat penyimpanan dokumen, seperti almari arsip dan kotak arsip. Terdapat dua tipe arsip dokumen: arsip sementara dan arsip permanen .Arsip sementara adalah tempat penyimpanan dokumen yang dokumennya akan diambil kembali dari arsip tersebut di masa yang akan datang untuk keperluan pengolahan lebih lanjut terhadap dokumen tersebut.Untuk menunjukkan urutan pengarsipan dokumen digunakan simbol berikut : = menurut abjad = Menurut nomor urut = kronologis, menurut tanggal

		**Arsip permanen.** Simbol ini digunakan untuk menggambarkan arsip permanen yang merupakan tempat penyimpanan dokumen yang tidak diproses lagi dalam sistem akuntansi yang bersangkutan.
		***On-Line computer Process.*** Simbol ini menggambarkan pengolahan data dengan komputer secara *on-line.* Nama program ditulis dalam simbol
		***Keying (typing, verifying).*** Simbol ini menggambarkan pemasukan data ke dalam komputer melalui *on-line* terminal.
		**Pita magnetik *(magnetic tape).*** Simbol ini menggambarkan arsip komputer yang berbentuk pita magnetik. Nama arsip ditulis di dalam simbol.
		***On-line storage.*** Simbol ini menggambarkan arsip komputer yang berbentuk *on-line* (di dalam *memory* komputer).
		**Keputusan.** Simbol ini menggambarkan keputusan yang harus dibuat dalam proses pengolahan data. Keputusan yang dibuat ditulis dalam simbol.

	Tidak	
		**Garis alir*(flowline)*.** Simbol ini menggambarkan arah proses pengolahan data. Anak panah tidak digambarkan jika arus dokumen mengarah ke bawah dan ke kanan. Jika arus dokumen mengalir ke atas atau ke kiri, anak panah perlu dicantumkan.
		**Persimpangan garis alir.** Jika dua garis alir bersimpangan, untuk menunjukkan arah masing-masing garis, salah satu gari dibuat sedikit melengkung tepat pada persimpangan kedua garis tersebut.
		**Pertemuan garis alir.** Simbol ini digunakan jika dua garis alir bertemu dan salah satu garis mengikuti arus garis lainnya.
		**Mulai/berakhir *(terminal).*** Simbol ini menggambarkan awal dan akhir sistem.
		Masuk ke sistem. Karena kegiatan di luar sistem tidak perlu digambarkan dalam bagan alir, maka diperlukan simbol untuk menggambarkan masuk ke sistem yang digambarkan dalam bagan alir.

		Keluar ke sistem. Karena kegiatan di luar sistem tidak perlu digambarkan dalam bagan alir, maka diperlukan simbol untuk menggambarkan keluar ke sistem lain.

2. Program *Flowchart*

   Program *flowchart* adalah diagram alir yang menggambarkan urutan logika dari suatu prosedur pemecahan masalah. Untuk menggambarkan program *flowchart* tersedia simbol-simbol standar, berikut ini adalah gambaran dari simbol-simbol standar yang digunakan program *flowchart*

2.13 Penelitian sebelumnya

Agar penelitian ini dapat di pertanggung jawabkan secara akademis, maka penelitian akan menampilkan penelitian yang telah dilakukan oleh penelitian terdahulu sebagai berikut:

Pada penelitian I Putu Herryawan yang berjudul "Analisa Dan Penerapan Algoritma DES Untuk Pengamanan Data Gambar Dan Vidio" dijelaskan bahwa Sistem pada keamanan data dan kerahasiaan data merupakan salah satu aspek penting dalam perkembangan kemajuan teknologi informasi namun yang cukup disayangkan adalah ketidakseimbangan antara setiap perkembangan suatu teknologi yang tidak diiringi dengan perkembangan pada sistem keamanannya itu sendiri, dengan demikian cukup banyak sistem-sistem yang masih lemah dan harus ditingkatkan keamanannya. Oleh karena itu pengamanan data yang sifatnya rahasia haruslah benar-benar diperhatikan.Untuk mengatasi masalah tersebut

maka diperlukan suatu aplikasi pengamanan data yang dapat mencegah dan mengamankan data-data yang kita miliki dari orang-orang yang tidak berhak mengaksesnya. Salah satunya adalah metode algoritma kriptografi simteris, karena algoritma ini menggunakan kunci yang sama pada saat melakukan proses enkripsi dan dekripsi sehingga data yang kita miliki akan sulit untuk dimengerti maknanya dan untuk proses enkripsi data yang sangat besar akan sangat cepat. Algoritma kriptografi (*cipher*) yang digunakan adalah DES.

Sedangkan pada penelitian Deni Mustopa "Perancangan Program Keamanan Data Dengan Menggabungkan Algoritma Kriptografi DES dan Mars" dijelaskan Kriptografi merupakan bidang pengetahuan yang mengunakan persamaan matematis untuk melakukan proses enkripsi maupun dekripsi. Teknik ini digunakan untuk mengkonversi data kedalam bentuk kode – kode tertentu, untuk tujuan agar informasi yang disimpan tidak dapat terbaca oleh siapa pun kecuali orang – orang yang berhak.

Dalam tugas akhir ini akan disajikan analisis algoritma kriptografi DES dan MARS yang mana kedua algoritma tersebut merupakan algoritma kriptografi simetris. Tugas akhir ini pula menampilkan implementasi program dan menampilkan bagaimana cara mengenkripsi dan mendekripsi dengan kedua algoritma tersebut.

BAB III

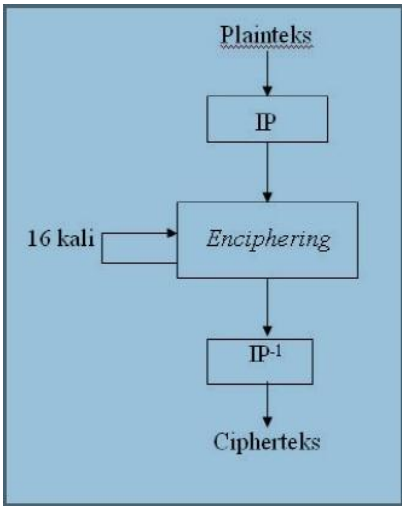
ANALISIS DAN PERANCANGAN

3.1 Analisis

Analisis adalah penguraian dari suatu pembahasan, dalam hal ini pembahasan mengenai perancangan keamanan data menggunakan algoritma kriptografi *DES* yang berguna untuk mengetahui apa saja yang dapat dijadikan isi perancangan yang akan dibuat.

