IMPLEMENTASI MODE OPERASI CIPHER BLOCK CHAINING (CBC) PADA PENGAMANAN DATA

Dewi Rosmala[1], Riki Aprian [2]

Jurusan Teknik Informatika
Institut Teknologi Nasional Bandung

ABSTRAK

Kerahasiaan dan keamanan data adalah hal yang sangat penting dalam komunikasi data, baik dengan tujuan keamanan bersama, maupun untuk privasi individu. Para pengguna komputer yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyiasati cara mengamankan informasi yang akan dikomunikasikan atau yang akan disimpan. Perlindungan terhadap kerahasiaan data meningkat, salah satu caranya dengan menerapkan ilmu kriptografi.

Kriptografi adalah salah satu ilmu yang digunakan untuk menjaga kerahasiaan dan keamanan data sudah berkembang sejak jaman Yunani kuno. Kriptografi semakin berkembang dari jaman ke jaman sampai saat ini. Salah satu metode kriptografi yang cukup handal, stabil dan menjadi induk dari algoritma – algoritma kriptografi yang populer saat ini adalah Cipher Block Chaining (CBC).

Cipher Block Chaining (CBC), mode ini merupakan mekanisme umpan balik (feedback) pada sebuah blok, dan dalam hal ini hasil enkripsi blok sebelumnya di umpan balikkan ke dalam enkripsi blok yang current. Caranya, blok plainteks yang current di-XOR-kan terlebih dahulu dengan blok ciphertext hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi. Dengan mode CBC, setiap blok ciphertext begantung tidak hanya pada blok plainteksnya tetapi juga pada seluruh blok plainteks sebelumnya.

Penulis mencoba turut serta membuat sebuah perangkat lunak untuk mengamankan data dengan metode kriptografi Cipher Block Chaining (CBC). Penulis memilih Cipher Block Chaining (CBC) dengan alasan kemudahan dalam mengimplementasikan metode tersebut. Perangkat lunak yang dirancang oleh penulis dapat melakukan proses enkripsi dan dekripsi untuk jenis file teks, dokumen dan gambar.

***Kata Kunci** : Perangkat Lunak, Kiptografi, Enkripsi, Cipher Block Chaining (CBC)*

ABSTRACT

Secrecy and security data are extremely important in communication data, either by security purposes along, nor for privacy of individuals. The a computer user who wanting to the data unknown by parties who are not interested always trying anticipate way secure information would be communicated or to be kept. Protection against secrecy data increase, well one way by applying science cryptography.

Cryptography science is one used for keeping and security data is growing since the ancient greeks. Cryptography growing from age to age till today. One method pretty reliable, cryptographic stable and into a nucleus of an algorithm cryptography algorithm popular today is ciphers block chaining (CBC).

Ciphers block chaining (CBC), that style is a feedback mechanism (feedback), on a block and in this result encription blok formerly in turn it into a block current encription. How, blok plainteks that current In XORright beforehand with encription blok ciphertext the previous next comes into results XOR function the encryption. With cbc, fashion any blok ciphertext begantung not only on blok plainteksnya but on the whole block plainteks before.

Writer try participate make a software to secure data by method cryptography ciphers block chaining (CBC). Choose ciphers writer block chaining (CBC) by reason ease in implementing this method. Software designed by writers can run the encryption of and dekripsi to a kind of text file, documents and pictures.

Keywords: *Software, Kiptografi, Encryption, Cipher Block Chaining (CBC)*

PENDAHULUAN

Latar Belakang

Kerahasiaan dan keamanan data adalah hal yang sangat penting dalam komunikasi data, baik dengan tujuan keamanan bersama, maupun untuk privasi individu. Para pengguna komputer yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha menyiasati cara mengamankan informasi yang akan dikomunikasikan atau yang akan disimpan. Sehingga perlindungan terhadap kerahasiaan data meningkat, salah satu cara adalah penyandian data atau enkripsi.

Enkripsi merupakan suatu proses pengubahan pesan asli menjadi karakter yang tidak dapat dibaca. Ada beberapa algoritma enkripsi yang biasa digunakan seperti *Block Cipher*, *Stream Cipher*, *Data Encryption Standard* (DES), *Triple* DES, *Advanced Encryption Standard* (AES), dan sebagainya. Dimana setiap algoritma memiliki karakteristik tersendiri. Sedangkan proses pengubahan kembali hasil enkripsi menjadi pesan asli dinamakan dekripsi.

