PENERAPAN METODE PENGAMANAN DATA ENSKRIPSI DAN DESKRIPSI MENGGUNAKAN METODE TWOFISH PADA PT. GAYA MAKMUR TRACTOR

Arif Novianto [1], Vivi Sahfitri [2], Baibul Tujni [3]
Mahasiswa Universitas Bina Darma [1], Dosen Universitas Bina Darma [2],
Dosen Universitas Bina Darma [3]
Jalan Jendral Ahmad Yani No. 12 Palembang
email: arif.nov@gmail.com, vivi_sahfitri@mail.binadarma.ac.id, baibul_tujni@mail.binadarma.ac.id

Abstrak - PT. Gaya Makmur Tractor merupakan salah satu perusahaan kontraktor yang ada di Kota Palembang yang berpusat di Kota Jakarta, sering melakukan pengiriman laporan melalui email. Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi, terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak tertentu, sehingga perlu dilakukan penyandian data supaya beberapa pihak yang tidak memiliki kewenangan tidak akan dapat membuka informasi yang dikirim. Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan sistem kriptografi yaitu dengan menyediakan isi informasi (*plaintext*) menjadi isi yang tidak dipahami melalui proses enkripsi (*encipher*), dan untuk memperoleh kembali informasi yang asli, dilakukan proses deskripsi (*decipher*), dengan menggunakan kunci yang benar. Berdasarkan latar belakang inilah maka peneliti berkeinginan mengangkat permasalahan tersebut sebagai bahan penelitian. Adapun judul penelitian adalah "Penerapan Metode Pengamanan Data *Enskripsi* dan *Deskripsi* Menggunakan Metode *Twofish* Pada PT. Gaya Makmur Tractor".

Kata Kunci : Enskripsi, Deskripsi, Metode Twofish

1. PENDAHULUAN

Dengan berkembangnya teknologi informasi diharapkan dapat menjadi media yang paling efektif untuk mencari dan menyebarkan informasi. Salah satunya adalah komputer yang saat ini sudah bukan barang baru dan kini tidak hanya digunakan untuk kepentingan perkantoran tetapi juga dapat digunakan untuk kepentingan bisnis. Oleh sebab itu, komputer telah menjadi kebutuhan manusia dan memberikan manfaat yang luar biasa, bukan saja digunakan oleh ribuan pakar untuk mengakses komputer, berbagi *file*, dan mengirim *e-mail* (surat elektronik), tetapi lebih dari itu komputer telah menciptakan suatu sistem informasi global yang menjadikan

dunia ini semakin kecil. Hal ini dapat dipahami karena dengan adanya komputer, suatu informasi yang dahulu sangat sulit diperoleh, kini semuanya bisa diperoleh hanya dalam waktu hitungan menit.

Teknologi informasi yang didukung oleh perkembangan perangkat keras (*Hardware*) dan perangkat lunak (*Software*) secara langsung maupun tidak langsung. Sebagai contohnya yaitu para eksekutif yang banyak menggunakan teknologi sebagai alat bantu dalam mengambil keputusan. *Software* atau perangkat lunak merupakan perintah (program komputer) yang bila dieksekusi memberikan fungsi dan unjuk kerja seperti yang diinginkan atau yang mengatur struktur data memungkinkan program memanipulasi informasi secara professional dan mengatur dokumen yang menggambarkan operasi kegunaan program. Perangkat lunak komputer telah berkembang selama terahir diantaranya perangkat lunak pengolahan kata, perangkat lunak pengolahan angka, multiemdia, hiburan, manajemen *database* dan perangkat lunak keuangan.

Kriptografi adalah ilmu untuk menjaga keamanan pesan yang bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak bertanggung jawab. Terdapat dua konsep utama pada kriptografi yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi atau data yang hendak dikirim berupa data jelas (*plaintext*) diubah menjadi bentuk yang hampir tidak dikenali berupa data random (*ciphertext*) sebagai informasi awalnya dengan menggunakan algoritma tertentu. Sedangkan dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk yang tersamar (*ciphertext*) tersebut menjadi informasi awal (*plaintext*).