3.1.1 Analisis permasalahan

Dalam pembahasan kriptografi yang sedang penulis bahas yaitu mengenai pengamanan data dengan menggunakan algoritma kriptografi *DES* Berikut dibawah ini analisa rancangan dari permasalahan yang sedang di bahas yang dijelaskan pada gambar 3.1 :



Gambar 3.1 Skema Global Algoritma DES

Skema global dari algoritma *DES* adalah sebagai berikut

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

3.1.2 Analisis Data

Analisis data merupakan tahapan dimana dilakukannya analisis terhadap data-data apa saja yang diolah dalam sistem atau prosedur sebuah rancangan, dalam hal ini data yang akan di enkripsi pada aplikasi kriptografi adalah berupa file *Txt, Doc.*

3.1.3 Analisis keamanan data

Pertukaran informasi setiap detik di internet membuat banyak terjadi pencurian informasi itu sendiri oleh pihak-pihak yang tidak bertanggung jawab. Oleh karna itu agar data yang dikirim aman dari orang yang tidak bertanggung

jawab, data tersebut harus disembunyikan dengan cara menyandikan data tersebut menggunakan algoritma kriptografi *DES*. Pertukaran data baik di jaringan lokal maupun di jaringan internet membawa informasi berupa pesan (*message*) yaitu suatu data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan disebut juga plainteks (*plaintext*) atau teks-jelas (*cleartext*). Pesan dapat berupa data atau informasi yang dikirimkan atau disimpan di dalam media perekaman. Pesan yang tersimpan tidak hanya berupa teks, tetapi dapat juga berbentuk citra (*image*), suara/bunyi (*audio*), dan juga video, atau pun berkas biner lainnya.

Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut chiperteks atau kriptogram. Chiperteks harus dapat ditransformasikan kembali menjadi plainteks semula agar pesan yang diterima bisa dibaca. Algoritma kriptografi yang digunakan disebut juga *cipher* yaitu suatu bentuk aturan untuk *enciphering* dan *deciphering*, atau fungsi matematika yang digunakan untuk proses enkripsi dan deskripsi. Beberapa *cipher* memerlukan algoritma yang berbeda untuk *enciphering* dan *deciphering*. Keamanan suatu data sering diukur dari banyaknya kerja (*work*) yang dibutuhkan untuk memecahkan chiperteks menjadi plainteksnya tanpa mengetahui kunci yang digunakan. Semakin banyak kerja yang diperlukan, semakin lama waktu yang dibutuhkan, maka semakin kuat algoritma kriptografi tersebut.

3.2 Langkah – Langkah Penyelesaian

Menurut (Munir, 2006) Dari permasalahan diatas, maka penulis mencoba untuk membuat sebuah rancangan yang berguna untuk mengamankan sebuah data dengan menggunakan algoritma kriptografi *DES*. Langkah – langkah simulasi dalam penyelesaian masalah diatas yaitu :

3.2.1 Proses Enkripsi

Langkah – langkah sebagai berikut :

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

3.2.2 Proses Deskripsi

1. Proses dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah K_1, K_2, …, K_{16}, maka pada proses dekripsi urutan kunci yang digunakan adalah K_{16}, K_{15}, …, K_1.
2. Untuk tiap putaran 16, 15, …, 1, keluaran pada setiap putaran *deciphering* adalah

   $$\boldsymbol{L_i = R_{i-1}}$$

   $$\boldsymbol{R_i = L_{i-1} \oplus f(R_{i-1}, K_i)}$$

3. yang dalam hal ini, (R_{16}, L_{16}) adalah blok masukan awal untuk deciphering. Blok (R_{16}, L_{16}) diperoleh dengan mempermutasikan cipherteks dengan matriks permutasi IP^{-1}. Pra-keluaran dari *deciphering* adalah adalah (L_0, R_0). Dengan permutasi awal IP akan didapatkan kembali blok plainteks semula.
4. Tinjau kembali proses pembangkitan kunci internal pada Gambar Selama *deciphering*, K_{16} dihasilkan dari (C_{16}, D_{16}) dengan permutasi PC-2. Tentu saja (C_{16}, D_{16}) tidak dapat diperoleh langsung pada permulaan *deciphering*. Tetapi karena (C_{16}, D_{16}) = (C_0, D_0), maka K_{16} dapat dihasilkan dari (C_0, D_0) tanpa perlu lagi melakukan pergeseran bit. Catatlah bahwa (C_0, D_0) yang merupakan bit-bit dari kunci eksternal *K* yang diberikan pengguna pada waktu dekripsi.
5. Selanjutnya, K_{15} dihasilkan dari (C_{15}, D_{15}) yang mana (C_{15}, D_{15}) diperoleh dengan menggeser C_{16} (yang sama dengan C_0) dan D_{16} (yang sama dengan C_0) satu bit ke kanan. Sisanya, K_{14} sampai K_1 dihasilkan dari (C_{14}, D_{14}) sampai (C_1, D_1). Catatlah bahwa (C_{i-1}, D_{i-1}) diperoleh dengan menggeser C_i dan D_i dengan cara yang sama seperti pada Tabel 1, tetapi pergeseran kiri (*left shift*) diganti menjadi pergeseran kanan (*right shift*).

3.3 Mode *DES*

Menurut (Munir, 2006) *DES* dapat di operasikan dengan *mode*, *ECB, CBC, OFB,* dan *CFB.* Namun karena kesederhanaannya, *mode ECB* lebih sering di gunakan pada paket program komersil meskipun sangat rentan terhadap serangan *Mode CBC* lebih *kompleks* dari pada *ECB* namu memberikan tingkat keamanan yang lebih bagus dari mode *ECB.* mode *CBC* hanya kadang-kadang saja digunakan.