Untuk merahasiakan data yang sangat penting maka digunakanlah metode kriptografi yang akan mengenkripsi dan deskripsikan data. Salah satu metode yang akan digunakan dalam pembuatan perangkat lunak ini adalah metode *Cipher Block Chaining* (CBC), karena metode ini diimplementasikan pada level *binary digit* (*bit*), sehingga pola proses enkripsi tidak dapat terbaca, serta proses enkripsi dan dekripsi memerlukan waktu yang singkat. Berdasarkan latar belakang tersebut, makadibuatlah sebuah tugas akhir yang berjudul *" Perangkat Lunak Enkripsi Dekripsi Data Menggunakan Algoritma Cipher Block Chaining (CBC) ".*

Rumusan Masalah

Berdasarkan latar belakang yang disebutkan diatas, permasalahan yang dirumuskan adalah sebagai berikut :

1. Bagaimana menjaga dan merahasiakan data menjadi *ciphertext* dengan menggunakan mode operasi CBC.
2. Bagaimana mengembalikan data yang sudah dienkripsi menjadi data asli menggunakan mode operasi CBC.

Tujuan

Membangun perangkat lunak dengan menggunakan mode operasi *Cipher Block Chaining* (CBC) pada pengamanan data dengan mengubah data yang dienkripsi menjadi *ciphertext*.

Batasan Masalah

Adapun batasan dalam pembangunan aplikasi ini adalah sebagai berikut:

1. Perangkat lunak dapat melakukan enkripsi untuk file teks (*.txt), *Rich Text Format* (*.rtf), file dokumen (*.doc), file *Adobe Acrobat* (*.pdf), file gambar (*.jpg, *.jpeg, *.jpe, *.bmp, *.gif, *.png, *.pcx, *.wmf, *.tif, *.psd), file *corel draw* (*.cdr), file *microsoft visio* (*.vsd).

2. Data yang telah dienkripsi dapat disimpan dengan *extention*sesuai dengan pilihan penguna.
3. Panjang kunci yang dapat dimasukkan oleh *user* maksimal 16 karakter atau 128 bit.
4. Data teks yang akan dienkripsi setiap 16 karakter
5.

Metodologi Penyusunan Penelitian
Kerangka Pengembangan Sistem

Metode yang digunakan dalam pengembangan perangkat lunak ini adalah Model *Waterfall*.Setiap tahap dijelaskan sebagai berikut :

1. *Sistem Engineering*, merupakan tahap untuk melakukan pengumpulan data dan penetapan kebutuhan semua elemen sistem.
2. *Analysis*, merupakan tahap untuk menganalisis hal-hal yang diperlukan dalam pelaksanaan proyek pembuatan atau pengembangan perangkat lunak.
3. *Design*, merupakan tahap penerjemahan dari keperluan atau data yang telah dianalisis ke dalam bentuk yang mudah dimengerti oleh pemakai (*user*).
4. *Coding*, merupakan tahap untuk menerjemahkan data atau pemecahan masalah yang telah dirancang ke dalam bahasa pemrograman komputer yang telah ditentukan.
5. *Testing*, merupakan tahap untuk melakukan uji coba terhadap program yang telah dibuat.
6. *Maintenance*, merupakan tahap perawatan perangkat lunak yang telah selesai dibuat supaya berjalan sesuai dengan keinginan user dan terhindar dari gangguan-gangguan yang menyebabkan kerusakan.

LANDASAN TEORI
Kriptografi[2]

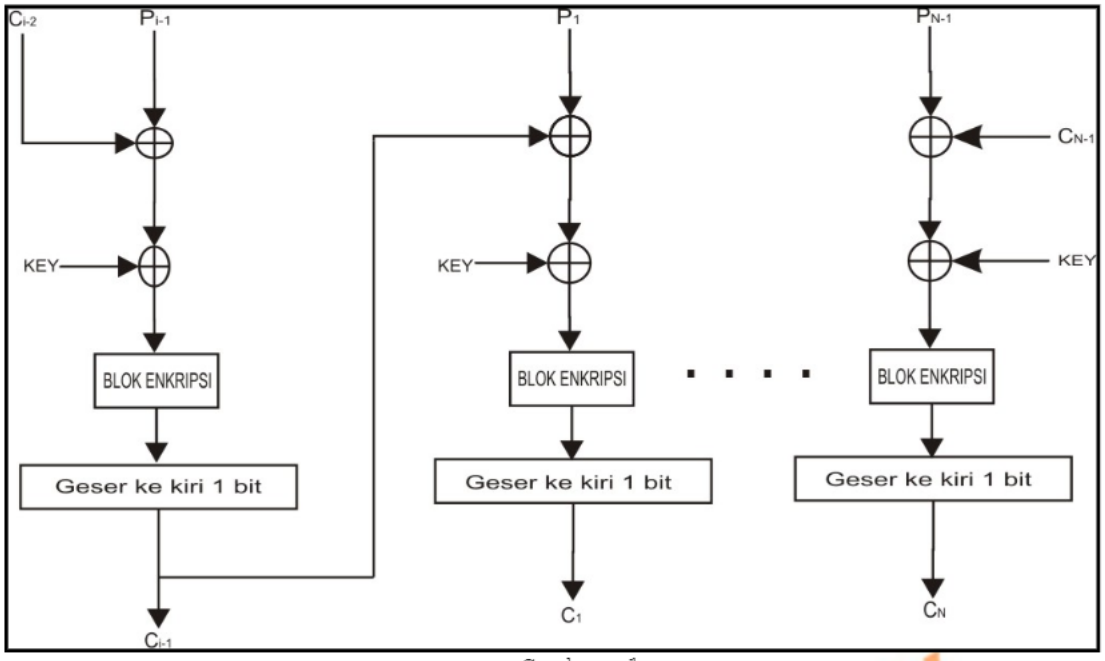
Kriptografi berasal dari bahasa Yunani yaitu *cryptos* yang berarti *secret* (rahasia) dan *graphein* yang berarti *writing* (menulis). Jadi kriptografi berarti *secret writing* (tulisan rahasia). Sedangkan definisi kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi.

