APLIKASI PEMAHAMAN DAN PENERAPAN FAST (k,n) THRESHOLD SECRET SHARING SCHEME

Roy Suhendra Sinaga[1] , Swingly Purba[2], Ruth Meivera Siburian[3]

Mahasiswa Teknik Informatika, Fakultas Teknologi Industri, Institut Sains Dan Teknologi TD Pardede
Dosen Teknik Informatika, Fakultas Teknologi Industri, Institut Sains Dan Teknologi TD Pardede Email :
[1]roysuhe19@gmail.com, [2]swinglypurba@gmail.com, [3]v_manut@yahoo.com
Jl. DR. TD. Pardede No.8 Medan 20153

ABSTRAK

Sebuah skema secret sharing memperbolehkan sebuah rahasia untuk dibagikan kepada n partisipan sedemikian sehingga hanya k orang dari mereka yang dapat mengkonstruksi pesan kembali, tetapi sembarang (k
– 1) tidak dapat memperoleh informasi apapun mengenai rahasia. Dalam literatur, dapat ditemukan berbagai skema secret sharing yang menerapkan berbagai macam teorema. Suatu skema secret sharing dikatakan ideal apabila share yang dihasilkan memiliki ukuran bit yang sama dengan ukuran bit rahasia. Skema secret sharing dari Shamir merupakan salah satu skema secret sharing yang ideal. Namun, kekurangan dari skema Shamir ini adalah memiliki proses komputasi yang banyak, terutama untuk proses recovery.

Untuk memperbaiki masalah tersebut, maka Jun Kurihara, Shinsaku Kiyomoto, Kazuhide Fukushima, Toshiaki Tanaka dari KDDI (Kokusai Denshin Denwa Institute) R&D (Research and Development) Laboratories, Inc., Jepang memperkenalkan (k, n)-threshold secret sharing scheme yang cepat. Prosedur kerja dari skema ini terbagi menjadi dua bagian, yaitu proses distribusi dan recovery. Prosedur kerja dalam skema ini menggunakan operasi logika XOR dan algoritma eliminasi Gauss.

Penulisan tugas akhir ini akan memfokuskan pembahasan pada prosedur kerja dari skema secret sharing ini dan mengimplementasikannya untuk melakukan distribusi dan recovery rahasia. Perangkat lunak hasil rancangan akan mampu melakukan proses distribusi dan recovery rahasia. Selain itu, perangkat lunak juga menyediakan laporan hasil proses perhitungan sehingga dapat dilihat rincian proses perhitungan yang dilakukan.

Kata Kunci : *Aplikasi, Secret Sharing Scheme*

1. PENDAHULUAN

Dalam kehidupan sehari-hari, sering ditemui persoalan penyimpanan rahasia digital. Agar data rahasia digital tersebut aman, maka harus dipecahkan dan disimpan di beberapa tempat (lokasi). Namun, persoalan yang ditemui dalam proses pemecahan dan penyimpanan rahasia digital ini adalah tempat penyimpanan beberapa rahasia sering terlupakan ataupun beberapa pecahan data jatuh ke tangan orang lain, sehingga orang tersebut dapat mengetahui beberapa informasi mengenai data rahasia tersebut. Hal ini dapat diatasi dengan menerapkan protokol kriptografi secret sharing. Konsep (k, n)-threshold secret sharing scheme pertama kali diperkenalkan oleh Shamir dan Blakley pada tahun 1979. Konsep ini memperbolehkan n orang partisipan untuk memegang pecahan (share) yang berbeda yang dihasilkan dari rahasia s. Sedangkan, untuk menyusun kembali rahasia

maka diperlukan k buah pecahan (share) yang berbeda yang masing-masing dipegang oleh partisipan berbeda.

Oleh karena itu, penulis merancang sebuah perangkat lunak pemahaman dan penerapan yang mampu untuk menampilkan proses kerja dari skema secret sharing tersebut sehingga dapat membantu proses pemahaman terhadap cara kerja
dari skema secret sharing tersebut sekaligus menerapkannya untuk melakukan distribusi dan recovery rahasia dengan mengambil tugas akhir yang berjudul " Aplikasi Pemahaman dan Penerapan Fast (k, n)-Threshold Secret Sharing Scheme".

