PENERAPAN APLIKASI PENGAMANAN DATA/FILE DENGAN METODE ENKRIPSI DAN DEKRIPSI ALGORITMA 3DES DALAM JARINGAN LOKAL AREA

Arisantoso[1)], Mochamad Sanwasih[2)], Moh. Reza Pahlevi [3)]

[1), 2),3)] Teknik Informatika Universitas Islam Attahiriyah Jakarta
Jalan Kampung Melayu Kecil III No. 15, Tebet, Jakarta Selatan 12840
Email : arisantoso2008@gmail.com[1)], wawanwawan451@yahoo.com[2)], mr.reza11080179@gmail.com[3)]

Abstrak

Semakin pesatnya perkembangan internet di dunia berdasarkan data statistik internetworldstat.com populasi pengguna internet tahun 2016 adalah 7,340,159,492 hal ini tentunya dapat memberikan kemudahan, keuntungan dan manfaat bagi penggunanya. Namun diiringi keberadaan resiko terhadap ancaman dari aktivitas peyalahgunaannya seperti pencurian data melalui jaringan internet. Beberapa kebocoran data dan informasi yang dilakukan oleh pihak lain dikarenakan banyaknya pengguna computer yang tidak perduli terhadap keamanan data dan tidak ada aplikasi yang membantu dalam hal keamanan data sehingga data tersebut dapat tersimpan dengan aman sewaktu menggunakan internet.

Menjaga keamanan dan kerahasiaan data adalah hal yang sangat penting dan perlu adanya upaya keseriusan guna meningkatkan kesadaran keamanan informasi baik dilingkungan pemerintah, instansi dan organisasi. Salah satu teknik mengamankan data yaitu dengan teknik penyandian atau kriptografi. Teknik Kriptografi adalah suatu teknik yang digunakan untuk mengamankan data dengan kata sandi yang dimengerti oleh pihak yang berhak mengakses data tersebut. Salah satu metode teknik kriptografi yaitu menggunakan algoritma Triple Data Encryption Standard (3DES). Algoritma 3DES ini merupakan pengembangan dari algoritma Data Encryption Standard (DES). Perbedaan antara kedua algoritma tersebut pada dasarnya algoritma yang digunakan sama namun pada algoritma DES menggunakan satu kunci yang berukuran 56bit dan 3DES menggunakan tiga kunci yang berukuran 168bit.

Hasil penelitian ini adalah menerapkan aplikasi pengamanan data menggunakan bahasa pemrograman Microsoft Visual Studio .Net. Cara kerja pengenkripsian pada kirim dan terima data yaitu pengguna mengirimkan data melalui jaringan lokal area lalu penerima data menginstal, membuka file dengan hak aksesnya (password) dari pengirim. Cara mengembalikan data yang orisinal tanpa mengalami cacat yaitu dengan cara dekripsi artinya kapasitas File yang telah dienkripsi dan kapasitas File hasil dekripsi sama dengan file asli sebelum dienkripsi.

Kata kunci: *Algoritma 3DES, Enkripsi, Dekripsi, Keamanan Data,Visual Studio.Net.*

1. Pendahuluan

Semakin pesat perkembangan dan meningkatnya kebutuhan informasi secara cepat mendorong meningkatnya kemajuan teknologi informasi secara pesat pula, termasuk didalamnya perkembangan teknologi pengiriman pesan. Saat ini pengiriman pesan dari jarak jauh bukan merupakan suatu halangan lagi dalam hal pengiriman pesan. Pesan dapat dikirim secara cepat dengan dukungan teknologi *internet*, *intranet* dan lain-lain. Perkembangan internet saat ini berdasarkan data statistik dari situs *internetworldstat.com* jumlah populasi pengguna *internet* pada tahun 2016 adalah *7,340,159,492*. Sejalan perkembangan dunia *internet* yang memberikan kemudahan, keuntungan dan manfaat bagi orang banyak dalam melakukan transaksi kirim pesan atau yang lainnya, teriring pula bersamanya keberadaan resiko ancaman dan aspek negatif dari aktivitas penggunaannya seperti pencurian data melalui jaringan *internet*.

Beberapa kebocoran data dan informasi tersebut akibat aksi yang dilakukan oleh pihak lain dikarenakan, sebagai berikut :

1. *Pertama*, masih banyaknya masyarakat pengguna komputer pada saat *on-line* yang tidak peduli dengan keamanan data yang dimiliki di dalam komputer sewaktu menggunakan *internet*.
2. *Kedua*, tidak adanya aplikasi yang dapat membantu dalam hal keamanan data sehingga data tersebut dapat tersimpan dengan aman.

