APLIKASI PENGAMANAN FILE MICROSOFT OFFICE DENGAN ALGORITMA DES (*DATA ENCRYPTION STANDARD)*

I Gede Made Karma
Jurusan Akuntansi – Politeknik Negeri Bali
Bukit Jimbaran, PO BOX 1064 Tuban, Badung, Bali
Telp: 0361-701981, Fax.: 0361-701128
E-mail: igmkarma@yahoo.com, Telp. 081338158240

Abstrak: Microsoft Office merupakan sebuah aplikasi perkantoran yang sangat populer pada kalangan pemakai komputer. Microsoft Office yang dilengkapi dengan aplikasi pengolah kata (MS. Word), aplikasi lembar kerja (MS. Excel), aplikasi presentasi (MS. Powerpoint) dan aplikasi basis data (MS. Access) banyak dipergunakan untuk menyimpan berbagai macam data/informasi yang berguna dan penting, serta dapat pula bersifat rahasia. Untuk mencegah pengaksesan data/informasi yang penting dan rahasia oleh orang yang tidak berhak, maka diterapkan sistem pengamanan. Pengamanan terhadap data/informasi ini lebih sering dilakukan dengan pengamanan pada saat pengaksesannya dengan menggunakan password.

Untuk mengamankan data/informasi yang tersimpan dalam sebuah file, telah dikembangkan sebuah cara dengan menerapkan teknik enkripsi. Teknik ini menerapkan teknik permutasi yang dilakukan secara berulang, sampai diperoleh hasil yang tidak dikenali lagi. Untuk mengetahui bentuk aslinya, diterapkan teknik dekripsi, yang merupakan kebalikan langkah enkripsi. Dalam penelitian ini diimplementasikan teknik enkripsi dengan algortima DES yang termasuk ke dalam sistem kriptografi simetri dan tergolong jenis *cipher* blok.

Berdasarkan hasil pengujian aplikasi yang dikembangkan, ternyata teknik enkripsi yang memanfaatkan algortima DES ini dapat dipergunakan untuk mengamankan semua jenis file MS. Office versi 2007. File yang dienkripsi ternyata tidak dapat dikenali dan sekaligus tidak dapat diakses oleh program pembuatnya, yaitu masing-masing MS. Word, MS. Excel, MS. Powerpoint dan MS. Access.

Kata kunci: MS. Office, pengamanan, enkripsi, dekripsi, algoritma DES.

The Application of MS. Office File Protection using DES (Data Encryption Standard) Algorithm

Abstract: *Microsoft Office is an office suite that is very popular in the computer users. Microsoft Office with a word processing application (MS. Word), a spreadsheet application (MS. Excel), a presentation application (MS. Powerpoint) and database applications (MS. Access) is widely used to store various kinds of data/information that is useful and*

important, and can also be confidential. To prevent the accessing of data/information that is important and confidential by an unauthorized person, then applied the security system. Security of data/information is more often carried out by security when accessing it using a password.

To secure the data/information stored in a file, have developed a way to implement encryption techniques. This technique implements a permutation technique carried out repeatedly, to obtain results that are not recognizable anymore. To know the original form, applied decryption techniques, which is the opposite of encryption step. In this study the technique implemented is DES encryption with algorithms that belong to the symmetric cryptographic systems and classified the type of block ciphers.

Based on the results of testing of applications developed, it turns encryption technique that utilizes DES algorithm can be used to secure all file types of MS. Office 2007 version. Encrypted files were not identifiable and can not be accessed simultaneously by the program creators, namely MS. Word, MS. Excel, MS. Powerpoint and MS. Access.

Keywords : MS. Office, security, encryption, decryption, DES algorithm.

1. PENDAHULUAN

Microsoft Office (MS. Office) saat ini dapat dikatakan sebagai sebuah paket aplikasi perkantoran yang sangat populer. Sebagai sebuah paket aplikasi, MS. Office dilengkapi dengan aplikasi pengolah kata (MS. Word), aplikasi lembar kerja atau *spreadsheet* (MS. Excel), aplikasi untuk presentasi (MS. Powerpoint) dan aplikasi pengolah database (MS. Access). Sebuah perpaduan aplikasi yang lengkap dan komplit, ditambah kemudahan pengoperasian, maka sangat wajar banyak orang yang mempergunakannya untuk berbagai keperluan pribadi maupun membantu pekerjaan kantor.

Banyak dan beragamnya kemampuan yang dimiliki oleh aplikasi-aplikasi yang dimiliki oleh MS. Office menjadikannya sebagai pilihan utama dalam menyimpan dan mengolah berbagai macam data/informasi. Akan terdapat beragam data/informasi yang disimpan dalam berbagai file MS. Office, baik data/informasi yang bersifat umum, tapi ada juga yang bersifat penting dan rahasia. Lalu bagaimana dengan pengamanan datanya? MS. Office ternyata sudah menyiapkan sistem pengamanan terhadap file yang diolahnya, yaitu dengan menyiapkan sistem pengamanan dengan teknik enkripsi yang dilengkapi dengan kata kunci atau *password*. Hanya saja, pengamanan dengan sistem ini memiliki kelemahan, yaitu *password* dengan mudah dapat ditebak orang, atau kalau *password* dilupakan maka otomatis file juga tidak dapat diakses.