2. LANDASAN TEORI

Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. (Dony Ariyus, Pengantar Ilmu Kriptografi, 2008, 13).

Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu: Enkripsi, Dekripsi. Kunci.

Bilangan bulat positif yang mempunyai aplikasi penting dalam ilmu komputer adalah bilangan prima. Bilangan prima adalah bilangan bulat positif yang lebih besar dari 1 yang hanya habis dibagi oleh 1 dan dirinya sendiri.

Matriks adalah suatu susunan bilangan-bilangan yang berbentuk empat persegi panjang.

Suatu Linear Feedback Shift Register (LFSR) adalah suatu mekanisme untuk menghasilkan sekuens bit biner. Register memiliki sebarisan sel yang ditentukan oleh vektor inisialisasi yakni, biasanya, menjadi kunci rahasia.

Threshold Generator, Generator ini mencoba untuk mengambil konsep seputar masalah sekuritas dari generator terdahulu dengan menggunakan sejumlah variasi dari LFSR. Teorinya adalah jika menggunakan lebih banyak LFSR, maka akan lebih sulit untuk memecahkan *cipher*- nya.Pastikan bahwa panjang dari semua LFSR adalah bilangan prima relatif dan semua polinomial *feedback* adalah primitif untuk memaksimalkan periodenya. Jika lebih dari setengah bit *output* adalah 1, maka ouput dari generator adalah 1. Jika lebih dari setengah bit *output* adalah 0, maka output dari generator adalah 0.

Protokol adalah aturan yang berisi rangkaian langkah-langkah, yang melibatkan dua atau lebih orang, yang dibuat untuk menyelesaikan suatu kegiatan. Sedangkan, protokol kriptografi adalah protokol yang menggunakan kriptografi. Orang yang berpartisipasi dalam protokol kriptografi memerlukan protokol tersebut misalnya untuk berbagai komponen rahasia untuk menghitung sebuah nilai, membangkitkan rangkaian bilangan acak, meyakinkan identitas orang lainnya (otentikasi) dan sebagainya.

Protokol kriptografi dibangun dengan melibatkan beberapa algoritma kriptografi. Sebagian besar protokol kriptografi dirancang untuk dipakai oleh kelompok yang terdiri dari 2 orang pemakai, tetapi ada juga beberapa protokol yang dirancang untuk dipakai oleh kelompok orang yang terdiri dari dua orang pemakai.Tingkah laku register diatur oleh sebuah counter (clock).

Jika seorang pegawai berhenti bekerja, dengan bagian tunggal dari resep yang diperolehnya, informasi tersebut sama sekali tidak berguna. Skema pembagian paling sederhana membagi sebuah pesan diantara dua orang. Berikut dirincikan sebuah protokol dimana Trent dapat memecahkan sebuah pesan diantara Alice dan Bob:

1. Trent membuat deretan *string* acak R yang panjangnya sama dengan pesan rahasia M.
2. Trent melakukan operasi XOR antara M dengan R, sehingga menghasilkan S.

$$M \oplus R = S$$

3. Trent memberikan R kepada Alice dan S kepada Bob.

Untuk merekonstruksi pesan, Alice dan Bob hanya memerlukan satu langkah untuk dilakukan, yaitu:

4. Alice dan Bob meng-XOR-kan pecahan mereka secara bersama-sama untuk merekonstruksipesan

$$R \oplus S = M$$

Namun, protokol ini memiliki kelemahan. Jika sembarang pecahan hilang dan Trent sedang tidak berada di tempat, maka pesan rahasia tidak dapat diperoleh.

Skema *sharing* yang jauh lebih kompleks, disebut dengan skema *threshold*, dapat melakukan semua hal tersebut ataupun lebih, secara matematis. Pada tingkatan yang paling sederhana, anda dapat mengambil

beberapa pesan dan memecahkannya menjadi n pecahan, yang disebut *shadow* atau *share*, sedemikian sehingga m buahdari mereka dapat digunakan untuk merekonstruksi pesan. Secara lebih tepat, skema ini disebut *(m,n)-threshold scheme*.