Algoritma kriptografi selalu terdiri dari dua bagian, yaitu enkripsi dan dekripsi. Enkripsi *(encryption)* adalah proses untuk menyandikan *plaintext* atau *cleartext* menjadi bentuk *ciphertext*. Sedangkan dekripsi *(decryption)* adalah proses mengembalikan *ciphertext* menjadi *plaintext* semula. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci. Kunci biasanya berupa string atau deretan bilangan.

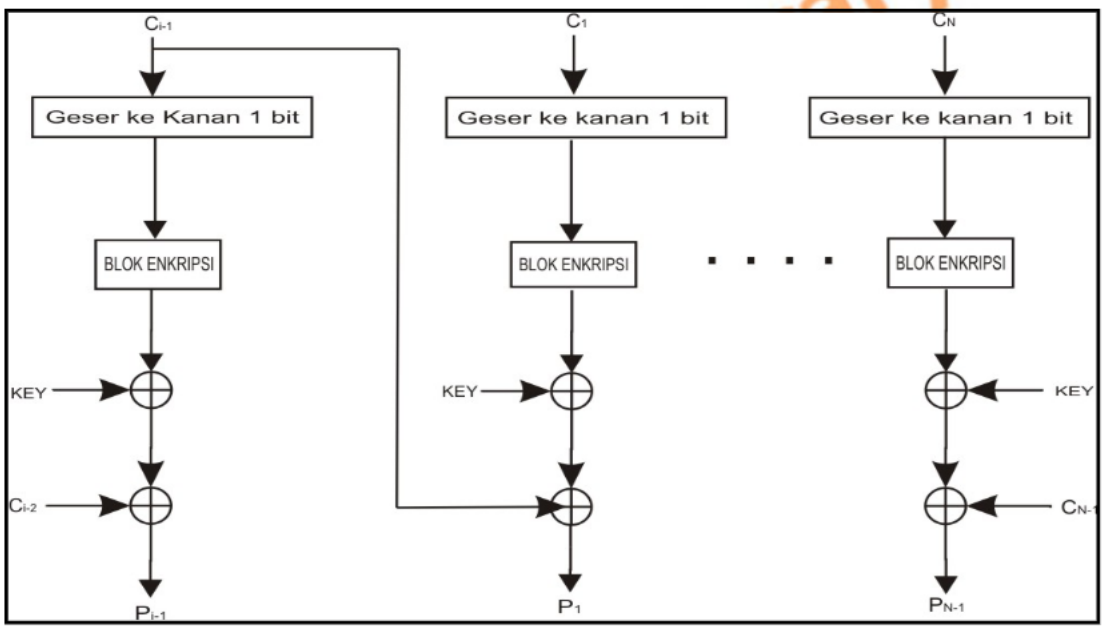
Mode *CipherBlockChaining* (CBC) [2]

Algoritma *Cipher Block Chaining* merupakan penerapan mekanisme umpan balik pada sebuah blok *bit* dimana hasil enkripsi blok sebelumnya diumpanbalikkan ke dalam proses enkripsi blok *current*. Caranya, blok *plaintext* yang *current* di-XOR-kan terlebih dahulu dengan blok *ciphertext* hasil enkripsi sebelumnya, selanjutnya hasil peng-XOR-an ini masuk ke dalam fungsi enkripsi. Dengan algoritma CBC, setiap blok *ciphertext* tidak hanya bergantung pada blok *plaintext*nya tetapi juga pada seluruh blok *plaintext* sebelumnya.

Dekripsi dilakukan dengan memasukkan blok *ciphertext* yang *current* ke fungsi dekripsi, kemudian meng-XOR-kan hasilnya dengan blok *ciphertext* sebelumnya. Dalam hal ini, blok *ciphertext* sebelumnya berfungsi sebagai umpan maju *(feedforward)* pada akhir proses dekripsi.