3.3.1 *ECB*

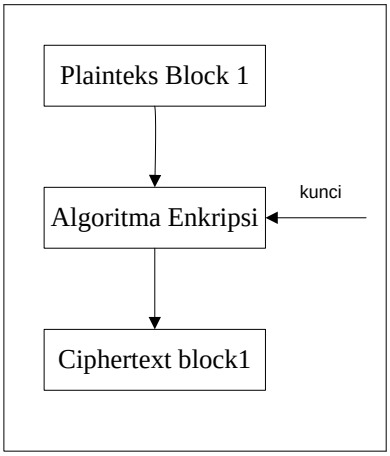
Pada mode electronic code book *ECB* ini suatu blok kode yang panjang dibagi dalam bentuk urutan binary menjadi satu blok tanpa mempengaruhi blok blok lain. Satu blok terdiri dari 64 bit atau 128 bit. Setiap blok merupakan bagian dari pesan yang dienkripsi. Kata code book di dalam *ECB* muncul dari fakta bahwa blok asli yang sama selalu dienkripsi menjadi blok teks kode yang sama maka secara teoritis dimungkinkan untuk membuat buku ukuran blok, semakin besar pula ukuran blok kode maka semakin besar pula pula ukuran buku kodenya. Misalnya jika blok berukuran 64bit, buku kode terdiri dari 2^{64}-1 buah kode (entry), yang berarti terlalu besar untuk disimpan. Lagi pula setiap kunci mempunyai buku kode yang berbeda. Secara matematis, enkripsi dengan mode ECB dinyatakan sebagai berikut :

C = chiperteks

P = Plainteks

$C_1 = E_k(P_i)$ dan deskripsi $P_i = D_k(C_i)$

Yang dalam hal ini P_i dan C_i masing-masing adalah blok teks-asli dan teks-kode ke-*i*



Gambar 3.2 Blok Kode Enkripsi Pada Mode ECB

Keuntungan mode *ECB*

1. Karena tiap blok plainteks dienkripsi secara independen, maka kita tidak perlu mengenkripsi file secara *liniear*. Kita dapan mengenkripsi 5 blok pertama,kemudian blok-blok ditengah dan seterusnya.

   Mode ECB cocok untuk mengenkripsi arsip (file) yang diakses secara acak, misalnya arsip-arsip basisdata. Jika basisdata dienkripsi dengan mode ECB, maka sembarang record dapat dienkripsi atau didekripsi secara independe dari record lainnya (dengan asumsi setiap record terdiri dari sejumlah blok diskrit yang sama banyaknya).

   Jika mode ECB dikerjakan dengan prosesor paralel (multiple processor), maka setiap prosesor dapat melakuka enkripsi atau dekripsi blok plainteks yang berbeda-beda
2. jika satu atau lebih bit pada blok cipherteks mengalami kesalahan, maka kesalahan ini hanya mempengaruhi cipherteks yang bersangkutan pada waktu dekripsi. Blok-blok cipherteks lainnya bila didekripsi tidak terpengaruh oleh kesalahan bit cipherteks tersebut.

Kelemahan mode *ECB*

1. karena bagian plainteks sering berlubang(sehingga terdapat blok-blok plainteks yang sama) maka hasil enkripsinya menghasilkan blok chiperteks yang sama.

   Di dalam email, pesan sering mengandung bagian yang redunda seperti string 0 atau spasi yang panjang, yang bila dienkripsi maka akan menghasilkan pola-pola cipherteks yang mudah dipecahkan dengan serangan yang berbasis statistic (menggunakan frekuensi kemunculan blok cipherteks). Selain itu email

merupakan struktur yang teratur yang menimbulkan pola-pola yang khas dalam cipherteksnya.

2. Pihak lawan dapat memanipulasi cipherteks untuk membodohi atau mengelabuhi penerima pesan. Manipulasi misalnya dengan menghapus beberapa buah blok atau menyisipkan beberapa buah blok cipherteks baru.

3.3.2 *Cipher Block Chaining (CBC)*

Pada mode CBC terdapat mekanisme umpan balik pada sebuah blok, yaitu blok plainteks current di-XOR-kan terlebih dahulu dengan dengan blok cipherteks hasil enkripsi sebelumnya. Selanjutnya hasil operasi XOR ini dimasukkan ke dalam fungsi enkripsi. Dengan demikian pada mode CBC, setiap blok cipherteks bergantung tidak hanya pada blok plainteksnya, tetapi juga pada seluruh blok plainteks sebelumnya. Dekripsi dilakukan dengan cara memasukkan blok cipherteks current ke dalam fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok cipherteks sebelumnya. Secara matematis proses enkripsi dapat dinyatakan sebagai berikut:

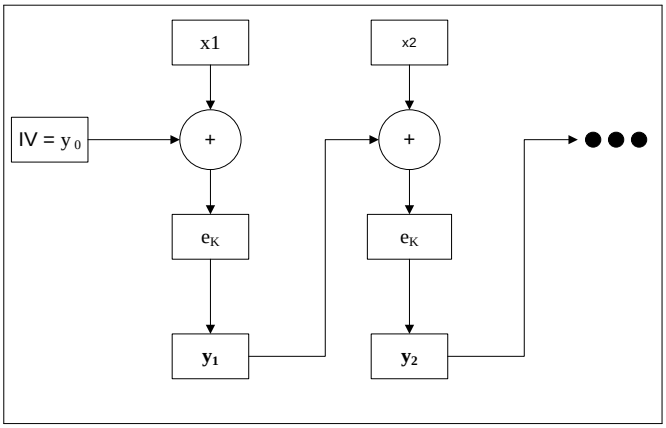
$$Ci=EK(Pi \text{ Xor } Ci\text{-}1)$$

sedangkan proses dekripsi dapat dinyatakan sebagai berikut:

$$Pi=DK(Ci) \text{ Xor } Ci\text{-}1$$

Dalam hal ini C0 merupakan IV (Initialization Vactor). IV dapat diberikan oleh pengguna atau dibangkitkan secara acak oleh aplikasi. IV ini merupakan rangkaian bit yang tidak bermakna dan hanya digunakan sebagai inisialisasi untuk membuat setiap blok cipherteks menjadi unik. Gambar 3 memperlihatkan skema enkripsi dan dekripsi dengan mode CBC.