Untuk mengamankan informasi yang tersimpan dalam sebuah file, telah dikembangkan sebuah teknik yang disebut teknik enkripsi. Teknik enkripsi ini menerapkan prinsip pengkonversian sebuah karekter menjadi karakter lain, sehingga informasi yang tersimpan dalam file tersebut kemudian menjadi tidak sama dengan aslinya. Untuk mengetahui

informasi aslinya, diterapkan teknik dekripsi. Ada berbagai teknik enkripsi yang sudah dikembangkan orang. Dari sekian banyak teknik enkripsi tersebut, ada sebuah teknik enkripsi yang memanfaatkan algoritma DES, yang akan diimplementasikan menjadi sebuah aplikasi untuk mengamankan file MS. Office.

2. METODE PENELITIAN

Dalam pengembangan aplikasi ini, pendekatan yang dipergunakan adalah metode terstruktur dengan metode pengembangan *Waterfall* dengan menerapkan teknik berorientasi objek, yaitu suatu metode pengembangan sistem yang membagi aktifitas pekerjaan menjadi proses yang bertahap dan berkelanjutan satu sama lainnya dengan tahapan sebagai berikut:

1. **System Engineering (Rekayasa Sistem)**, merupakan kegiatan untuk menentukan informasi apa yang dibutuhkan oleh sistem atau menentukan kebutuhan-kebutuhan dari sistem yang akan dibuat.
2. **Analisa Sistem,** dilakukan untuk memperoleh informasi tentang sistem, menganalisis data-data yang ada dalam sistem. Informasi yang dikumpulkan terutama mengenai kelebihan dan kekurangan sistem.
3. **Perancangan (Design)**, merupakan perancangan system baru berdasarkan data-data yang telah dikumpulkan pada tahap sebelumnya dengan cara merancang perangkat lunak diantaranya dengan membuat diagram UML, struktur file, struktur menu, merancang input dan merancang output.
4. **Penulisan Program (*coding*)**, Penulisan program menggunakan bahasa pemprograman VB.Net dan file Microsoft Office 2007 sebagai data ujinya.
5. **Pengujian Sistem**, Menguji aplikasi yang dibuat apakah sudah sesuai dengan spesifikasinya atau tidak dan mengetahui apakah hasil implementasi telah bebas dari kesalahan program (*error free*), baik kesalahan logika maupun kesalahan sintaks.
6. **Penulisan Laporan**, Pada tahap akhir akan dibuat sebagai laporan yang mencakup seluruh proses kegiatan yang telah dilaksanakan selama pembuatan aplikasi.

3. PEMBAHASAN DAN HASIL

DES merupakan kependekan dari *Data Encryption Standard*, yaitu sebuah standar teknik enkripsi yang telah diresmikan oleh pemerintah Amerika Serikat (US) di tahun 1977. Algoritma DES dikembangkan di IBM dibawah kepemimpinan W.L. Tuchman pada tahun 1972. Algoritma ini didasarkan pada algoritma LUCIFER yang dibuat oleh Horst Feistel. DES kemudian dijadikan standar ANSI di tahun 1981. Horst Feistel merupakan salah satu periset yang mula-mula mengembangkan DES ketika bekerja di IBM Watson Laboratory di Yorktown Heights, New York. Algoritma ini telah disetujui oleh *National Bureau of Standard* (NBS) setelah penilaian kekuatannya oleh *National Security Agency* (NSA) Amerika Serikat.

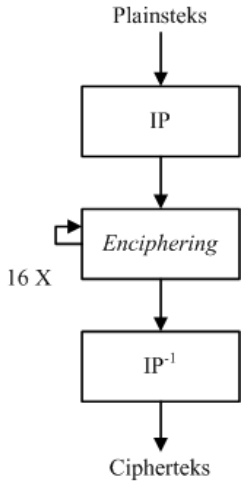
DES merupakan *block cipher* yang beroperasi dengan blok berukuran 64-bit dan kunci 56-bit. *Brute-force attack* terhadap DES membutuhkan kombinasi 2 pangkat 56, atau sekitar 7 x 10 pangkat 16, atau 70 juta milyar [1][2].

Skema global dari algoritma DES yang digambarkan dalam Gambar 1, dapat dijelaskan 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 (*inverse initial permutation* atau IP^{-1}) menjadi blok cipherteks.