Gambar 1
Skema Enkripsi dengan Algoritma CBC



Gambar 2
Skema Deskripsi dengan Algoritma CBC

Secara matematis, enkripsi dan dekripsi dengan algoritma CBC dinyatakan sebagai:

$$C_i = E_k(P_i \oplus C_{i-1})$$

$$P_i = D_k(C_i) \oplus C_{i-1} \quad \text{Rumus Mode Operasi CBC.....(1)}$$

Analisis dan Perancangan

Kebutuhan Perangkat Lunak

Perangkat lunak ini diharapkan dapat memenuhi kebutuhan-kebutuhan antara lain sebagai berikut :

1. Perangkat lunak dapat melakukan enkripsi untuk file teks (*.txt), *rich text format* (*.rtf), file dokumen (*.doc),

file *adobe acrobat* (*.pdf), file gambar (*.jpg, *.jpeg, *.jpe, *.bmp, *.gif, *.png, *.pcx, *.wmf, *.tif , *.psd), file *corel draw* (*.cdr), file *microsoft visio* (*.vsd).

2. Perangkat lunak dapat membuka semua file yang telah dienkripsi.
3. Untuk melakukan proses enkripsi dan dekripsi dibutuhkan kunci.
4. *Extention* file hasil dekripsi akan sesuai dengan *extention* file semula, yaitu *extention* file sebelum file tersebut di enkripsi.

Algoritma CBC Proses Enkripsi

Adapun susunan algoritma *cipher block chaining* dalam proses enkripsi adalah sebagai berikut:

1. Membagi *plaintext* menjadi blok yang telah ditentukan ukurannya, pada perangkat lunak ini tiap blok berukuran 128 bit
2. Satu blok plain text yang telah dibagi itu di-XOR-kan dengan IV (*Initialization Vector*) yang telah ditentukan
3. Kemudian hasil tersebut di-XOR-kan lagi dengan kunci
4. Hasil XOR tersebut di geser satu bit ke kiri
5. Hasil tersebut menjadi IV untuk blok berikutnya
6. Proses diulang sampai blok berakhir

Contoh Enkripsi :

Misal :

```
Kunci = AAAABBBBCCCCDDDD
Hex                                =
41414141424242424343434344444444
IV/C0                              =
20,25,30,14,255,254,244,233,150,14
0,111,125,13,55,16,180
Hex                                =
14191E0EFFFEF4E9968C677D0D3710B4

Plainteks = RIKIAPRIANEFENDI
Hex                                =
52494B4941505249414E4546454E4449

P              XOR              IV
           =52494B4941505249414E4
           546454E4449
           XOR14191E0EFFFEF4E9968
           C677D0D3710B4
           =
           66505547BEAEA6A0D7C222
           3B487954FD

Hasil XOR Kunci   =
                  66505547BEAEA6A0D7
                  C2223B487954FD
                  XOR
                  414141414242424243
                  43434344444444
                  =
                  27111406FCECE4E295
                  8161780C3D10B9
Geser    1    bit    ke    kiri    =
                  4E22280DF9D9C9C52B
                  02C2F0187A2172

Hasilnya = N"(13■┘╔┼+2┬≡24z!r
```

Algoritma CBC Proses Dekripsi

Sedangkan susunan algoritma *cipher block chaining* dalam proses dekripsi adalah sebagai berikut:

1. Membagi *plaintext* menjadi blok yang telah ditentukan ukurannya, pada perangkat lunak ini tiap blok berukuran 128 bit
2. Proses dekripsi dilakukan dari blok paling akhir
3. Hasil pembagian blok tersebut di geser 1 bit ke kanan
4. Kemudian hasil pergeseran tersebut di-XOR-kan dengan kunci
5. Kemudian hasil tersebut di-XOR-kan lagi dengan blok *ciphertext* sebelumnya
6. Proses diulang sampai blok paling awal, blok paling awal di-XOR-kan dengan IV