Keamanan informasi baik berupa data maupun dokumen adalah sangat penting. Oleh karena itu perlu ada upaya serius guna meningkatkan kesadaran keamanan informasi (*Information Security Awareness*) tersebut baik di lingkungan pemerintah maupun swasta. Kasus *Wikileaks* hingga panama *papers* yang menghebohkan terhadap kebocoran data menjadi pelajaran penting tentang perlunya metode keamanan informasi melalui teknik kriptografi karena dokumen yang di-*release* oleh situs *Wikileaks* dan panama *papers* merupakan dokumen yang tidak terenkripsi.

Dalam Teknik kriptografi terdapat proses untuk menyandikan (enkripsi dan dekripsi) data yang akan dikirimkan. Enkripsi data dilakukan saat pengiriman informasi dengan cara mengubah atau menyandikan informasi sedangkan dekripsi dilakukan saat penerimaan

informasi yang telah disandikan menjadi informasi saat kondisi awal dengan menggunakan kunci rahasia yang sebelumnya telah disepakati bersama.

Salah satu metode kriptografi enkripsi dan dekripsi data adalah metode algoritma *Triple Data Encryption Standard* (3DES). Metode algoritma triple des merupakan pengembangan dari metode algoritma *Data Encryption Standard* (DES). Dengan menggunakan metode algoritma 3DES, kata kunci akan dienkripsi terlebih dahulu pada saat disimpan dan kemudian didekripsi pada saat proses verifikasi.

Berdasarkan latar belakang pendahuluan tersebut di atas, rumusan masalahnya antara lain sebagai berikut :

1. Bagaimana membuat aplikasi Enkripsi dan Dekripsi menggunakan bahasa pemrograman *Visual Studio .Net*?
2. Bagaimana proses kerja pengenkripsian pada pengiriman data?
3. Apakah aplikasi yang dirancang dapat mengembalikan data yang sudah diolah dengan teknik dekripsi menjadi data yang orisinal tanpa mengalami cacat sedikitpun?

Adapun tujuan dari penelitian ini adalah :

1. Untuk membuat atau merancang program aplikasi kriptosistem menggunakan bahasa pemograman jaringan dengan *Microsoft Visual Studio Net*.
2. Untuk mengetahui cara kerja dan output program Aplikasi kriptosistem dengan pemrograman *Visual Studio NET*.

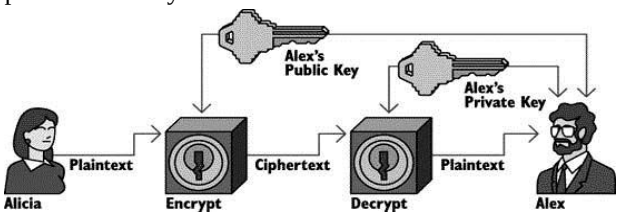
Metode yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Metode Studi Kepustakaan
   Metode studi pustaka yaitu pengumpulan data dari buku, jurnal, *internet* maupun perpustakaan yang erat hubungannya dengan judul penelitian.
2. Metode Pengembangan Sistem
   Metode pengembangan sistem yang digunakan dalam merancang aplikasi enkripsi dan dekripsi data yaitu dengan simbol-simbol alur data menggunakan *Flowchart* program.
3. Perancangan sistem menggunakan metode algoritma *Triple Data Encryption Standard* (3DES) dengan bahasa pemrograman *Visual Studio .Net*.
4. Pengujian Sistem terhadap aplikasi yang telah dirancang menggunakan metode *blackbox system*.

Menurut Jogiyanto definisi aplikasi adalah penggunaan dalam suatu *computer*, intruksi atau pernyataan yang disusun sedemikian rupa sehingga *computer* dapat memproses input menjadi *output*. Aplikasi dapat diartikan juga sebagai program komputer yang dibuat untuk menolong manusia dalam melaksanakan tugas tertentu.[1]

Definisi Data adalah sumber utama untuk menjalankan sebuah organisasi dan sangat rawan dari incaran penyerangan komputer. Apabila seseorang mencuri data dari suatu organisasi artinya ia mencuri aset dari organisasi tersebut, sama seperti ia mencuri uang atau surat berharga.[2].