Dengan mode CBC, kesalahan pada satu bit plainteks akan mempengaruhi blok cipherteks yang berkoresponden dan blok-blok cipherteks selanjutnya. Sedangkan kesalahan satu bit pada cipherteks hanya akan mempengaruhi satu blok plainteks yang berkoresponden dan satu bit pada blok berikutnya dengan posisi bit yang berkoresponden pula.



Gambar 3.3 Blok Kode Enkripsi Pada Mode CBC

3.3.3 *Cipher Feedback (CFB)*

Mode CBC memiliki kelemahan yaitu proses enkripsi hanya dapat dilakukan pada ukuran blok yang utuh sehingga mode CBC tidak efisien jika diterapkan pada aplikasi komunikasi data. Permasalahan ini dapat diatasi pada mode CFB. Mode CFB mengenkripsikan data dalam unit yang lebih kecil daripada ukuran blok. Proses enkripsi pada unit yang lebih kecil daripada ukuran blok ini membuat mode CFB berlaku seperti cipher aliran. Karena hal inilah, mode CFB dapat diterapkan pada aplikasi komunikasi data.Unit yang dienkripsi dapat berupa bit per bit. Bila unit yang dienkripsi berupa satu karakter setiap kalinya, maka mode CFB ini disebut CFB 8-bit. Mode ini membutuhkan sebuah

antrian yang berukuran sama dengan ukuran blok asukan. Secara formal, proses enkripsi mode CFB n-bit dapat dinyatakan sebagai berikut:

$$Ci = Pi \text{ Xor } MSBm(EK(Xi))$$

$$Xi+1 = LSBm\text{-}n(Xi) \,||\, Ci$$

sedangkan proses dekripsi dapat dinyatakan sebagai berikut:

$$Pi = Ci \text{ Xor } MSBm(DK(Xi))$$

$$Xi+1 = LSBm\text{-}n(Xi) \,||\, Ci$$

Keterangan:

Xi = isi antrian dengan X1 adalah IV

E = fungsi enkripsi

K = kunci

M = panjang blok enkripsi

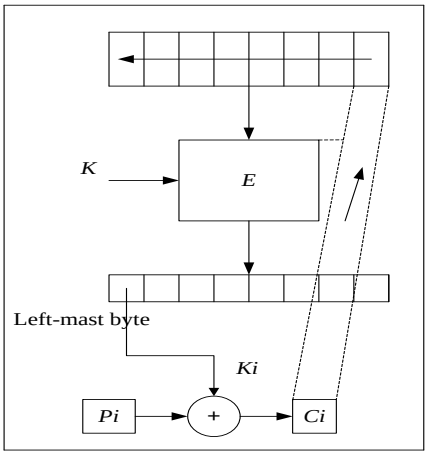
N = panjang unit enkripsi

|| = operator penyambungan (*concatenation*)

MSB = Most Significant Byte

LSB = Least Significant Byte

Mode CFB mempunyai keunikan tersendiri, yaitu untuk proses enkripsi dan dekripsi digunakan fungsi yang sama. Skema enkripsi dan dekripsi dengan mode CFB 8-bit dapat dilihat



Gambar 3.4 Proses Enkripsi CFB

3.3.4 *Output Feedback (OFB)*

Mode OFB berkerja dengan cara yang mirip dengan mode CFB, kecuali n-bit dari hasil fungsi enkripsi terhadap antrian disalin menjadi elemen paling kanan antrian. Gambar 5 menunjukkan skema enkripsi dan dekripsi pada mode OFB 8-bit. Secara formal, proses enkripsi mode OFB n-bit dapat dinyatakan sebagai berikut:

$$Ci = Pi \; XorMSBm(\; EK(Xi))$$

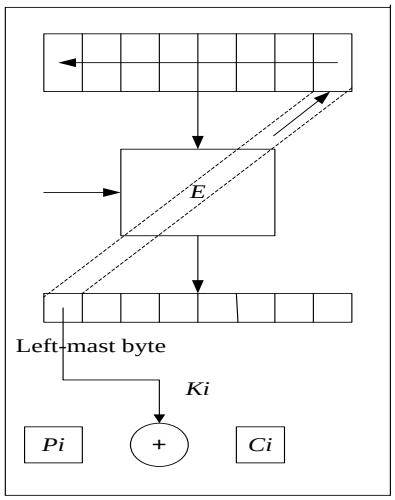
$$Xi+1 = \; LSBm\text{-}n(Xi) \; || \; MSBm($$

sedangkan proses dekripsi dapat dinyatakan sebagai berikut:

$$Pi = Ci \; Xor \; MSBm(\; DK(Xi))$$

$$Xi+1 = LSBm\text{-}n(Xi) \; || \; MSBm(\; EK(Xi))$$

Pada mode OFB tidak terdapat perambatan kesalahan. Kesalahan satu bit pada plainteks hanya mengakibatkan kesalahan satu bit yang berkoresponden pada cipherteks. Sebaliknya kesalahan satu bit pada cipherteks hanya mengakibatkan kesalahan satu bit yang berkoresponden pada plainteks.