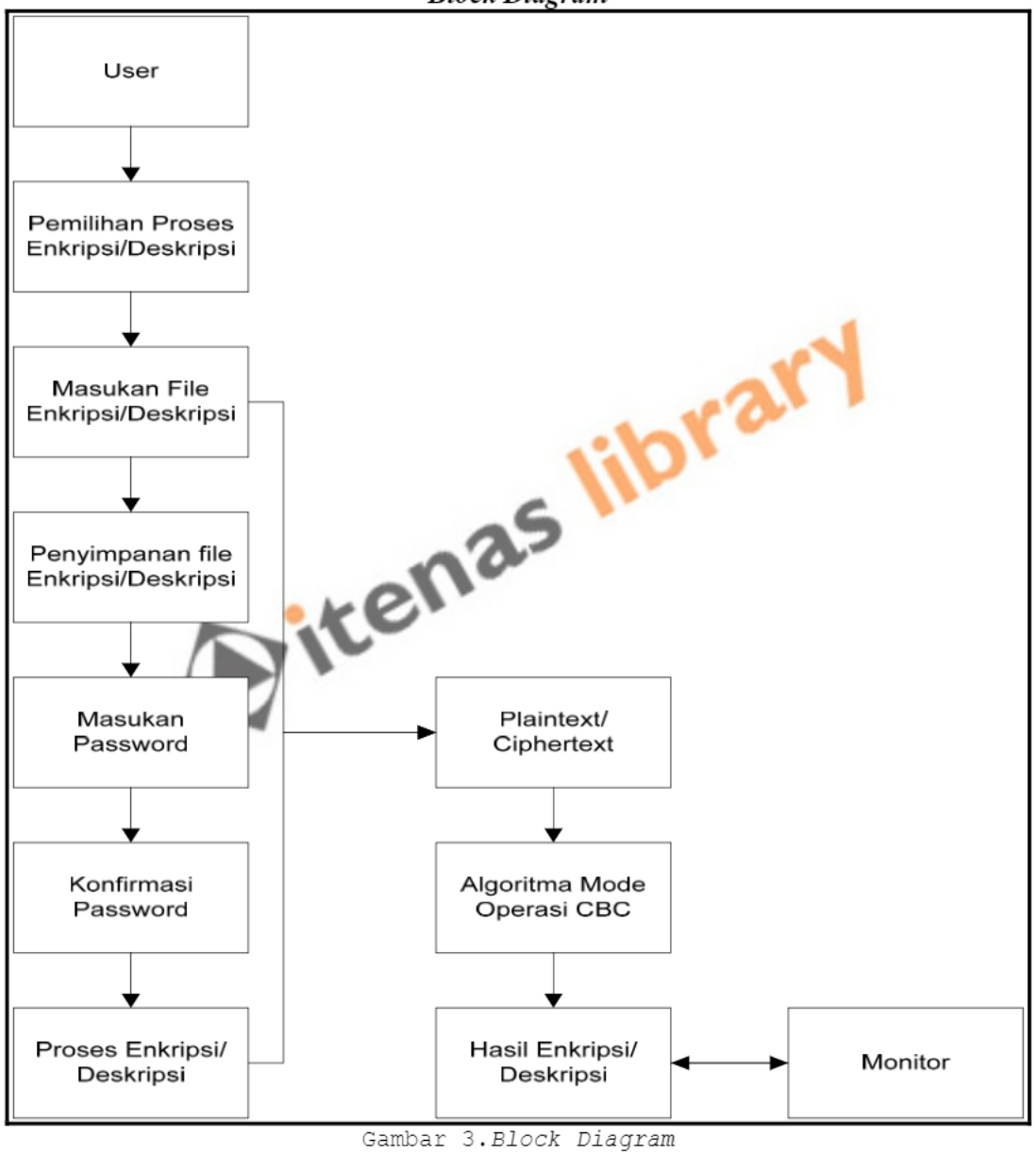
Contoh Dekripsi :

```
Ciphertext = N"(13■┘╔┼+2┬≡24z!r
Hex            =
               4E22280DF9D9C9C52B02
               C2F0187A2172
Geser     Kanan     1     Bit     =
                27111406FCECE4E2958
                161780C3D10B9
Hasil XOR Kunci  =
                27111406FCECE4E295
                8161780C3D10B9
                XOR
                414141414242424243
                43434344444444
```

```
                =                                          14191E0EFFFEF4E9968C
                66505547BEAEA6A0D7                         677D0D3710B4
                C2223B487954FD                             =
                                                           52494B4941505249414E
Hasil XOR IV    =                                          4546454E4449
              66505547BEAEA6A0D7C2
              223B487954FD      XOR       Hasilnya     =     RIKIAPRIANEFENDI
```