PT. Gaya Makmur Tractor merupakan salah satu perusahaan kontraktor yang ada di Kota Palembang yang berpusat di Kota Jakarta, sering melakukan pengiriman laporan melalui email. Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi, terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak tertentu, sehingga perlu dilakukan penyandian data supaya beberapa pihak yang tidak memiliki kewenangan tidak akan dapat membuka informasi yang dikirim. Salah satu cara yang digunakan untuk pengamanan data adalah

menggunakan sistem kriptografi yaitu dengan menyediakan isi informasi (*plaintext*) menjadi isi yang tidak dipahami melalui proses enkripsi (*encipher*), dan untuk memperoleh kembali informasi yang asli, dilakukan proses deskripsi (*decipher*), dengan menggunakan kunci yang benar.

Berdasarkan latar belakang inilah maka peneliti berkeinginan mengangkat permasalahan tersebut sebagai bahan penelitian. Adapun judul penelitian adalah "Penerapan Metode Pengamanan Data Enskripsi dan Deskripsi Menggunakan Metode Twofish Pada *PT. Gaya Makmur Tractor*" **.**

2. METODELOGI PENELITIAN

2.1 Waktu dan Tempat Penelitian

Penelitian penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode *twofish* pada *PT. Gaya Makmur Tractor* dilakukan mulai bulan Oktober 2011 sampai dengan Februari 2012.

2.2 Metode Pengumpulan Data

Dalam melakukan penelitian untuk mendapatkan data dan informasi, maka metode yang digunakan adalah metode studi pustaka, dalam hal ini yang akan dilakukan adalah melihat serta mempelajari permasalahan yang ada berdasarkan jurnal pada penelitian sebelumnya dan jurnal yang ada di *internet* yang berkaitan dengan data enskripsi dan deskripsi metode *twofish*.

2.3 Metode Pengembangan Perangkat Lunak

Menurut Pressman (2002:36) metode Pengembangan Perangkat Lunak terdiri dari berbagai jenis antara lain : Metode pengembangan Perangkat Lunak untuk penerapan metode pengamanan data enkripsi dan deskripsi menggunakan mode *chiper electronik code book* menggunakan model sekuensial linier untuk rekayasa perangkat lunak sering disebut juga dengan "Siklus Kehidupan Klasik" atau "Model Air Terjun". Model sekuensial linier melingkupi aktivitas-aktivitas sebagai berikut :

1. Rekayasa dan Pemodelan Perangkat Lunak, Pada aktivitas ini, pekerjaan dimulai dengan membangun syarat dari semua elemen sistem dan mengalokasian beberapa subset dari kebutuhan ke perangkat lunak.
2. Analisis Kebutuhan Perangkat Lunak, Untuk memahami sifat program yang dibangun, analisis harus memahami domain informasi,

tingkah laku, unjuk kerja, dan antara muka *(interface)* yang dibutuhkan.

3. Rancangan Perangkat Lunak, Proses rancangan menerjemahkan syarat/kebutuhan kedalam sebuah representasi perangkat lunak yang dapat diperkirakan demi kualitas sebelum dimulai pemunculan kode. Sebagaimana persyaratan, rancangan/desain didokumentasikan dan menjadi bagian konfigurasi perangkat lunak.
4. Pengkodean Perangkat Lunak, Dalam pembuatan perangkat lunak peneliti menggunakan *scripting php* yang cenderung mudah dipelajari dan mempunyai fasilitas yang mendukung dalam menghubungkan dengan sistem *windows.*
5. Pengujian Perangkat Lunak, Proses pengujian berfokus pada logika internal perangkat lunak, memastikan bahwa semua pernyataan sudah diuji, dan pada eksternal fungsional, yaitu mengarangkan pengujian untuk menemukan kesalahan.

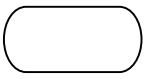
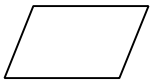
2.4 Manfaat Penelitian

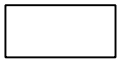
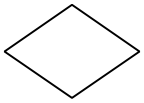
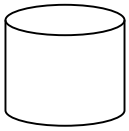
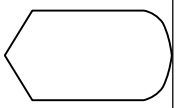
Manfaat dari penelitian ini adalah dengan adanya penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode twofish pada PT. Gaya Makmur Tractor ini dapat membantu pihak *PT. Gaya Makmur Tractor* dalam pengiriman dan penerimaan pesan terjaga kerahasiaan.