Di dalam proses *enciphering*, blok plainteks terbagi menjadi dua bagian, kiri (*L*) dan kanan (*R*), yang masing-masing panjangnya 32 bit. Kedua bagian ini masuk ke dalam 16 putaran DES. Pada setiap putaran *i*, blok *R* merupakan masukan untuk fungsi transformasi yang disebut *f*. Pada fungsi *f*, blok *R* dikombinasikan dengan kunci internal K_i. Keluaran dari fungsi *f* di-XOR-kan dengan blok *L* untuk mendapatkan blok *R* yang baru. Sedangkan blok *L* yang baru langsung diambil dari blok *R* sebelumnya. Ini terjadi dalam satu putaran DES. Gambar 2 memperlihatkan skema algoritma DES secara lebih rinci. Secara matematis, satu putaran DES dinyatakan sebagai berikut:

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



Gambar 1. Skema Global Algoritma DES

Karena ada 16 putaran, maka dibutuhkan kunci internal sebanyak 16 buah, yaitu K_1, K_2, …, K_{16}. Kunci-kunci internal ini dapat dibangkitkan sebelum proses enkripsi atau bersamaan pada saat proses enkripsi. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci eksternal panjangnya 64 bit atau 8 karakter [1][2].

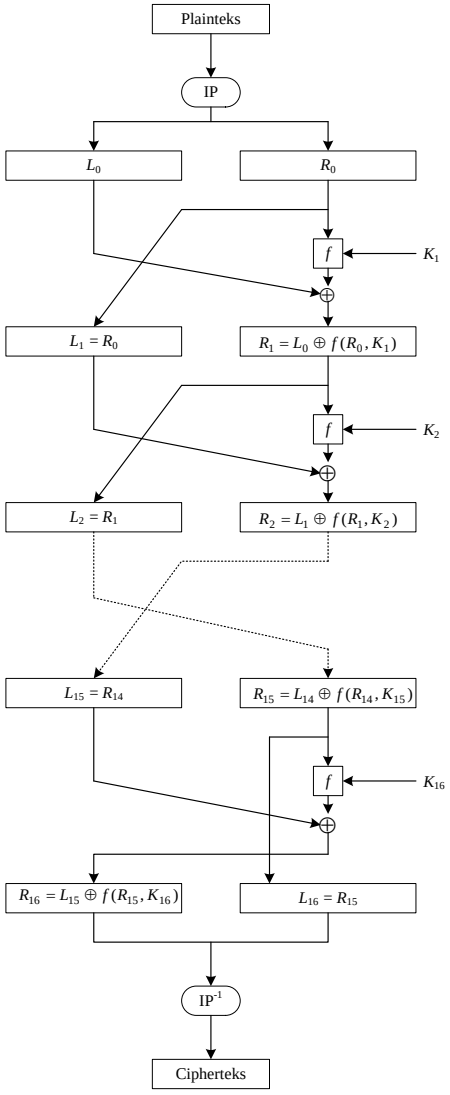
Permutasi terakhir dilakukan setelah 16 kali putaran terhadap gabungan blok kiri dan blok kanan. Proses permutasi menggunakan matriks permutasi awal balikan (*inverse initial permutation* atau IP^{-1})

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. Untuk tiap putaran 16, 15, …, 1, keluaran pada setiap putaran *deciphering* adalah:

$L_i = R_{i-1}$

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

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 [1][2].



Gambar 2. Algoritma Enkripsi dengan Algoritma DES

Teknik kriptografi merupakan salah satu solusi yang dapat dipilih untuk memproteksi file data/informasi perusahaan. Untuk menerapkan teknik kriptografi sebagai bagian yang terintegrasi dengan *security policy* perusahaan, terdapat tiga tahapan yang harus dilakukan yaitu analisis lingkungan, desain solusi dan implementasi.

3.1. Analisis Lingkungan

Tahapan analisis lingkungan bertujuan untuk mendapatkan gambaran menyeluruh mengenai struktur sistem informasi yang dimiliki oleh perusahaan. Tujuan tahapan ini adalah untuk menetapkan data/informasi apa saja yang mesti diamankan, dengan jumlah enkripsi yang minimal. Tahapan ini melalui kegiatan:

a. Mengidentifikasi data/informasi sensitif yang perlu diproteksi.
b. Melakukan analisis aliran data/informasi yang diperlukan untuk mengetahui aliran data dan aplikasi pengolahnya.
c. Melakukan identifikasi pengguna yang diperlukan untuk mengetahui siapa saja yang dapat mengakses data/informasi tersebut.
d. Identifikasi ragam ancaman terhadap keberadaan data/informasi.

Keseluruhan tahapan analisis sebaiknya juga dilakukan dengan mempelajari *security policy* yang telah diterapkan di perusahaan.

3.2. Desain Solusi

Setelah mendapatkan daftar kebutuhan pengamanan file maka langkah berikutnya adalah mendesain solusi pengamanan file dengan teknik kriptografi. Berdasarkan perkembangan teknologi pengamanan saat ini, terdapat dua strategi alternatif yang dapat digunakan yaitu dengan enkripsi secara internal pada file data/informasi dengan memanfaatkan fitur yang dimiliki oleh aplikasi pengolah data/informasi tersebut atau dengan melakukan enkripsi secara eksternal pada data/informasi tersebut.