Dengan sebuah (3,4)-*threshold scheme*, Trent dapat memecah rahasia resep sausnya antara Alice, Bob, Carol dan Dave, sedemikian sehingga tiga dari mereka dapat menggabungkan *shadow* mereka bersama dan merekonstruksi pesan. Jika Carol sedang liburan, maka Alice, Bob dan Dave dapat melakukannya. Demikian juga jika Bob tidak ada, Alice, Carol dan Dave dapat melakukannya. Namun, jika Bob dan Carol tidak ada, Alice dan Dave tidak dapat merekonstruksi pesan.

Adi Shamir menggunakan persamaan polinomial pada sebuah *field* terbatas untuk mengkonstruksikan sebuah *threshold scheme*. Pilihlah sebuah bilangan

$$w_{(i,j)} = \left(\bigoplus_{h=0}^{k-2} r_{h,i+j}^{h}\right) \oplus s_{j-i} = s_{j-i} \oplus r_j^0 \oplus r_{i+j}^1.$$

prima, p, yang harus lebih besar daripada semua bilangan yang digunakan pada *shadow* dan rahasia. Untuk membagikan sebuah rahasia, hasilkan sebuah polinomial berderajat m – 1. Sebagai contoh, jika anda ingin membuat sebuah (3,n)-*threshold scheme*, maka hasilkan sebuah polinomial kuadratik seperti berikut:

$$(ax^2 + bx + M) \bmod p$$

dimana p adalah sebuah bilangan prima acak yang lebih besar daripada semua koefisien. Koefisien a dan b dipilih secara acak, dirahasiakan dan dibuang setelah *shadow* diperoleh, sementara M adalah pesan dan bilangan prima harus dibuat publik. *Shadow* diperoleh dengan mengevaluasi polinomial pada n poin berbeda:

$$k_i = F(x_i)$$

Dengan perkataan lain, *shadow* pertama dapat berupa polinomial yang dievaluasi pada x = 1, *shadow* kedua dapat berupa polinomial yang dievaluasi pada x = 2, dan seterusnya. Karena polinomial kuadratik memiliki tiga koefisien yang tidak diketahui, yaitu a, b dan M, maka tiga buah *shadow* dapat digunakan untuk menghasilkan tiga buah persamaan. Namun, satu atau dua *shadow* tidak dapat, tetapi empat atau lima *shadow* berlebihan.

Penjelasan mengenai algoritma distribusi akan menggunakan contoh untuk (k, n) = (3, 5) dan n = n_p dan dapat dirincikan sebagai berikut:

1. Pecahkan s menjadi (n_p – 1) buah segmen dengan panjang masing-masing d bit. Dalam kasus ini,n_p = 5, maka n_p – 1 = 5 – 1 = 4 buah.

2. Persiapkan s0 yang berupa deretan bit nol dengan panjang d-bit.

3. Bangkitkan [(k – 1) * np – 1] buah bilangan acak dengan panjang d bit. Dalam kasus ini, k = 3 dannp = 5, maka [(k – 1) * np – 1] = [(3 – 1) * 5 – 1]
   = 2*5–1 = 9.

4. Eksekusi operasi XOR dengan persamaanberikut:

5. Gabungkan n_p – 1 buah segmen tersebut untuk menghasilkan *share* w_i yang akan diberikan kepada partisipan P_i.

Perangkat lunak adalah: Perintah (program komputer) yang bila dieksekusi memberikan fungsi dan unjuk kerja seperti yang diinginkan. Struktur data yang memungkinkan program memanipulasi informasi secara proporsional. Dokumen yang menggambarkan operasi dan kegunaan program. (Roger S. Pressman, 10, 2002). Rekayasa perangkat lunak adalah pengembangan dan penggunaan prinsip pengembangan untuk memperoleh perangkat lunaksecara ekonomis yang reliabel dan bekerja secara efisien pada mesin nyata.

Sekuensial linier mengusulkan sebuah pendekatan kepada perkembangan perangkat lunak yang sistematik dan sekuensial yang mulai pada tingkat dan kemajuan sistem pada seluruh analisis, desain, kode, pengujian dan pemeliharaan.