2.5 *Flowchart*

Flowchart berfungsi untuk memodelkan masukan, keluaran, proses maupun transaksi dengan menggunakan simbol-sombol tertentu seperti terminator termisi yang menandakan awal akhir dari suatu aliran. Data adalah pemasukan data secara digital melalui suatu media. Proses adalah poses yang dilakukan oleh komputer. *Decision* adalah pengambilan keputusan. *Magnetic disk* adalah data penyimpanan (data *storage*) dan display adalah menampilkan data pada monitor

Tabel 2.1 Simbol *Flowchart*

No.	Simbol	Keterangan
1	*Terminator* 	Termisi yang menandakan awal akhir dari suatu aliran.
2.	*Data* 	Pemasukan data secara digital melalui suatu media.

3.	*Proses* 	Proses yang dilakukan oleh komputer
4.	*Decision* 	Pengambilan Keputusan
5.	*Magnetic Disk* 	Data penyimpanan (data storage)
6.	*Display* 	Menampilkan data pada monitor

Sumber : Kristanto, Rekayasa Perangkat Lunak, Tahun 2004.

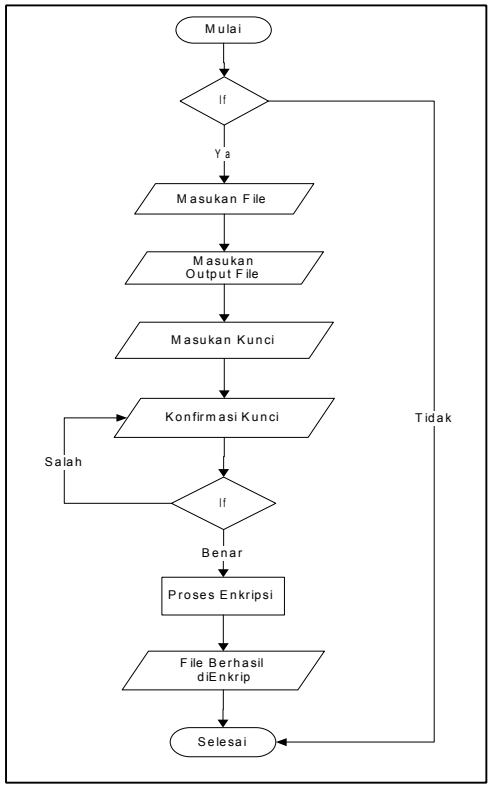
2.6 Perancangan

Perancangan dari Penerapan Metode Pengamanan Data *Enskripsi* dan *Deskripsi* Menggunakan Metode *Twofish* Pada PT. *Gaya Makmur Tractor* terdiri dari *flowchart* enkripsi, dekripsi dan perancangan tampilan.

2.6.1 Enkripsi dan Dekripsi *File*

1. Melakukan enkripsi *file*
   a. Pengguna memasukkan *input* kunci dan *file* yang akan di enkripsi. *File* yang dapat di enkrip antara lain adalah *file* teks, *file* gambar, file suara, dan lain sebagainya.
   b. Lakukan enkripsi *file* yang telah diinputkan.
   c. *File* yang telah terenkripsi menjadi file yang tidak terbaca.

Diagram alir untuk enkripsi *file* dapat dilihat pada gambar 2.2

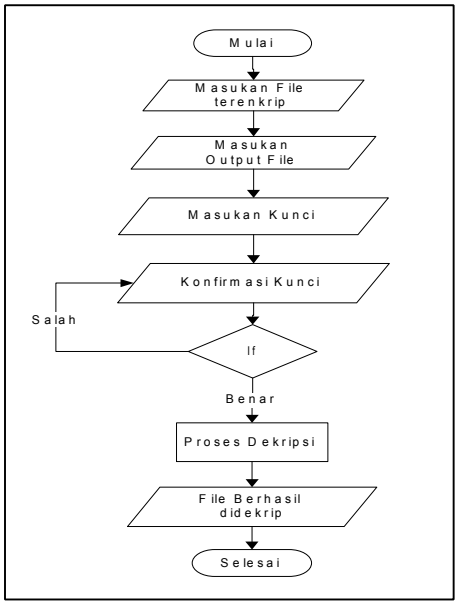


Gambar 2.2 Enkripsi File

2. Melakukan dekripsi *file*
   a. Masukkan kunci yang sama ketika file dienkripsi dan masukkan file yang sudah terenkripsi.
   b. Melakukan proses dekripsi untuk *file* yang telah diinputkan.