Strategi penyimpanan data yang lebih aman adalah dengan menambahkan fungsi enkripsi pada aplikasi. Enkripsi dilakukan di dalam aplikasi sehingga data dapat ditransfer dan disimpan dalam bentuk terenkripsi. Pendekatan ini menyediakan pengamanan *end-to-end* yang baik, namun membutuhkan perubahan pada aplikasi yaitu dengan menambahkan atau memodifikasi fungsi enkripsi dan dekripsi. Salah satu langkah efektif untuk mengimplementasikan strategi ini adalah dengan membangun *server* enkripsi yang menyediakan layanan enkripsi secara terpusat (*centralized encryption service*) untuk seluruh file data/informasi.

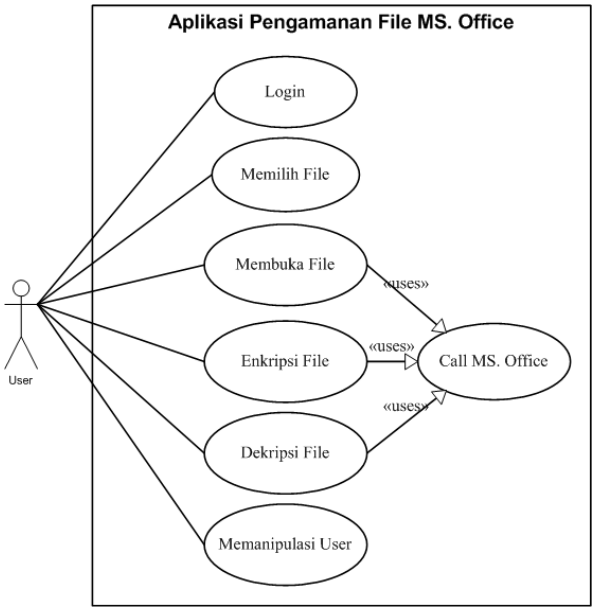
Pengimplementasian strategi ini tentunya membutuhkan sistem pengamanan yang ketat terhadap aplikasi dan server enkripsi. Solusinya adalah dengan menerapkan sistem otentikasi sehingga hanya user yang memiliki otoritas saja yang dapat mendekripsi data sensitif dengan mengakses kunci yang disimpan dalam server enkripsi.

Permasalahan yang diangkat dalam penelitian ini adalah bagaimana cara mengamanakan file data/informasi dengan teknik enkripsi secara eksternal. File data/informasi yang akan dijadikan objek adalah file yang dibuat dengan mempergunakan paket aplikasi MS. Office 2007, yaitu aplikasi MS. Word, MS. Excel, MS. Powerpoint dan MS. Access.

3.3. Pemodelan Sistem

3.3.1. Use Case Diagram

Berdasarkan jabaran hasil analisis masalah dan kebutuhan sistem seperti yang telah diuraikan di atas, maka dapat dibuatkan *use case diagram* dari sistem seperti yang digambarkan pada Gambar 3. Pada Gambar 1 terlihat bahwa sistem yang dibangun akan memiliki 7 (tujuh) buah *use case* yang mewakili proses utama pada sistem yang akan dibangun, yaitu *use case* Login, Memilih Pilih, Membuka File, Enkripsi File, Dekripsi File, Call MS.Office dan Memanipulasi User. *Use case* Login dapat dikatakan sebagai pintu masuk ke dalam sistem dan user selanjutnya dapat melakukan 4 (empat) kegiatan utama yaitu memilih, membuka, melakukan enkripsi dan dekripsi file. Kegiatan utama ini, selain memilih file, akan dihubungkan dengan kegiatan pemanggilan aplikasi MS. Office yang sesuai, yang ditunjukan oleh *use case* Call MS. Office. *Use case* Memanipulasi User adalah fasilitas tambahan untuk mengelola user.



Gambar 3. *Use Case Diagram* Sistem

3.3.2. Skenario Use Case

Pada bagian ini akan dijabarkan hanya *use case* dari kegiatan utama dari sistem. Pada Tabel 1 dijabarkan skenario dari *use case* Memilih File. Use case ini menangani pemilihan sebuah file MS. Office yang akan dijadikan objek pengamanan file.

Tabel 1. Skenario Use Case Memilih File

Deskripsi Use Case			
Nomor Use Case	2.0		
Nama Use Case	Memilih File		
Deskripsi	Melakukan pemilihan file database MS. Office 2007 untuk dijadikan objek simulasi pengamanan file.		
Aktor	User, Sistem		
Kondisi Awal	User sudah melakukan Login.		
Kondisi Akhir	User berhasil/tidak berhasil memilih file.		
Main Scenario			
No	Aksi Aktor	No	Hasil
M1	Memilih tombol Pilih	M2	Sistem menampilan window pemilihan file.
M3	User mencari dan memilih nama file yang diinginkan.	M4	Sistem memilih nama file terpilih dan menampilkan dalam textbox nama file.
Alternatif *Scenario*			
A1	Membatalkan proses pengamanan dengan menekan tombol Tutup	A2	Sistem kembali ke Menu Utama.
Exception			
E1	User tidak melakukan pemilihan file atau tidak menemukan file yang dicari.	E2	Semua proses diulangi dengan alternatif nama file yang lain atau user dapat membatalkan proses.