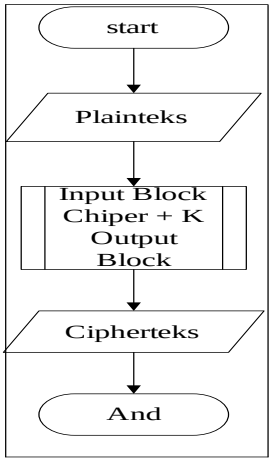


Gambar 3.5 Proses Enkripsi Mode *OFB*

3.3 Perancangan

Perancangan merupakan bagian dari metodologi pengembangan suatu perangkat lunak yang dilakukan setelah melalui tahapan analisis. Perancangan bertujuan untuk memberikan gambaran secara terperinci. Perancangan merupakan tahap lanjutan dari analisis, dimana pada perancangan digambarkan rancangan yang akan dibangun sebelum dilakukan pengkodean kedalam suatu bahasa pemrograman

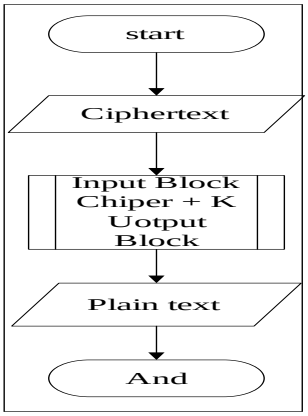
3.3.1 *Flowchart* Proses Enkripsi *DES* mode *ECB*



Gambar 3.6 *Flowchart* Proses Enkripsi Blok Kode ECB

1. Memulai proses enkripsi dengan blok berukuran 64 bit
2. Misalkan fungsi enkripsi E yang sederhana (tetapi lemah) adalah dengan meng XOR kan blok plainteks P_i dengan kunci K, kemudian geser secara wrapping bit bit dari P_i + K satu posisi ke kiri .
3. Setelah diproses maka menghasilkan cipherteks
4. Selesai

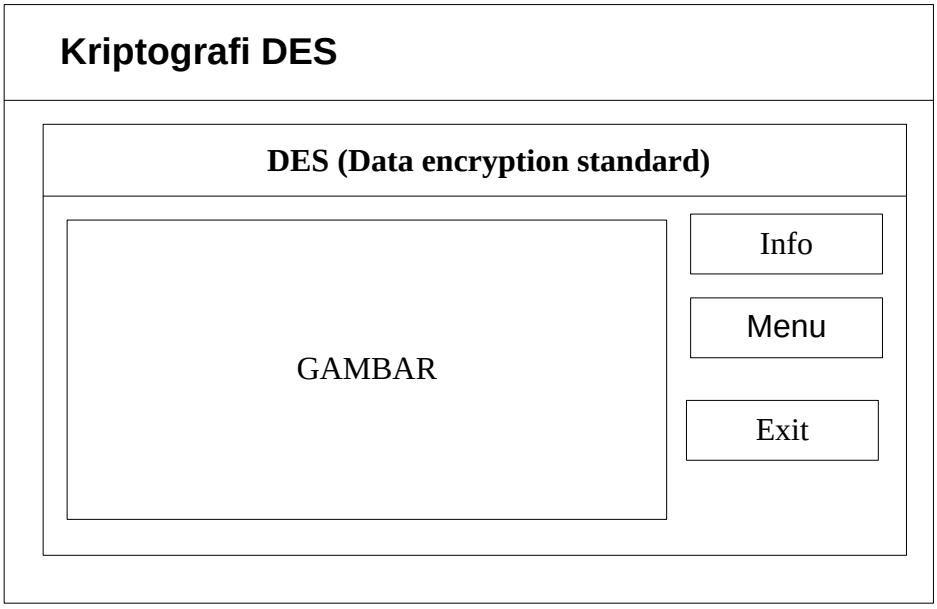
3.3.2 *Flowchart* Proses Deskripsi DES mode ECB



Gambar 3.7 *Flowchart* Deskripsi Blok Mode ECB

1. Memulai proses deskripsi dengan blok berukuran 64 bit
2. Blok cipherteks C_i hasil dari XOR dengan kunci K.
3. Setelah diproses maka menghasilkan plainteks.
4. Selesai

3.4 Perancangan *Interface* Kriptografi *DES*

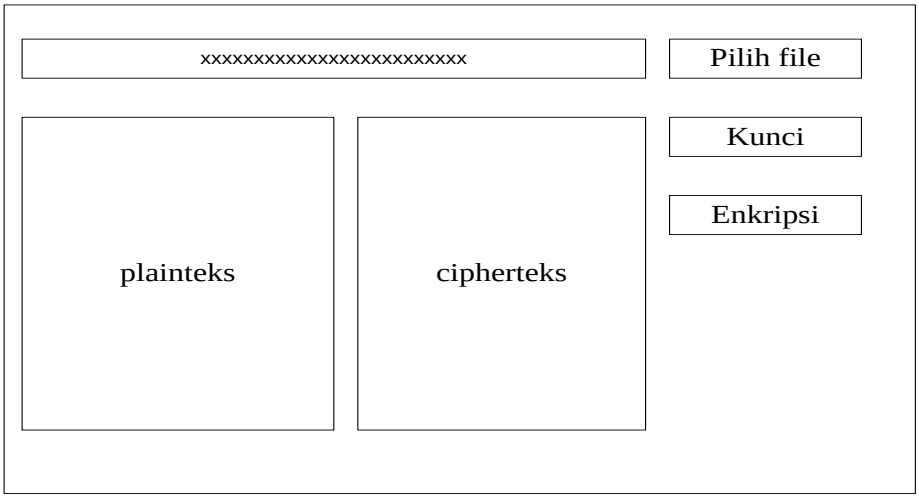


Gambar 3.8 Rancangan Dari Tampilan *Interface*

Dibawah ini merupakan keterangan dari gambar 3.8 diatas, yaitu :

1. *Frame* atas, merupakan judul atau nama rancangan yang akan dibuat
2. *Button* info yang berisi tentang kriptografi *DES* misalnya pengertian *DES,* sejarahnya, kelebihan dan kekurang *DES*
3. *Button* Menu yaitu terdapat proses enkripsi dan proses deskripsi yang mana proses enkripsi adalah proses penyandian teks asli kedalam kode-kode sedangan deskripsi kebalikan dari proses enkripsi
4. Button Exit