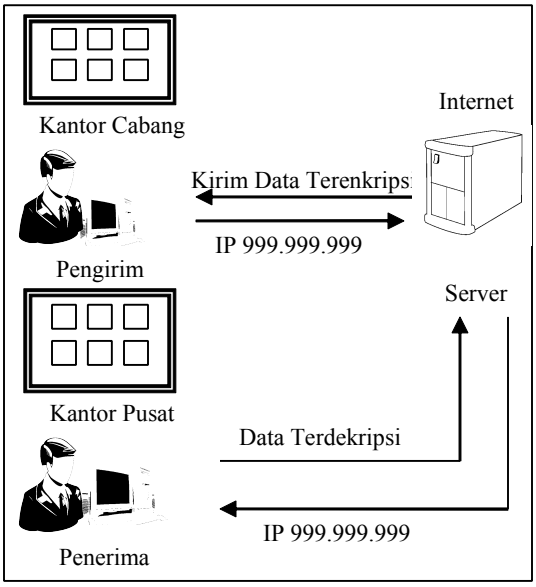
c. *File* akan menjadi seperti keadaan semula dan dapat terbaca kembali.

Diagram alir untuk dekripsi *file* dapat dilihat pada gambar 2.3



Gambar 2.3 Dekripsi File

2.6.2 Arsitektur Perangkat Lunak



Gambar 2.4 Arsitektur Perangkat Lunak

2.6.3 Storyboard

Storyboard adalah bagan alir menggambarkan penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode *twofish* seperti tabel di bawah ini.

Tabel 2.2 *Storyboard*

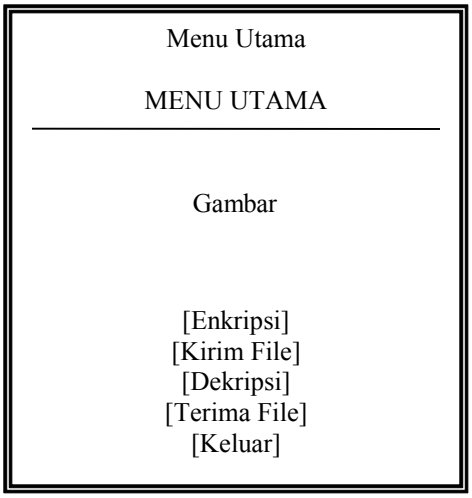
No.	Halaman	Isi	Keterangan
1.	Form Menu Utama	1. Text Menu Utama 2. Gambar 3. Tombol Enskripsi 4. Tombol Deskripsi 5. Tombol Keluar	Form ini akan tampil pertama ketika program di jalankan terdapat judul kriptografi twofish. Terdapat tombol untuk menampilkan form selanjutnya
2	Form Enksripsi	1. Text Enksripsi 2. Input File 3. Output File 4. Password 5. Ulangi Password 6. Tombol Enskripsi 7. Tombol Batal 8. Tombol Keluar	Form ini akan tampil ketika user klik tombol enskripsi
3	Form Kirim FIle	1. Text Kirim File 2. Input Host Name 3. Input Username 4. Input Password 5. Input File 6. Tombol Kirim 7. Tombol Batal	Form ini akan tampil ketika user klik tombol dekripsi.

		8. Tombol Keluar	
4.	Form Deskripsi	1. Text Deskripsi 2. Input File 3. Output File 4. Password 5. Ulangi Pasword 6. Tombol Enksripsi 7. Tombol Batal 8. Tombol Keluar	Form ini akan tampil ketika user klik tombol dekripsi.
5.	Form Terima File	1. Text Terima File 2. Host Name 3. Username 4. Password 5. Ouput File 6. Tombol Terima 7. Tombol Batal 8. Tombol Keluar	Form ini akan tampil ketika user klik tombol terima file.