Pada Tabel 2 dijabarkan skenario dari *use case* Membuka File. Use case ini menangani pembukaan file yang telah dipilih dijadikan objek pengamanan file dengan mempergunakan aplikasi Microsoft Office 2007.

Tabel 2. Skenario Use Case Membuka File

Deskripsi Use Case			
Nomor Use Case	3.0		
Nama Use Case	Membuka File		
Deskripsi	Melakukan pembukaan file yang telah dipilih dengan mempergunakan aplikasi MS. Office 2007.		
Aktor	User, Sistem, MS. Office 2007		
Kondisi Awal	User sudah melakukan Login.		
Kondisi Akhir	User berhasil/tidak berhasil membuka file dengan MS. Office 2007.		
Main Scenario			
No	Aksi Aktor	No	Hasil

M1	Memilih tombol Buka	M2	Sistem akan mengaktifkan aplikasi MS. Office yang sesuai dengan jenis file yang dipilih.
Alternatif *Scenario*			
A1	Membatalkan proses pengamanan dengan menekan tombol Tutup	A2	Sistem kembali ke Menu Utama.
Exception			
E1	User belum melakukan pemilihan file.	E2	Semua proses diulangi dengan melakukan pemilihan file database.
E3	Aplikasi MS. Office 2007 tidak terinstall	E4	Sistem akan menampilkan kesalahan dan proses dibatalkan.

Tabel 3 menjabarkan skenario dari *use case* Enkripsi File. *Use case* menangani proses pengamanan file dengan melakukan enkripsi terhadap file, sehingga file ini kemudian tidak dikenali sebagai file oleh aplikasi pembuatnya.

Tabel 3. Skenario *Use Case* Enkripsi File

Deskripsi *Use Case*			
Nomor *Use Case*	4.0		
Nama *Use Case*	Enkripsi File		
Deskripsi	Melakukan proses enkripsi untuk melakukan pengamanan file.		
Aktor	User, Sistem, MS. Office 2007		
Kondisi Awal	User sudah melakukan Login dan telah memilih file yang akan diamankan.		
Kondisi Akhir	User berhasil/tidak melakukan pengamanan file.		
Main Scenario			
No	Aksi Aktor	No	Hasil
M1	Memilih tombol Enkripsi pada Form.	M2	Sistem melakukan enkripsi
M3	Sistem mengaktifkan aplikasi MS. Office 2007 yang sesuai untuk membuka file yang telah dienkripsi.	M4	MS. Office 2007 tidak mengenali file yang telah dienkripsi. File berhasil dienkripsi.
Alternatif *Scenario*			
A1	Membatalkan proses enkripsi file dengan menekan tombol Tutup	A2	Sistem kembali ke Menu Utama.
Exception			
E1	User belum memilih file.	E2	Semua skenario diulang.

Tabel 4 menjabarkan skenario dari *use case* Dekripsi File, yaitu proses pembukaan kunci terhadap file. Proses yang terjadi merupakan kebalikan dari proses pada *use case* Enkripsi File. Hasil dari proses ini adalah file menjadi mungkin untuk dimanipulasi. *Use case* ini juga baru bisa dijalankan apabila user sudah melakukan Login.

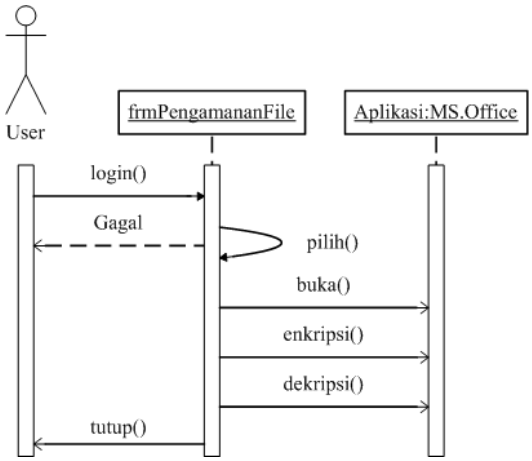
Tabel 4. Skenario *Use Case* Dekripsi File

Deskripsi Use Case			
Nomor Use Case	5.0		
Nama Use Case	Dekripsi Database		
Deskripsi	Melakukan dekripsi file yang telah dienkripsi sebelumnya untuk tujuan pengamanan.		
Aktor	User, Sistem, MS. Office 2007.		
Kondisi Awal	User sudah melakukan Login dan telah melakukan proses enkripsi.		
Kondisi Akhir	User berhasil/tidak berhasil membuka pengaman file.		
Main Scenario			
No	Aksi Aktor	No	Hasil
M1	Memilih tombol Dekripsi pada Form.	M2	Sistem melakukan dekripsi.
M3	Sistem mengaktifkan aplikasi MS. Office 2007 untuk membuka file yang telah didekripsi.	M4	MS. Office 2007 berhasil membuka file yang telah didekripsi.
Alternatif *Scenario*			
A1	Membatalkan dekripsi file dengan menekan tombol Tutup.	A2	Sistem kembali ke Menu Utama.
Exception			
E1	User belum memilih file.	E2	Semua skenario diulang.