3.5 Rancangan Enkripsi

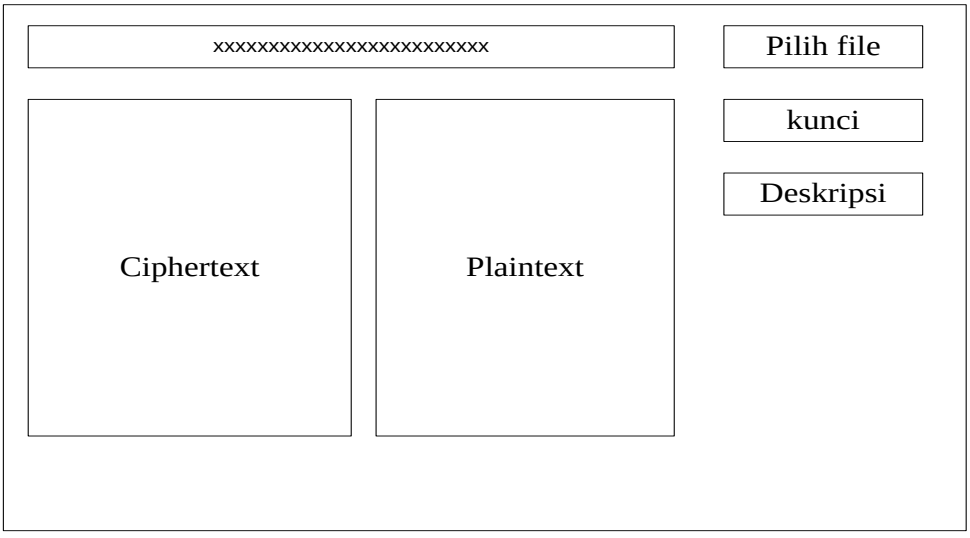


Gambar 3.9 Rancangan Proses Enkripsi

Dibawah ini merupakan keterangan dari gambar 3.9 diatas, yaitu :

1. pada button pilih file yaitu proses pencarian data yang ingin di enkripsi
2. button kunci
3. button enkripsi proses penyandian plainteks pesan menjadi cipherteks

3.6 Rancangan Deskripsi



Gambar 3.10 Rancangan Proses Deskripsi

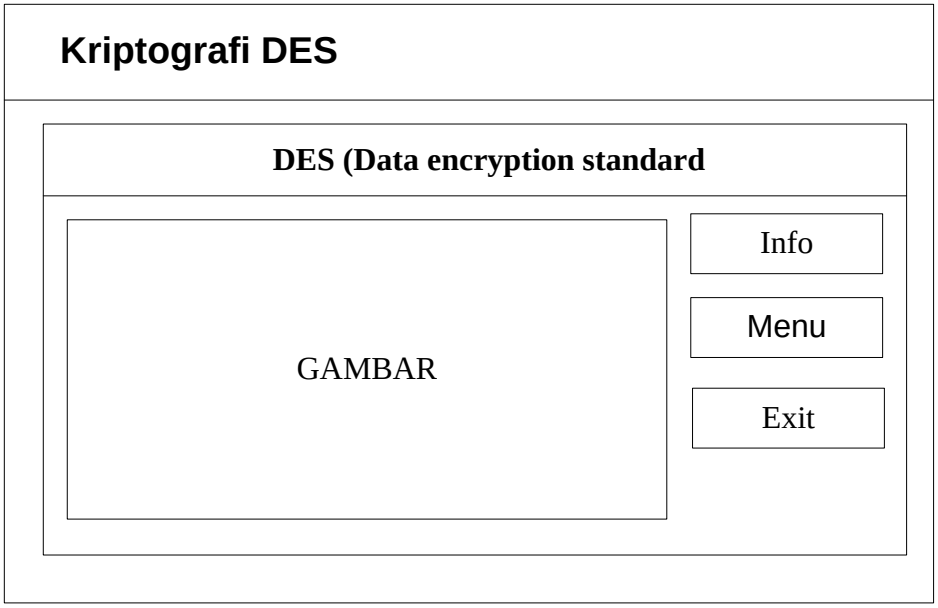
Dibawah ini merupakan keterangan dari gambar 3.10 diatas, yaitu :

1. pada button pilih file yaitu proses pencarian data yang ingin di deskripsi
2. button kunci
3. button deskripsi proses pengembalian cipherteks menjadi plainteks kembali

BAB IV

HASIL DAN PEMBAHASAN

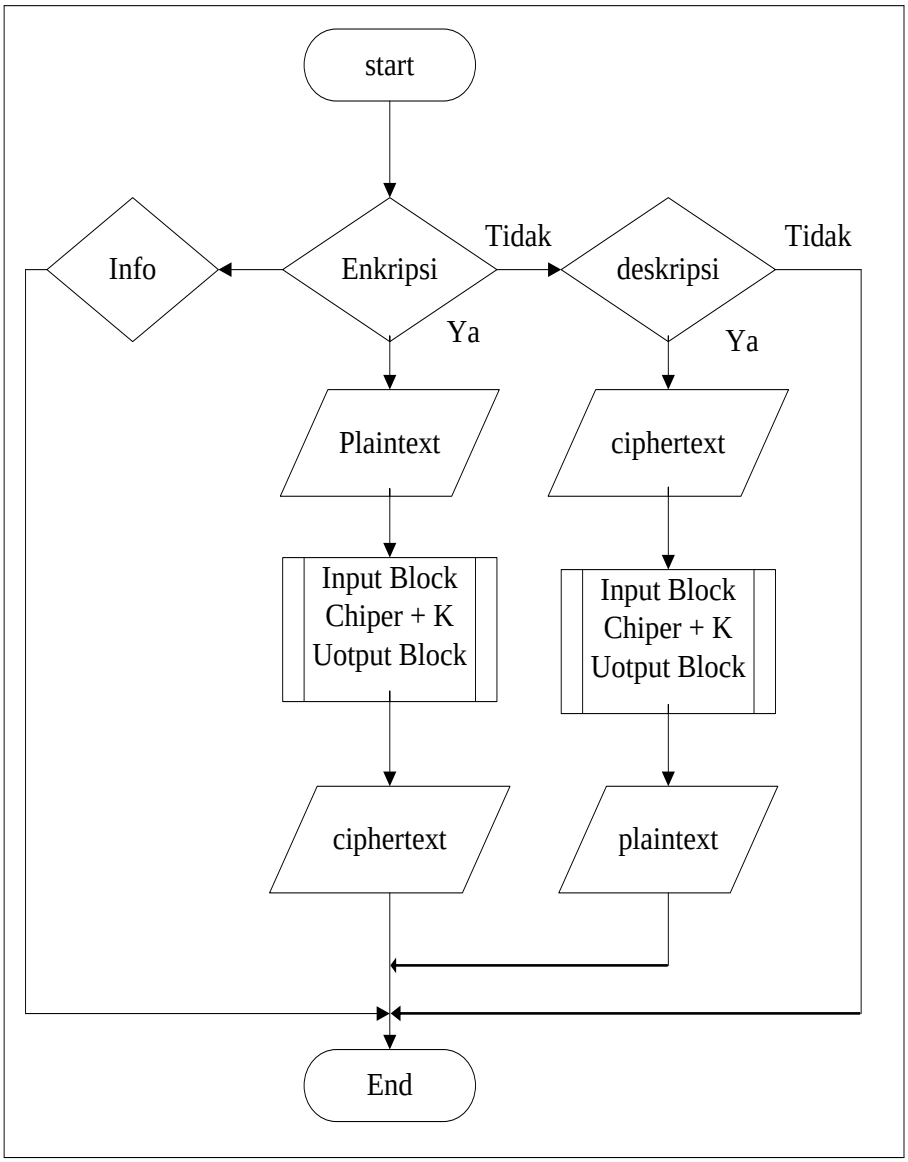
4.1 Rancangan Interface kriptografi *DES (Data Encryption Standard)*