Roy Suhendra Sinaga[1] , Swingly Purba[2], Ruth Meivera Siburian[3]
APLIKASI PEMAHAMAN DAN PENERAPAN FAST (k,n) THRESHOLDSECRET SHARING SCHEME

Prototyping adalah suatu proses yang memungkinkan penciptaan sebuah model perangkat lunak yang hendak dibangun agar dapat diketahui terlebih dahulu efisiensi suatu algoritma, adaptabilitassistem operasi atau interaksi manusia dan komputer

yang sesuai. Urutan langkah-langkah umum yang dilakukan pada *prototyping* ialah:

a. Pengumpulan kebutuhan-kebutuhan
b. Perancangan secara cepat
c. Pembuatan *prototype*
d. Evaluasi *prototype* oleh pengguna
e. Penyempurnaan *prototype*
f. Pembuatan *prototype*

3. HASIL DAN PEMBAHASAN

3.1 Analisis dan Perancangan

Persyaratan fungsional yang harus dipenuhi oleh perangkat lunak adalah sebagai berikut:

1. Untuk bagian pemahaman, nilai k dan n dengan nilai maksimal 10, sedangkan untuk bagian aplikasi,nilai k dan n dibatasi maksimal 50, dimana k ≤ n.

2. Untuk bagian pemahaman, pesan rahasia denganpanjang maksimal 50 karakter, sedangkan untuk bagian aplikasi, panjang pesan rahasia maksimal 1000 karakter.

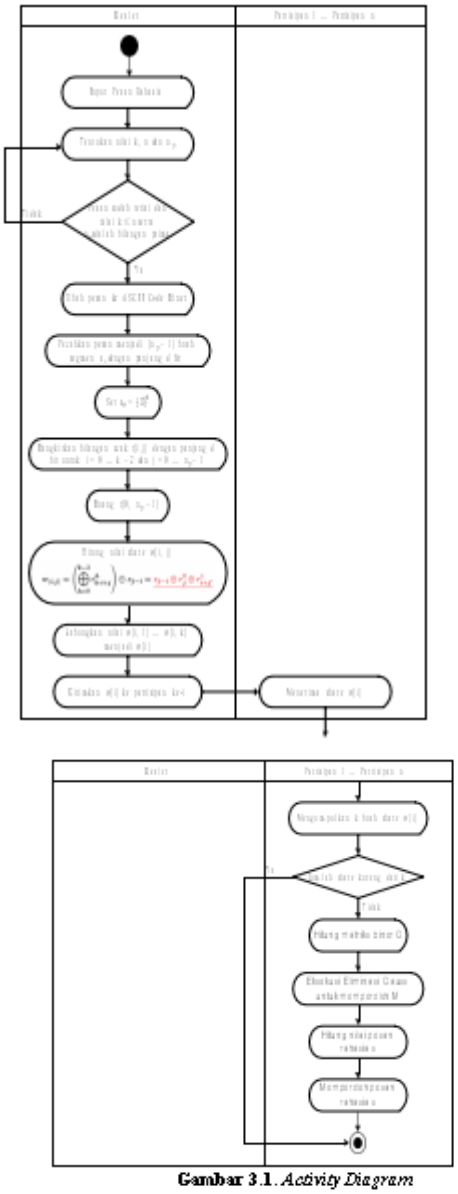
3. Untuk bagian aplikasi, file rahasia yang dapat dibuka berekstensi *.txt dan akan menghasilkan beberapa file share yang berekstensi *.kdi.

4. Pembangkitan dan pengujian bilangan prima menggunakan metode Rabin-Miller dengan batasanminimal 1 digit dan maksimal 2 digit.

5. Perangkat lunak akan menampilkan laporan hasilproses perhitungan yang dapat disimpan dalam bentuk text file.

Persyaratan non-fungsional dari sistem, maka harus dilakukan analisis terhadap kinerja,informasi, ekonomi, keamanan aplikasi, efisiensi, dan pelayanan customer. Panduan ini dikenal dengan analisis PIECES (performance, information, economic, control, eficiency, dan services).