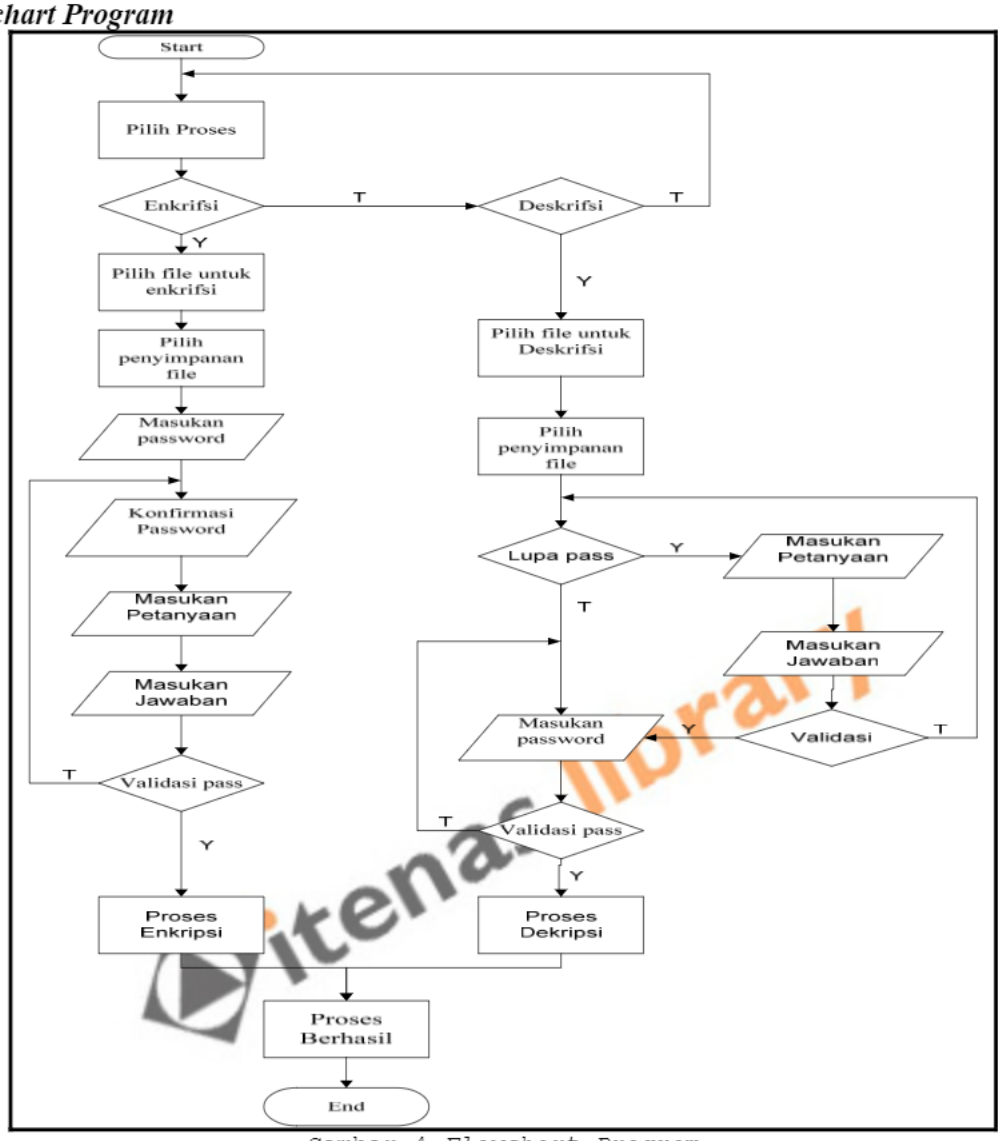
PERANCANGAN

Block Diagram



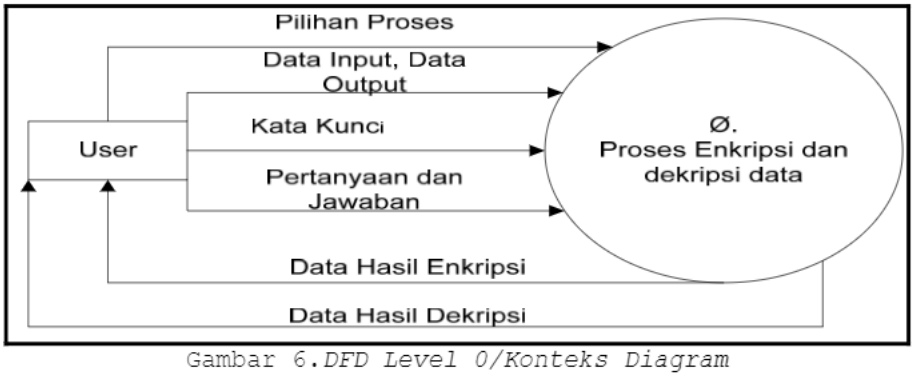
Gambar 3.*Block Diagram*

Flowchart Program

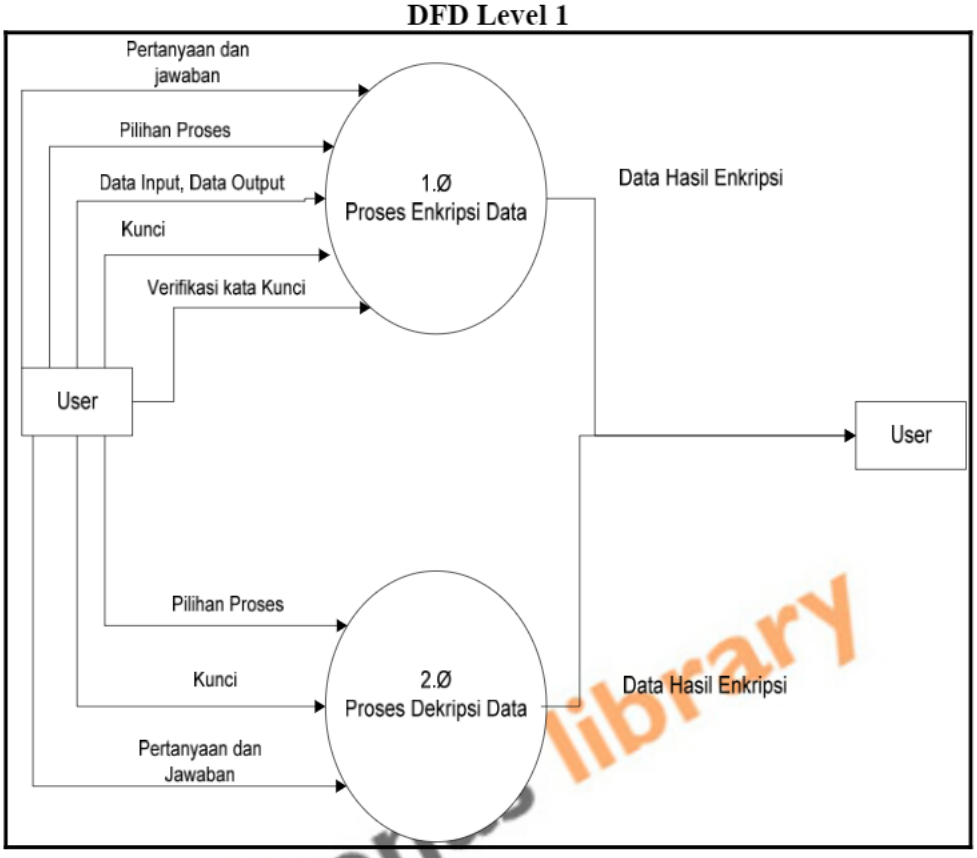


Gambar 4.*Flowchart Program*

DFD Level 0 / Konteks Diagra



Gambar 6.*DFD Level 0/Konteks Diagram*



Gambar 7.*DFD Level 1*

IMPLEMENTASI DAN PENGUJIAN

Perangkat Keras Yang Digunakan

Tabel 2.Perangkat Keras yang digunakan

Hardware	Spesifikasi
Prosesor	Intel Pentium(R) 4 CPU 1.80 GHz
Mainboard	ASUS
Memory	1024 Mb
Harddisk	320 Gb
VGA Card	ATI Radeon 9550 / X1050 Series
Monitor	Samsung SyncMaster 551v

Pemilihan Perangkat Lunak

Perangkat lunak yang dipilih oleh penulis untuk penerapan sistem yang telah dirancang dan dibuat oleh penulis adalah sebagai berikut :

1. Windows Xp Professional