2.7 Rancangan Antar Muka

1. *Form* menu utama

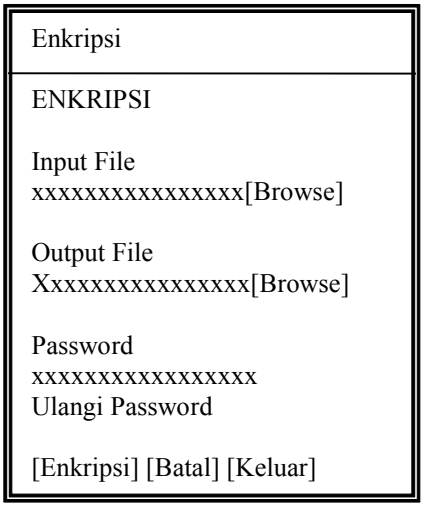
Form menu utama merupakan *link* ke *form* menu utama yang berfungsi untuk menampilkan *form* induk dari penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode *twofish*.



Gambar 2.5 *Form* Menu Utama

2. *Form* enkripsi *file*

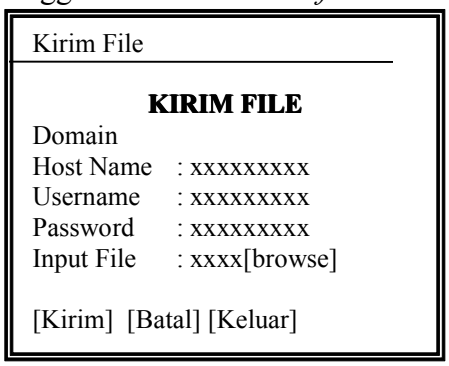
Form enkripsi *file* merupakan *link* ke *form* enkripsi *file* yang berfungsi untuk menampilkan proses enkripsi *file* pada penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode *twofish*.



Gambar 2.6 *Form* enkripsi *file*

3. *Form* kirim *file*

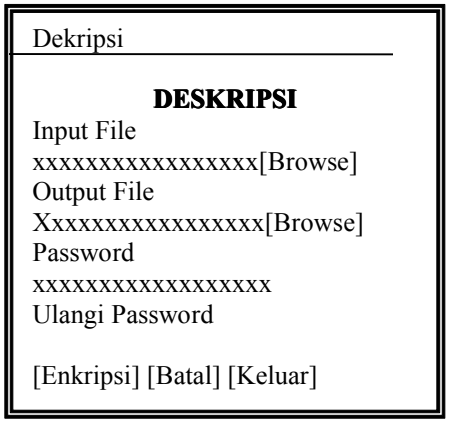
Form kirim *file* merupakan *link* ke *form* kirim *file* yang berfungsi untuk menampilkan proses pengiriman data pada penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode *twofish.*.



Gambar 2.7 *Form* Kirim *File*

4. *Form* dekripsi *file*

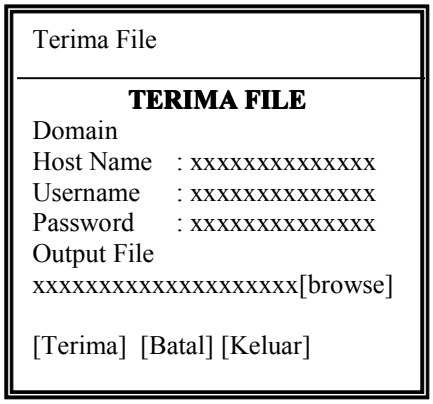
Form deskripsi *file* merupakan *link* ke *form* dekripsi *file* yang berfungsi untuk menampilkan proses dekripsi *file* pada penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode *twofish*.



Gambar 2.8 *Form* deskripsi *File*

5. *Form* terima *file*

Form terima *file* merupakan *link* ke *form* terima *file* yang berfungsi untuk menampilkan proses pengiriman data pada penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode *twofish.*



Gambar 2.9 *Form* Terima *File*

3. HASIL

3.1 Hasil

Hasil dari rancangan program pada pembahasan bab III yang dibuat skripsi ini adalah tampilan dari masing-masing *form*, bagaimana cara penggunaannya, adapun hasil dari rancangan program ini adalah penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode *twofish* pada *PT. Gaya Makmur Tractor.* Manfaat dari penelitian ini adalah dengan adanya penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode twofish pada *PT.*

Gaya Makmur Tractor ini dapat membantu pihak *PT. Gaya Makmur Tractor* dalam pengiriman dan penerimaan pesan terjaga kerahasiaan.