Gambar 4.1 Rancangan Antar Muka

Pada halaman antar muka ini terdapat tulisan dan gambar seperi pada barisan pertama yaitu kriptografi DES dan baris ke dua DES (Data Encryption Standard), sedangkan halaman tengah terdapat Gambar dan di sebelah kanan terdapat *link* seperti *link* info yang berisi tentang informasi DES (Data Encryption

Standard), link Menu yang terdapat proses enkripsi dan deskripsi dan yang terakhir link Exit.

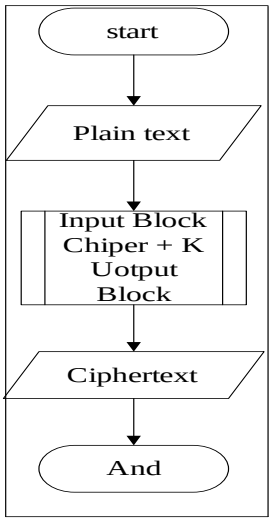


Gambar 4.2 flowchart Alur Kerja Pengguna

4.2 Proses Enkripsi

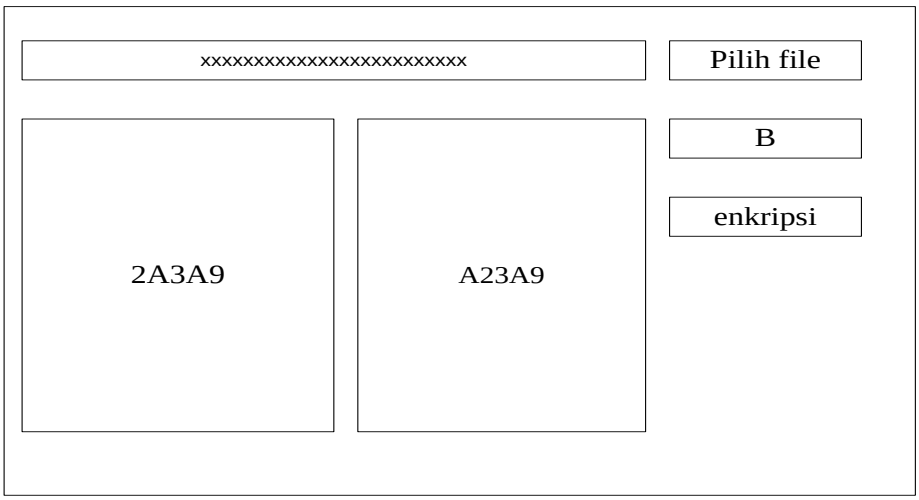
Enkripsi merupakan proses pengamanan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan

khusus. Adapun proses enkripsi dalam algoritma kriptografi *DES (Data Encyption standar)* pada mode ECB dapat dilihat pada gambar ini



Gambar 4.3 *Flowchart* Proses Enkripsi Blok Kode *ECB*

4.2.1 Rancangan Proses Enkripsi



Menurut (Munir, 2006) ini adalah proses enkripsi menggunkan Mode ECB dan menggunakan file doc yang kurang dari 64 bit.

Langkah 1 :User pilih file yang ingin di enkripsi

Langkah 2 :User menginputkan kunci dalam hal ini contoh kunci yang diinput hurup B

Langkah 3 :User mengklik tombol Enkripsi, maka plainteks akan dip roses menjadi cipherteks

Diketahui teks-asli (dalam biner) adalah 10100010001110101001

Teks asli dibagi menjadi blok-blok yang berukuran 4 bit :

1010 0010 0011 1010 1001 dalam notasi HEX adalah 2A3A9

Missal kunci K yang digunakan adalah 1011 yang panjangnya juga 4 bit dalam notasi HEX adalah B

Proses yang dilakukan yaitu dengan meng-XOR-kan blok teks asli P_i dengan K, kemudian geser secara wrapping bit-bit dari P_{i+} K satu posisi ke kiri

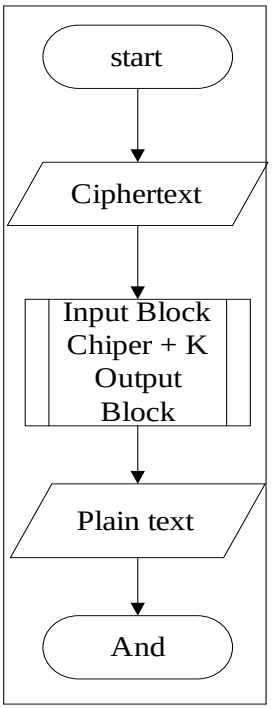
Proses enkripsi digambarkan sebagai berikut