Sistem operasi pada komputer yang digunakan dalam pembuatan perangkat lunak enkripsi dekripsi adalah Windows Xp Professional karena sistem operasi ini umum digunakan. Selain itu sistem operasi ini memiliki konfigurasi yang baik untuk mendukung kerja perangkat lunak enkripsi dekripsi data ini.

2. Borland Delphi 6.0

Dengan memakai Delphi, penulis dapat membuat perangkat lunak enkripsi dekripsi data ini dengan cukup mudah.

Tampilan Sistem

Proses pembangunan aplikasi, berikut inimerupakan tampilan dari aplikasi yang dibuat :

Tampilan Pemilihan Proses Enkripsi

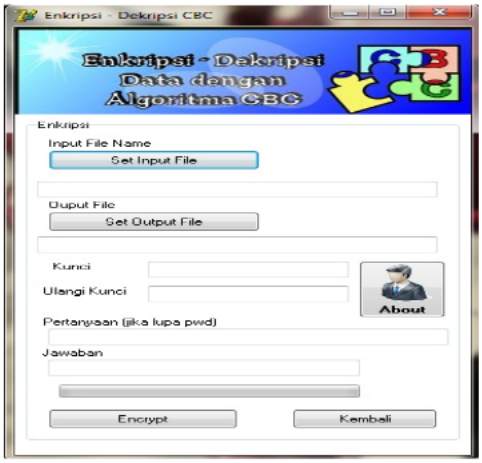
Berikut adalah tampilan form pada saat pemilihan proses :

Gambar 8
Tampilan Pemilihan Proses

Tampilan pemilihan proses Enkripsi ini adalah tampilan awal dari perangkat lunak enkripsi data menggunakan algoritma kriptografi CBC. Setelah memilih proses yang diinginkan, *user* dapat memilih tombol selanjutnya, untuk proses lebih lanjut. *User* juga dapat memilih untuk keluar dari perangkat lunak enkripsi dekripsi data, dengan memilih tombol keluar.