3.4. Perancangan Sistem

3.4.1. Sequence Diagram

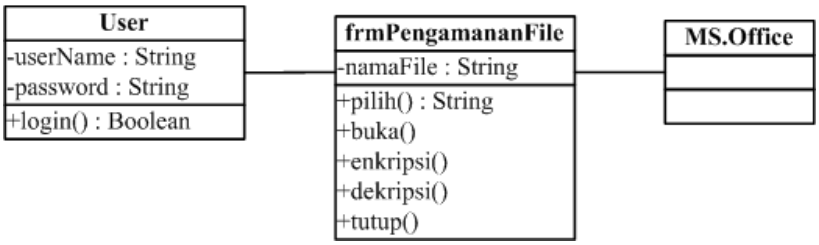
Berpedoman pada kebutuhan perangkat lunak, *use case diagram* dan deskripsinya yang telah dijelaskan pada bagian sebelumnya, maka pada Gambar 4 disajikan *sequence diagram* dari sistem yang akan dibangun. *Sequence diagram* ini menggambarkan urut-urutan proses dari sistem yang akan dibangun dan interaksi antar objek yang ada di dalam sistem.



Gambar 4. *Sequence* Diagram

3.4.2. Class Diagram

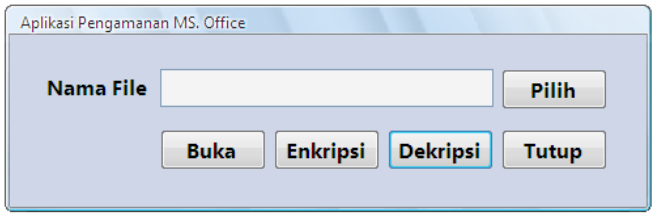
Hasil dari identifikasi class dan gambaran dari *sequence diagram*, selanjutnya dapat digambarkan dalam sebuah *class diagram*. Diagram yang tersaji dalam Gambar 5 ini adalah diagram yang menunjukkan class-class yang dimiliki oleh sistem dan interaksi atau hubungan di antara mereka.



Gambar 5. Class Diagram

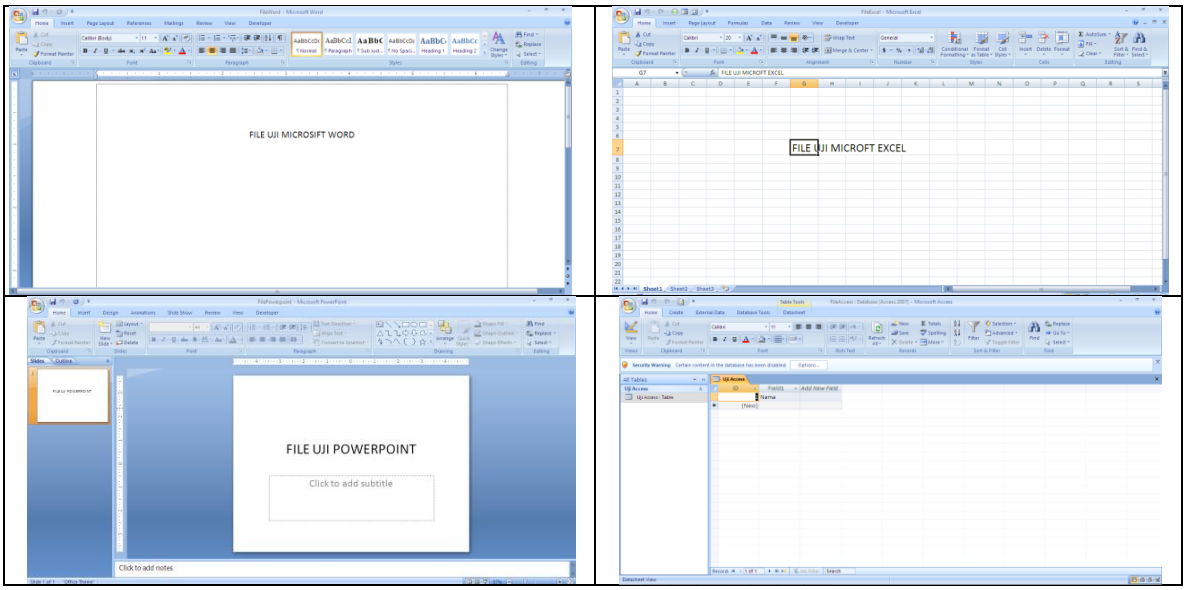
3.5. Implementasi

Form pada Gambar 6 ini dipergunakan untuk melakukan simulasi pengamanan sebuah file MS. Office yang dipilih oleh user.