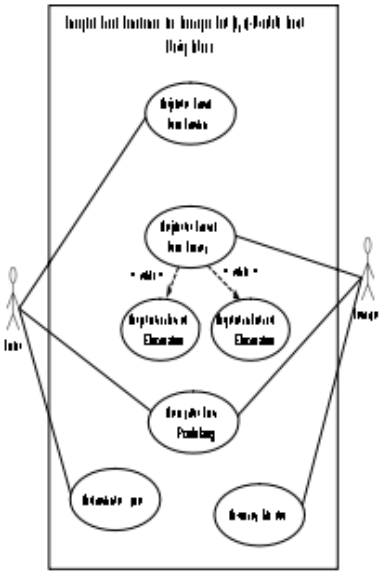
Agar dapat lebih memahami mengenai prosedur kerja dari skema ini maka diberikan gambar *activity diagram* dari skema tersebut seperti terlihat pada gambar 3.1 berikut:



Gambar 3.1. ***Activity Diagram*** **dariProsedur Kerja** ***Fast*** **(k, n)-*Threshold Secret Sharing Scheme***

Roy Suhendra Sinaga[1] , Swingly Purba[2], Ruth Meivera Siburian[3]

Setelah menganalisis prosedur kerja dari Fast (k, n)-Threshold Secret Sharing Scheme, maka tahapan selanjutnya adalah memodelkan sistem yang akan dirancang. Alat bantu yang digunakan untuk menganalisis dan memodelkan sistem adalah use case.



Roy Suhendra Sinaga[1] , Swingly Purba[2], Ruth Meivera Siburian[3]

APLIKASI PEMAHAMAN DAN PENERAPAN FAST (k,n) THRESHOLDSECRET SHARING SCHEME

Gambar 3.2. Diagram use case perangkat lunak

Perangkat lunak pemahaman dan penerapan *Fast* (k, n)-*Threshold Secret sharing scheme* ini dirancang dengan menggunakan bahasa pemrograman Microsoft Visual Basic 2005 dengan menggunakan beberapa objek dasar seperti :

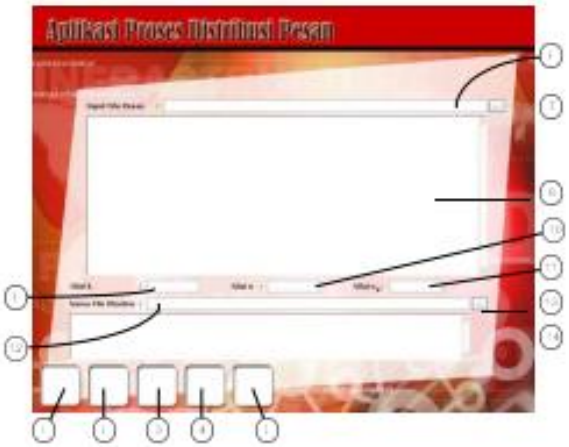
1. *Label*, yang digunakan untuk menampilkan keterangan.
2. *Button*, yang digunakan sebagai tombol eksekusi.
3. *Save File Dialog*, yang digunakan untuk menampilkan dialog *save*.
4. *Open File Dialog*, yang digunakan untuk menampilkan dialog *open*.
5. *Textbox*, yang digunakan sebagai tempatpengisian data input.
6. *Richtextbox*, yang digunakan untuk menampilkan hasil proses perhitungan.
7. *Combobox*, yang digunakan untuk menyediakan pilihan kecepatan proses.

Rancangan tampilan dari perangkat lunak pemahaman dan penerapan Fast (k, n)-Threshold Secret sharing scheme ini yaitu : Form ‘Main’, Form ‘Tutorial Distribusi’, Form ‘Tutorial Recovery’, Form ‘Aplikasi Distribusi’, Form ‘Aplikasi Recovery’, Form ‘Teori’ dan Form ‘Laporan’.

Gambar 3.3. Rancangan form Main

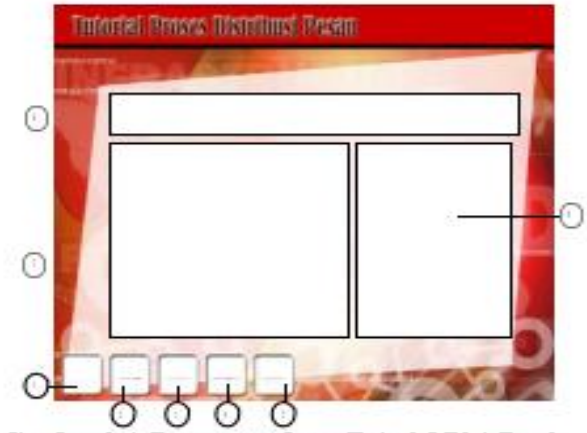
Gambar 3.5. Rancanganform Tutorial Recovery