Tampilan Pemilihan File Enkripsi

Berikut adalah tampilan form pada saat *user* memilih tombol selanjutnya pada form pemilihan proses enkripsi :

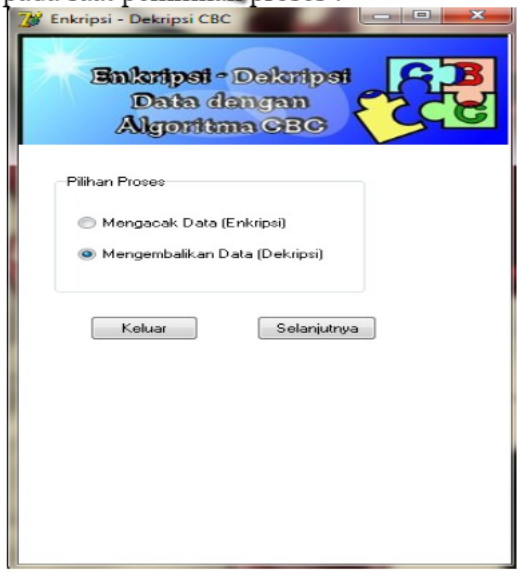


Gambar 9
Tampilan Pemilihan File Enkripsi

Pada tampilan ini *user* diminta untuk memasukan file yang akan diproses, menyimpan data hasil enkripsi yang sudah diproses, memasukan kata sandi, konfirmasi kata sandi, memasukan pertanyaan dan jawaban. Setelah *user* melakuan perintah tersebut maka *user* dapat memilih tombol *Encrypt* sehingga proses dapat dilanjutkan.

Tampilan Pemilihan Proses Dekripsi

Berikut adalah tampilan form pada saat pemilihan proses :

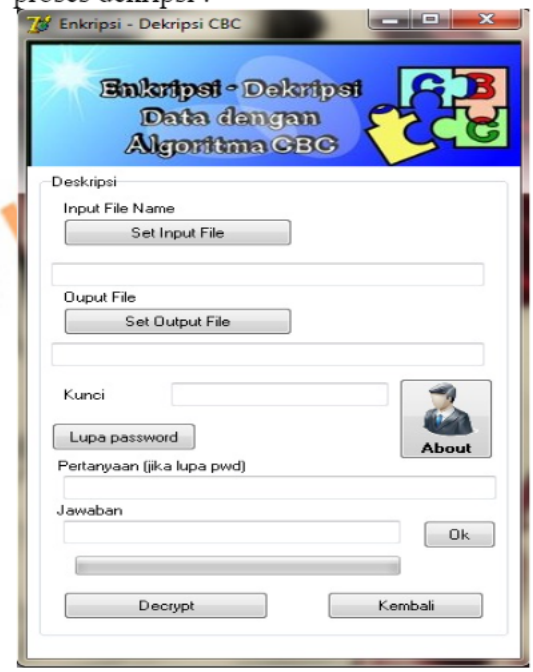


Gambar 10
Tampilan Pemilihan Proses

Tampilan pemilihan proses Dekripsi ini adalah tampilan awal dari perangkat lunak dekripsi data menggunakan algoritma kriptografi CBC. Setelah memilih proses yang diinginkan, *user* dapat memilih tombol selanjutnya, untuk proses lebih lanjut. *User* juga dapat memilih untuk keluar dari perangkat lunak enkripsi dekripsi data, dengan memilih tombol keluar.

Tampilan Pemilihan File Dekripsi

Berikut adalah tampilan form pada saat *user* memilih tombol selanjutnya pada form pemilihan proses dekripsi :



Gambar 11
Tampilan Pemilihan File Dekripsi

Pada tampilan ini *user* diminta untuk memasukan file hasil enkripsi yang akan diproses, menyimpan hasil dekripsi yang sudah diproses, memasukan kata sandi, jika lupa kunci *user* dapat menjawab pertanyaan, jika jawabannya benar maka perangkat lunak akan mengirimkan pesan yang isinya kunci pada saat proses enkripsi. Setelah *user* melakuan perintah

tersebut maka *user* dapat memilih tombol *Decrypt* sehingga proses dapat dilanjutkan.

PENUTUP

Kesimpulan

Setelah melalui tahapan pengujian perangkat lunak enkripsi dekripsi data menggunakan algoritma kriptografi *Cipher Block Chaining* ini, bahwa disimpulkan perangkat lunak pengamanan data menggunakan metode *Cipher Block Chaining* (CBC) dapat merahasiahkan data dengan cara merubah data seperti file *teks*, *Rich Text Format*, file dokumen menjadi ciphertext yang tidak dapat dimengerti. Sedangkan file gambar setelah dienkripsi tidak dapat dibuka karena datanya telah rusak, file *microsoft visio* dan file *Adobe Acrobat* setelah dienkripsi akan menampilkan pesan *error* karena datanya *corrupted.* Perangkat Lunak ini juga berhasil mengembalikan data yang sudah dienkripsi menjadi data asli.

DAFTAR PUSTAKA

1. Mardianto. 2010. *Enkripsi SMS Menggunakan Elliptic Curve Cryptography (ECC)*. Bandung : Institut Teknologi Telkom
2. Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Informatika.
3. Ratih. 2007. *Studi dan Implementasi Enkripsi Pengiriman Pesan Suara Menggunakan Algoritma Twofish.* Bandung : Institut Teknologi Bandung
4. Wisnu, Ranga. 2008. *Implementasi Algoritma RC6 Untuk Enkripsi SMS pada Telepon Seluler*. Bandung : Institut Teknologi Bandung.