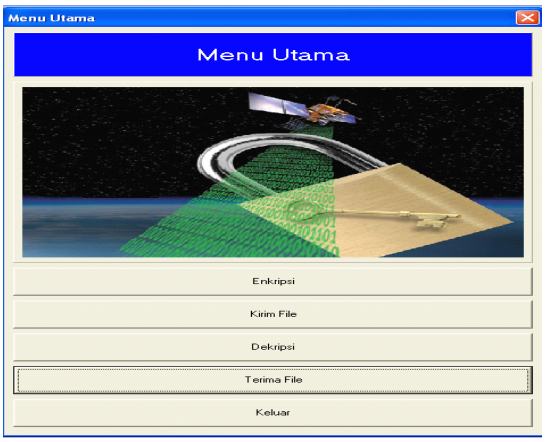
3.2 Pembahasan

Dalam menjalankan program penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode *twofish* pada *PT. Gaya Makmur Tractor* ini sudah dibuat *file.exe* jadi untuk menjalankan penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode *twofish* pada *PT. Gaya Makmur Tractor* ini cukup mengklik *file* yang sudah dibuat, apabila *file* sudah diklik maka penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode *twofish* pada *PT. Gaya Makmur Tractor* langsung masuk ke menu utama. Adapun cara menjalankannya adalah sebagai berikut, hidupkan komputer dengan sistem operasi minimal *windows XP,* pada *desktop* komputer terdapat *shortcut* steganografi.exe klik dua kali, maka secara otomatis akan tampil perangkat lunak enkripsi dan dekripsi data dengan mode *chiper electronik code book* dan menampilkan menu utama.

Adapun *form-form* pada sebuah penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode *twofish* ini memiliki sub-sub *form* sebagai berikut :

1. ***Form* Menu Utama,**

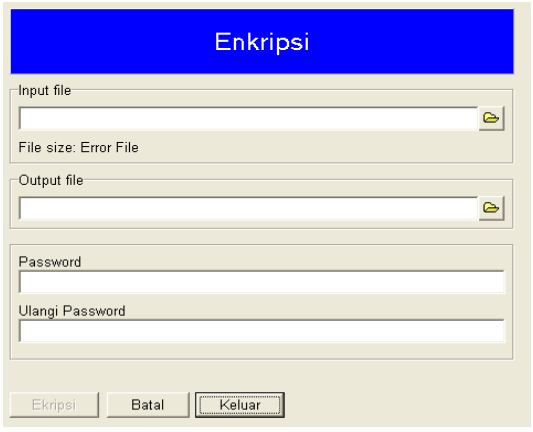
   Form menu utama merupakan tampilan pertama ketika program dijalankan, pada *form* menu utama ini terdapat gambar, menu dan sub menu tombol enkripsi, kirim file, dekripsi, terima file dan keluar.



Gambar 3.1 *Form* Menu Utama

2. ***Form* Enkripsi,**

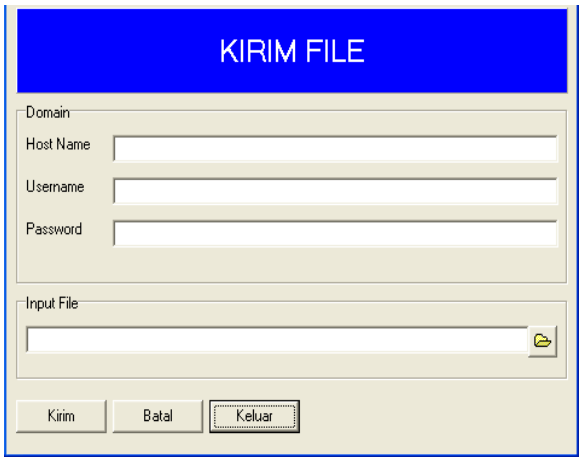
   Form enkripsi merupakan halaman yang menampilkan form enkripsi untuk enkripsi *file.*