Gambar 6. Antarmuka Proses Pengamanan File

Untuk melakukan pengamanan sebuah file, dalam hal ini file MS. Office, maka user harus menentukan file yang akan diamankan. Penentuan file ini dilakukan dengan cara memilih tombol Pilih yang terdapat dalam form. Dengan menekan tombol Pilih ini, sistem akan menampilkan sebuah *window*, sehingga user dimungkinkan untuk memilih file yang diinginkan. File yang mungkin untuk dipilih adalah semua file yang dibuat mempergunakan aplikasi MS. Office 2007. Setelah dipilih, nama file akan ditampilkan kembali di form.



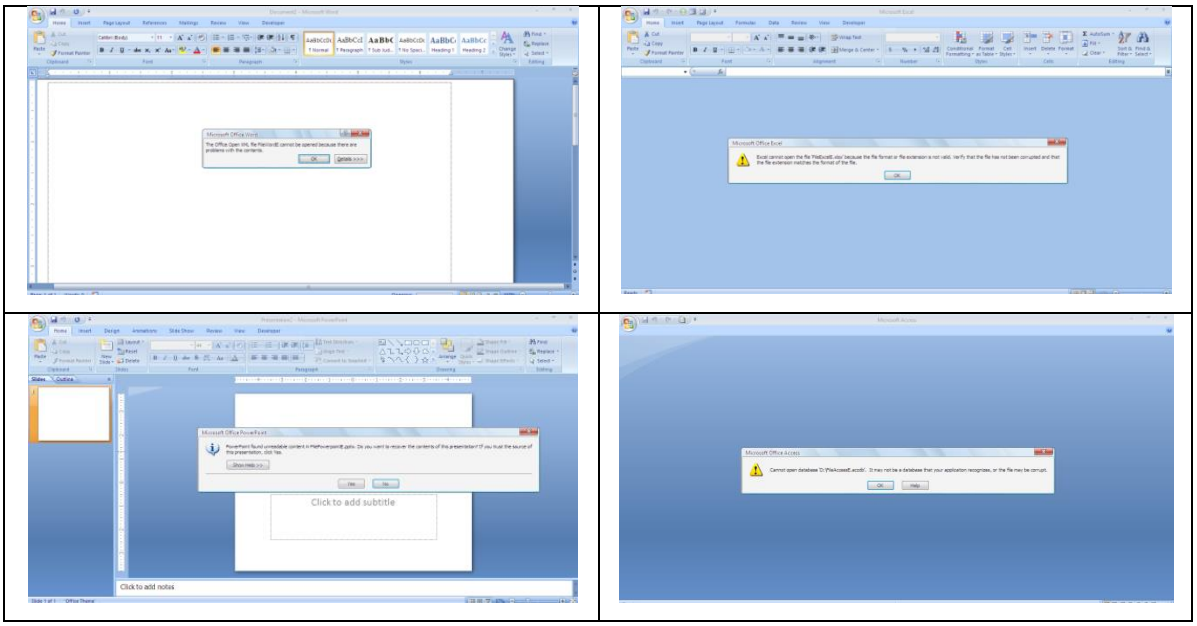
Gambar 7. Tampilan Setelah User Menekan Tombol Buka

Untuk menunjukkan sekaligus pembuktian bahwa proses pengamanan file berhasil dilakukan, ada baiknya dilakukan terlebih dahulu pembukaan file tersebut. Pembukaan dilakukan secara langsung dengan mempergunakan aplikasi MS. Office 2007. Pembukaan file dilakukan dengan menekan tombol Buka. Gambar 7 menunjukkan tampilan setelah file yang dipilih dibuka dengan aplikasi pembuatnya masing-masing.