Roy Suhendra Sinaga[1] , Swingly Purba[2], Ruth Meivera Siburian[3]
APLIKASI PEMAHAMAN DAN PENERAPAN FAST (k,n) THRESHOLDSECRET SHARING SCHEME



Gambar 3.6. Rancangan form Aplikasi Distribusi

Gambar 3.8. Rancangan form Form Teori



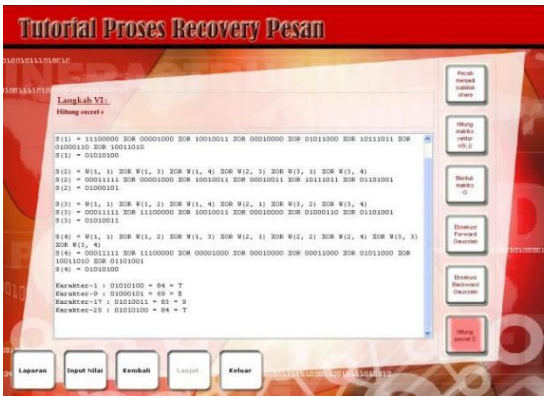
Gambar 3.4. Rancangan form Tutorial Distribusi

Gambar 3.8. Rancangan form Form Teori

Gambar 3.7. Rancangan form Aplikasi Recovery

Gambar 3.9. Rancangan form Form Laporan

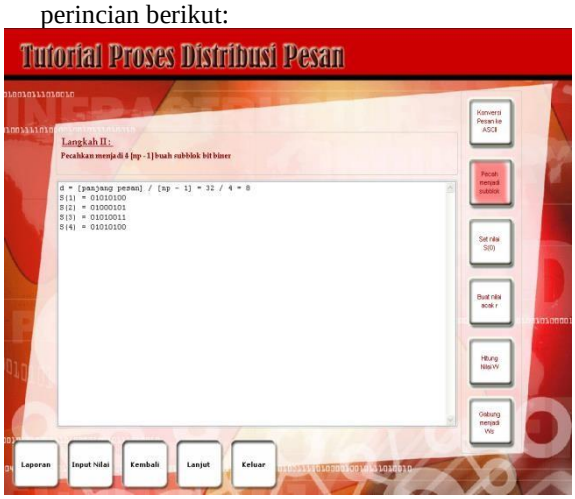
Gambar 3.10. Tampilan Form " Main "



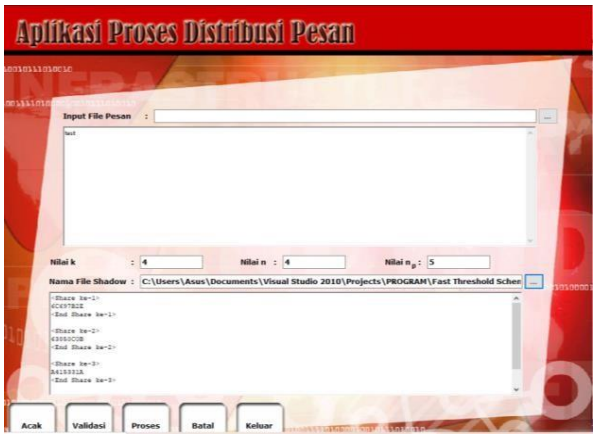
Gambar 3.12. Tampilan Form " PemahamanProses Recovery "

3.2 IMPLEMENTASI

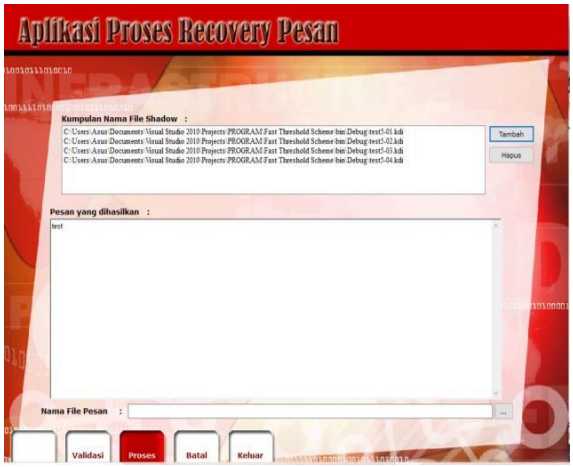
Perangkat lunak pemahaman dan penerapan Fast (k, n)-Threshold Secret Sharing Scheme ini memiliki beberapa tampilan output seperti perincian berikut:



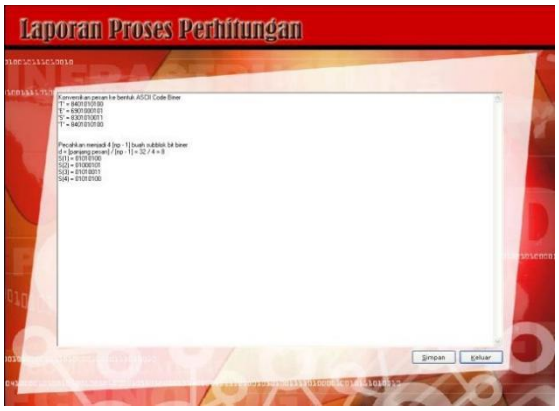
Gambar 3.11. Tampilan Form PemahamanProses Distribusi "



Gambar 3.13. Tampilan Form " Aplikasi ProsesDistribusi "



Gambar 3.14. Tampilan Form " Aplikasi ProsesRecovery "



Gambar 3.15. Tampilan Form " Laporan "

4. KESIMPULAN DAN SARAN

Setelah menyelesaikan tugas akhir ini, penulis menarik beberapa kesimpulan sebagai berikut:

1. Perangkat lunak dapat digunakan untuk memahami prosedur kerja dari metode *Fast* (k, n)-*Threshold Secret Sharing Scheme*, yaitu melalui fasilitas 'Pemahaman' yang disediakan oleh perangkat lunak.
2. Perangkat lunak juga dapat digunakan untuk melakukan pengamanan data *file* teks, yaitu melalui fasilitas 'Aplikasi' yang disediakan oleh perangkat lunak.

Penulis juga ingin memberikan beberapa saran yang mungkin berguna untuk pengembangan perangkat lunak lebih lanjut, yaitu :

1. Perangkat lunak dapat dikembangkan dengan merancang suatu *class* dari metode *Fast* (k, n)- *Threshold Secret Sharing Scheme* sehingga metode ini dapat diterapkan pada aplikasi lainnya misalnya aplikasi berbasis web untuk menjaga rahasia pengguna.
2. Perangkat lunak dapat dikembangkan dengan menerapkan metode ini untuk melakukan pengamanan *file* selain *text file* seperti *file audio, video*, gambar dan sebagainya.

DAFTAR PUSTAKA

Anton,H. 1987 . Aljabar Linear Elementer. Jakarta: Erlangga.

Ariyus,D. 2008. Pengantar Ilmu Kriptografi. Yogyakarta : Andi.

Fowler,M. 2005. Panduan Singkat Bahasa PemodelanObjek Standar. Addison:Wesley.

Hariyanto,B. 2004. Rekayasa Sistem Berorientasi Objek. Bandung :Informatika.

Kendall, K.E. dan Kendall, J.E. 2006. Analisis dan Perancangan Sistem. Jilid 1, Alih Bahasa Thamir Abdul Hafedh Al-Hamdany, Jakarta :Prenhallindo.

Kurihara, J., Kiyomoto, S., Fukushima, K., Tanaka,

T. 2008. A New (k, n)-Threshold Secret Sharing Scheme and Its Extension. 11th Information Security Conference, Taipei, Jepang : KDDI R&D Laboratories.

Kurniawan, J., 2004. Kriptografi : Keamanan Internet dan Jaringan Komunikasi. Bandung: Informatika.

Munir, R. 2006. Kriptografi, Bandung: Informatika.

Roger S. Pressman, Ph.D. 2002. Rekayasa Perangkat Lunak : Pendekatan Praktisi (Buku Satu), Yogyakarta : ANDI.

Schneier, B., 1996, Applied Crytography : Protocols, Algorithm, and Source Code in C, Second Edition, John Willey and Sons Inc.

Stallings, W. 2003. Cryptography and Network Security : Principle and Practice, Second Edition, Prentice Hall.