Gambar 3.2 *Form* Enktripsi

3. ***Form* Kirim *File*,**

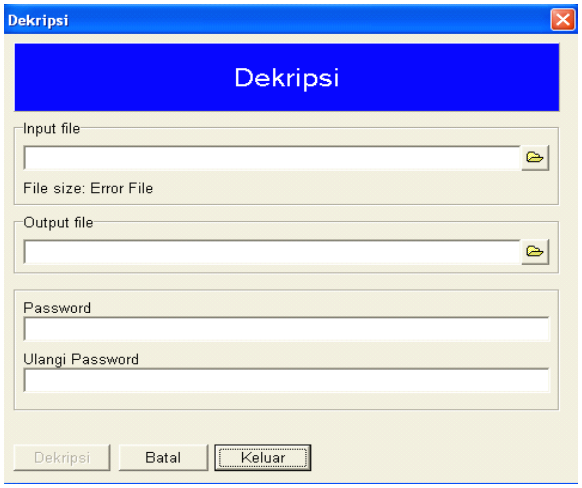
Form kirim *file* merupakan halaman yang menampilkan kirim file untuk kirim *file*.



Gambar 4.3 *Form* Kirim

4. ***Form* Dekripsi,**

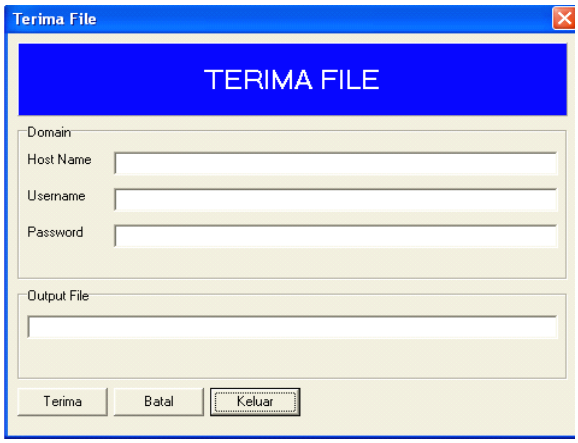
Form dekripsi merupakan halaman yang menampilkan dekripsi untuk dekripsi.



Gambar 4.4 *Form* Dekripsi

5. ***Form* Terima File,**

Form terima *file* merupakan halaman yang menampilkan terima *file* untuk terima *file*.



Gambar 4.5 *Form* Terima File

4. Kesimpulan

Berdasarkan dari penelitian yang telah dilaksanakan dan sudah diuraikan dalam penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode *twofish* pada *PT. Gaya Makmur Tractor*, maka penulis dapat menarik kesimpulan sebagai berikut :

1. Penelitian ini menghasilkan perangkat lunak penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode twofish pada *PT. Gaya Makmur Tractor*.
2. Perangkat lunak enkripsi dan dekripsi data dengan adanya penerapan metode pengamanan data enskripsi dan deskripsi menggunakan metode twofish pada *PT. Gaya Makmur Tractor* ini dapat membantu dalam pengiriman dan

penerimaan pesan terjaga kerahasiaan.

DAFTAR PUSTAKA

[1] Hamsah, M. 2010. Pembuatan Aplikasi Secure E-Book Untuk Karya Ilmiah Pens-ITS, Politeknik Negeri Surabaya.

[2] Kadir, A. 2000. Dasar Pemrograman Delphi 5.0, Andi, Yogyakarta.

[3] Kristanto, A. 2004. *Rekayasa Perangkat Lunak*, Gava Media, Yogyakarta.

[4] Mangkulo, A. 2005. *Membuat Aplikasi Database Dengan Delphi 8.0*, Elexmedia Komputindo, Jakarta.

[5] Mudeng, D. 2004. *Kriptografi Twofish*, Institut Teknologi Bandung.

[6] Munir, R. 2006. *Kriptografi*, Informatika, Bandung.

[7] Pratama, D. 2010. *Model Evaluasi CIPP (Context, Input, Process, Product)*.www.snapdrive.net%2Ffiles%2F649907%2FThe%2520CIPP%2520Evaluation%2520Model%2520 2003.doc

[8] Pressman, R. 2002. *Rekayasa Perangkat lunak*. ANDI, Yogyakarta.

[9] Ratih, 2003. *Studi dan Implementasi Enkripsi Pengiriman Pesan Suara Menggunakan Algoritma Twofish*. Jurnal Ilmu Komputer Dan Teknologi Informasi, Vol III No.2, Oktober 2003.

[10] Sutabri, T. 2004. Analisa Sistem Informasi, ANDI, Yogyakarta.