1010 0010 0011 1010 1001
1011 1011 1011 1011 1011 +

Hasil XOR : 0001 1001 1000 0001 0010
Geser 1 bit ke kiri 0010 0011 0001 0010 0100
Dalam notasi HES: 2 3 1 2 4
Jadi, hasil enkripsi teks asli 10100010001110101001 (A23A9) adalah 00100011000100100100 (23124 dalam notasi HEX)

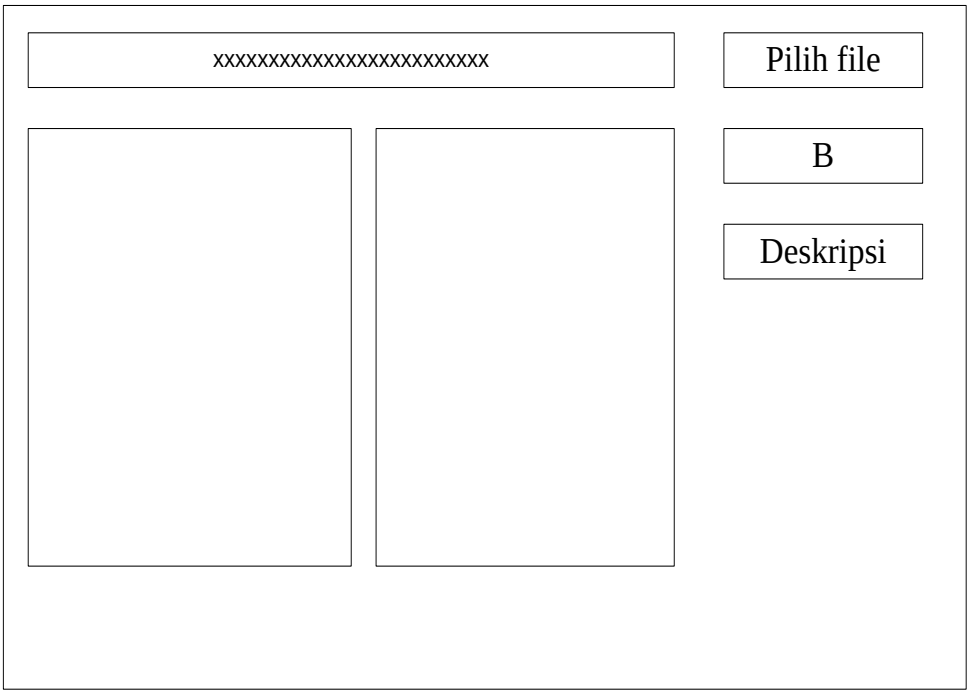
4.3 Proses Deskripsi

Deskripsi merupakan suatu proses penterjemahan sebuah karakter dengan kunci dan aturan tertentu menjadi sebuah karakter atau kalimat asli yang dapat dibaca dan diketahui informasi didalamnya. Adapun proses deskripsi dapa algoritma kriptografi *DES (Data Encyption standar)* pada mode ECB dapat dilihat pada gambar ini.



Gambar 4.5 *Flowchart* Deskripsi Blok Mode *ECB*

4.3.1 Rancangan Proses Deskripsi



Langkah 1 :User pilih file yang ingin di deskripsi

Langkah 2 :User menginputkan kunci dalam hal ini contoh kunci yang diinput hurup B

Langkah 3 :User mengklik tombol Enkripsi, maka plainteks akan dip roses menjadi plainteks

Contoh proses deskripsi

Diketahui cipherteks : 00011001100000010010 dibagi menjadi blok-blok yang berukuran 4 bit: 0001 1001 1000 0001 0010 dalam notasi HEX (19812)

Misalkan kunci K yang digunakan adalah panjangnya juga 4 bit : 1011

Proses deskripsi digambarkan sebagai berikut

```
0001 1001 1000 0001 0010
1011 1011 1011 1011 1011 +
_____________________________
1010 0010 0001 1010 1001
```

Makan hasil plainteks yang di dapan adalah 1010 0010 0001 1010 1001 atau dalam bilangan HEX A23A9

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil analisis dan penelitian dari uraian-uraian yang telah dikemukakan pada bab-bab sebelumnya tentang analisis dan perancangan keamanan data menggunakan algoritma kriptografi DES (Data Encryption Standard) makan akan dikemukakan kesimpulan sebagai berikut :

1. Berdasarkan dari penelitian ini, dapat disimpulkan bahwa Secara umum DES terbagi menjadi tiga kelompok, yaitu pemrosesan kunci, enkripsi data 64 bit, dan dekripsi data 64 bit. Dan algoritma kriptografi DES ini juga dapat menggunakan mode seperti ECB, CBC, CFB, OFB.
2. Penggunaan kunci merupakan sesuatu yang sangat penting dalam proses enkripsi dan dekripsi, sehingga dibutuhkan suatu kerahasiaan dalam pemakaian kuncinya

5.2 Saran

Dalam penggunaan kunci diusahakan mudah diingat dan disepakati oleh kedua belah pihak. Perancangan keamanan data menggunakan kriptografi *DES*

yang telah dibuat ini, mungkin terdapat kekurangan sehingga diharapkan akan ada pengembangan atau perbaikan dari perancangan ini.

DAFTAR PUSTAKA

Fatta, A. (2007). *Analisis dan Perancangan Sistem Informasi.* Yogyakarta: Andi.

Munir, R. (2006). *Kriptografi.* Bandung: Informatika.

Sadikin, R. (2012). *Kriptografi untuk Keamanan Jaringan.* Yogyakarta: Andi.

Simarmata, J. (2006). *Pengamanan Sistem Komputer Edisi I.* Yogyakarta: Andi.

Witten, L. (2004). *Metode Design dan Analisis Sistem Edisi 6.* Yogyakarta: Andi.