Secara terminologi (ilmu asal usul kata), kriptografi berasal dari gabungan dua kata dalam bahasa yunani yaitu: "kriptos" dan "graphia" . Kata *kriptos* digunakan untuk mendeskripsikan sesuatu yang disembunyikan, rahasia atau misterius. Sedangkan kata *graphia* berari tulisan. Kriptografi didefinisikan sebagai ilmu dan pelajaran untuk tulisan rahasia dengan pertimbangan bahwa komunikasi dan data dapat dikodekan untuk mencegah dari mata-mata atau orang lain yang ingin mengetahui isinya, dengan menggunakan kode-kode dan aturan-aturan tertentu dan metode lainnya sehingga hanya orang yang berhak yang dapat mengetahui isi pesan sebenarnya.



Gambar 1. *Konsep dasar Kriptografi*

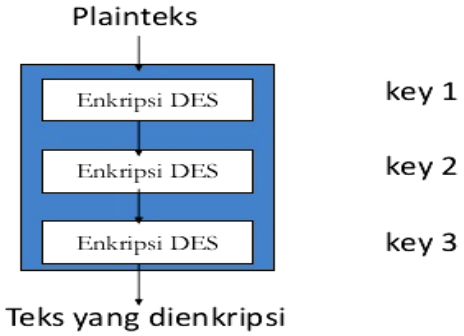
Encrypt atau enkripsi merupakan sebuah teknik yang dilakukan mengacak data asli menjadi kode rahasia sehingga menyulitkan orang yang tidak berkepentingan untuk mengakses dan mengetahui data yang asli. Sedangkan ***Decryption*** atau dekripsi adalah kebalikan dari enkripsi, dimana berfungsi untuk mendeskripsikan data yang telah dienkripsi sehingga data yang telah menjadi kode rahasia diubah kembali menjadi data biasa atau aslinya.[2]

Data yang dikirim melalui jaringan tidak jarang disadap oleh orang lain untuk kepentingan tertentu sehingga timbul usaha untuk melakukan pengkodean terhadap data sebelum dikirim melalui jaringan agar tidak bisa dibaca oleh penyadap. Ilmu matematika yang mendasari teknik enkripsi dan dekripsi disebut kriptologi sedangkan teknik dan sains dari proses enkripsi-dekripsi disebut kriptografi. Naskah asli disebut sebagai *plaintext* sedangkan naskah rahasia (yang telah dienkripsi) disebut juga *chipertext*.

Sebuah teknik enkripsi yang telah menjadi standar bagi pemerintah pada tahun 1977, atau dikenal dengan sebutan *Data Encryption Standard* (DES). Pada awalnya, algoritma DES diciptakan oleh IBM pada tahun

1970 dengan Lucifer. Algoritma DES ini dimasukkan dalam kategori *cipher modern* yang akan menggunakan algoritma rumit dengan kunci sepanjang 56bit (8byte). *Plaintext* dibagi ke dalam beberapa *blockcipher*, masing-masing 64 bit yang kemudian setiap blok dibagi dua menjadi 32bit blok kiri dan 32bit blok kanan. Setiap sub blok dipermutasi dan diberi kunci, dan proses ini dilakukan dalam 16 putaran.

Triple Data Encryption Standard (3DES) merupakan pengembangan dari DES dengan melakukan proses DES tiga kali dengan tiga kunci berbeda. 3DES memiliki tiga buah kunci yang berukuran 168bit (tiga kali kunci 56bit dari DES) dengan demikian tingkat kesulitan dalam menebak *chipertext* menjadi semakin tinggi.



Gambar 2. *Algoritma 3DES*

Berdasarkan informasi yang diperoleh, ditemukan beberapa penelitian yang membahas enkripsi dan dekripsi data menggunakan algoritma 3DES sebagai berikut:

1. Joko Susanto, Ilhamsyah dan Tedy Rismawan melakukan penelitian yang berjudul Aplikasi Enkripsi dan Dekripsi untuk keamanan Dokumen menggunakan *Triple Des* dengan memanfaatkan *USB Flash Drive*. Metode penelitian yang digunakan mencakup studi pustaka, perancangan dan metode berorientasi objek dengan pendekatan UML. Kesimpulan pada penelitian ini telah berhasil diuji dengan memanfaatkan *USB Flash Drive* dalam menjaga dokumen dengan ekstensi doc, docx, xls, xlsx dan pdf. [3]
2. Nasta Aulia, melakukan penelitian yang berjudul Jurnal Aplikasi Enkripsi dan Dekripsi menggunakan Visual Basic 2012 dengan Metode *Triple Des*. Metode Penelitian yang digunakan mencakup studi pustaka dan perancangan. Kesimpulan pada penelitian ini adalah aplikasi ini menggunakan dua metode enkripsi dan dekripsi agar lebih aman dan terjamin kerahasiaan data serta waktu yang dibutuhkan untuk proses enkripsi dan dekripsi dipengaruhi oleh kecepatan komputer yang digunakan dari ukuran file dengan ekstensi jpg.[4]
3. Adhytio Sasmita Chan, Permanan Ginting Munthe melakukan penelitian yang berjudul Perancangan Aplikasi Pengamanan File dengan Memanfaatkan *USB Flashdisk* Sebagai Kunci Menggunakan Algoritma *Triple Des*. Metode Penelitian yang digunakan mencakup studi pustaka dan perancangan. Kesimpulan pada penelitian ini adalah pengunaan *USB Flasdisk* sebagai alat proteksi sebuah file dengan cara mengenkripsinya, memproses file secara enkripsi dan dekripsi dengan menggunakan metode *triple des* sehingga keamanan file dengan ekstensi .doc lebih terjaga.[5]

Perbedaan dengan penelitian-penelitian sebelumnya diatas adalah metode pengembangan sistem yang dirancang menggunakan *flowchart* program, merancang basisdata agar aplikasi dapat dijalankan di dalam jaringan lokal area. Enkripsi dan dekripsi aplikasi pengamanan data dengan ekstensi *doc, docx, xls, xlsx, ppt, pptx, mdb, accdb, jpg, pdf, mp3, mp4* serta melakukan pengujian menggunakan metode *blackbox system.*

2. Pembahasan

Untuk menjalankan rancangan aplikasi yang telah dibangun dibutuhkan beberapa ruang lingkup yang diusulkan antara lain berupa perangkat keras (Hardware) maupun perangkat lunak (Software). Berikut ini adalah ruang lingkup untuk menjalankan aplikasi yang telah dibangun.

Dalam pembuatan perancangan aplikasi pengamanan data dengan teknik enkripsi dan dekripsi data menggunakan perangkat keras yang digunakan adalah :

1. *Prosesor Intel Core* i5 (3Ghz).
2. *RAM* DDR III 2 GB.
3. *Hardisk* dengan Kapasitas 250 GB.
4. Monitor 14 inci.

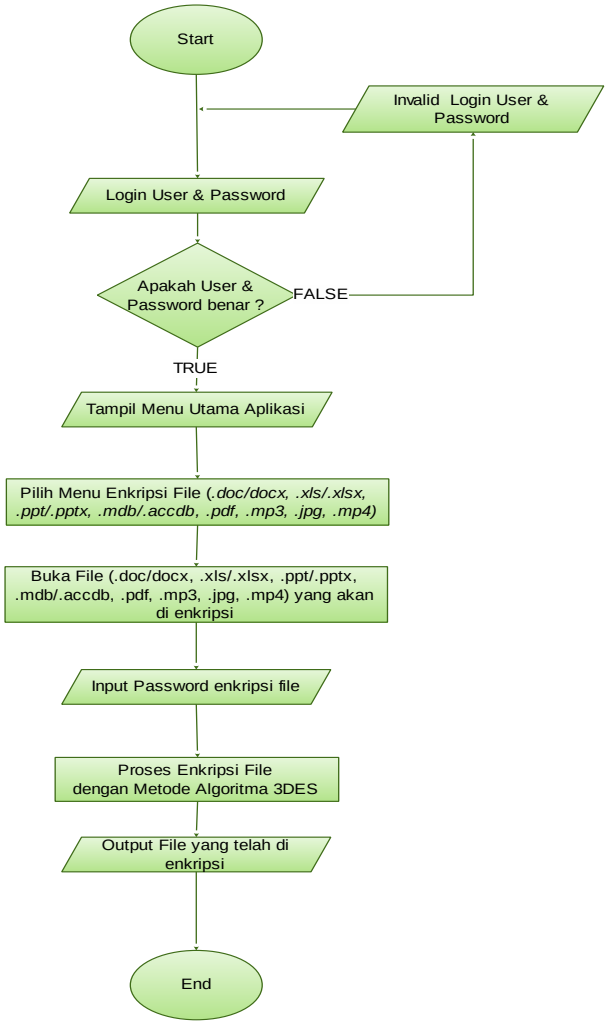
Perangkat lunak yang digunakan untuk pembuatan perancangan aplikasi ini antara lain :

1. Sistem Operasi *Microsoft Windows* 7.
2. *Microsoft Visual Studio .Net*
3. *Database Mysql*

Rancangan diagram yang diusulkan pada penelitian ini yaitu dengan menggunakan simbol-simbol *flowchart*. *Flowchart* adalah menggambarkan urutan logika dari suatu prosedur pemecahan masalah yang dituliskan dalam simbol-simbol tertentu.[6]

Dalam rancangan *flowchart* yang diusulkan menggunakan rancangan *flowchart* program. *Flowchart* Program merupakan bagan yang menjelaskan secara rinci langkah-langkah dari proses program.