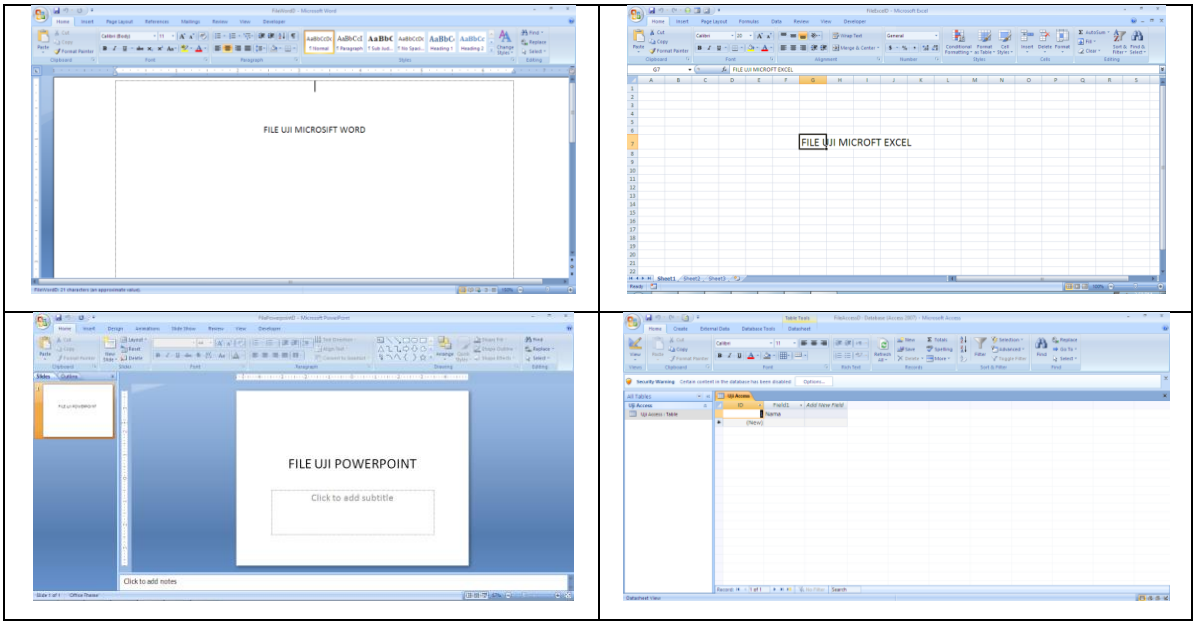
Untuk melakukan pengamanan file dengan teknik enkripsi, dapat dilakukan dengan cara menekan tombol Enkripsi. Proses enkripsi ini akan dapat dilakukan apabila user sudah memilih sebuah file, seperti yang sudah dijelaskan sebelumnya. Proses enkripsi ini akan menghasilkan sebuah file baru berjenis sama dengan nama file yang sama tetapi ditambah sebuah huruf “E” di bagian akhirnya. Proses enkripsi akan langsung dilanjutkan dengan proses pembukaan file hasil enkripsi. Gambar 8 menunjukkan tampilan aplikasi MS. Office ketika membuka file yang sudah dienkrispi.

Untuk dapat melakukan pembukaan dan manipulasi file setelah di-enkripsi adalah dengan melakukan proses dekripsi. Proses dekripsi terhadap file yang sudah di-enkripsi dapat dilakukan dengan menekan tombol Dekripsi. Proses dekripsi dilakukan dengan memanggil file yang sudah didekripsi sebelumnya. File hasil dari proses dekripsi adalah file yang namanya sesuai dengan nama file aslinya, dan ditambah akhiran “D”. Setelah proses

dekripsi, maka sistem akan memanggil aplikasi pembuat file yang didekripsi. Gambar 9 menyajikan tampilan aplikasi MS. Office ketika membuka file yang sudah didekripsi.



Gambar 8. Tampilan Setelah User Menekan Tombol Enkripsi



Gambar 9. Tampilan Setelah User Menekan Tombol Dekripsi

4. Kesimpulan

Berdasarkan uraian di atas, maka dapat ditarik kesimpulan sebagai berikut:

1. Pengamanan file MS. Office dapat dilakukan dengan melakukan enkripsi. File yang telah dienkripsi walau secara fisik tetap dapat dikenali sebagai file aslinya, ternyata tidak dapat diakses atau dibuka oleh aplikasi pembuatnya.
2. Untuk membuka file MS. Office yang sudah diamankan dengan proses enkripsi, dapat dilakukan dengan melakukan proses dekripsi. Proses dekripsi akan mengembalikan file ke bentuk aslinya, sehingga dapat dikenali dan sekaligus dapat diakses.
3. Program yang dibuat ternyata mampu mendemonstrasikan proses enkripsi dan dekripisi file MS. Office 2007.

Daftar Pustaka

[1] http://kur2003.if.itb.ac.id/file/DES.doc
[2] http://sufriadi.files.wordpress.com/2010/07/makalah-algoritma-kriptografi-des.docx
[3] Munir, Rinaldi, 2006, *Kriptografi*, Penerbit Informatika, Bandung
[4] Menezes, Alfred J., Paul C. van Oorschot & Scott A. Vanstone, 2001, *Hand Book of Applied Cripthography*, CRC Press.
[5] O'Docherty, Mike, 2005, *Object-Oriented Analysis and Design, Understanding System Development with UML 2.0,* John Wiley & Sons Ltd, West Sussex, England.
[6] Rumbaugh, James, Ivar Jacobson and Grady Booch, 1999, *The Unified Modeling Language Reference Manual*, Addison Wesley Longman, Inc.
[7] Larman, Craig. 2005. *Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development. 3rd Edition.* USA : Prantice Hall.
[8] Stallings, William, 2003, *Cryptography and Security Principles and Practice*, Prentice Hall International, Inc
[9] Kurniawan. Y, April 2004, *Kriptografi Keamanan Internet dan Jaringan Komunikasi*, Informatika Bandung