Rancangan *Flowchart* program enkripsi file sebagai berikut:

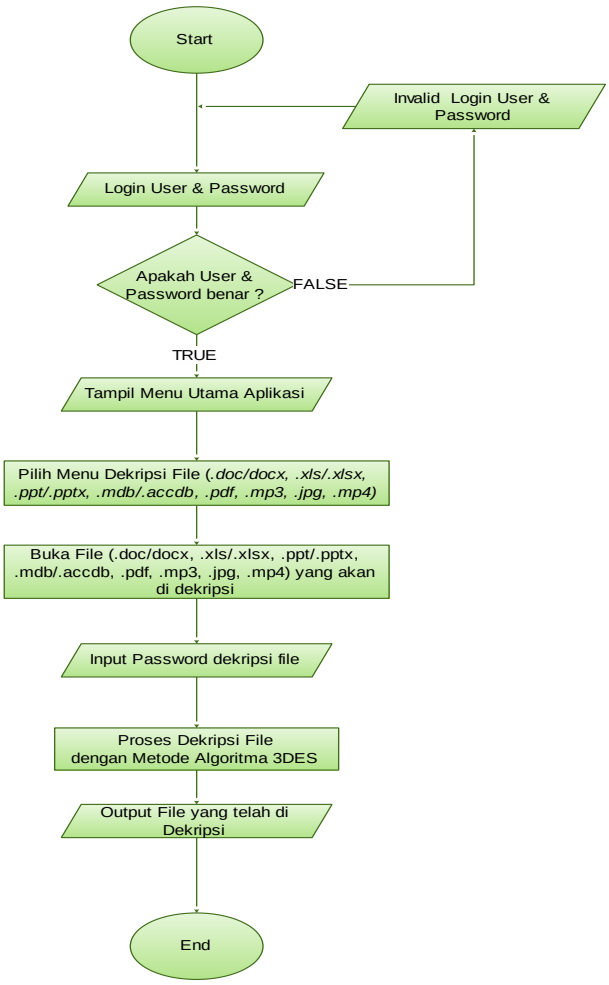


Gambar 3. *Flowchart Program Enkripsi File*

Keterangan :

1. Tahap pertama pengguna memulai aplikasi program.
2. Pengguna memasukkan login *username* dan *password*.
3. Sistem akan mengecek apakah *username* dan *password* sesuai dengan *database*, apabila benar maka sistem akan menampilkan menu utama, apabila salah maka sistem akan meminta pengguna untuk memasukkan kembali login *username* dan *password*.
4. Tahap selanjutnya pengguna memilih menu enkripsi file.
5. Pengguna memilih file yang akan dienkripsi sesuai data baik file (word, excel, powerpoint, pdf, jpg, mp3, mp4)
6. Pengguna menginput *password* enkripsi, dan memproses enkripsi File.
7. Pengguna dapat melihat *output* file yang telah dienkripsi, dan selesai dari program.

Rancangan *Flowchart* program dekripsi file sebagai berikut :



Gambar 4. *Flowchart Program Dekripsi File*

Keterangan :

1. Tahap pertama pengguna memulai aplikasi program.
2. Pengguna memasukkan login *username* dan *password*.
3. Sistem akan mengecek apakah *username* dan *password* sesuai dengan *database*, apabila benar maka sistem akan menampilkan menu utama, apabila salah maka sistem akan meminta pengguna untuk memasukkan kembali login *username* dan *password*.
4. Tahap selanjutnya pengguna memilih menu dekripsi file.
5. Langkah berikutnya Pengguna memilih file yang akan di deskripsi sesuai data baik file (*word, excel, powerpoint, pdf, jpg, mp3, mp4*)
6. Selanjutnya Pengguna menginput password enkripsi, dan memproses dekripsi File.
7. Pengguna dapat melihat *output* file yang telah di dekripsi, dan selesai dari program.

Penerapan Implementasi aplikasi pengamanan data/file dengan metode enkripsi dan dekripsi algoritma *3des* dapat dilihat pada gambar berikut ini :

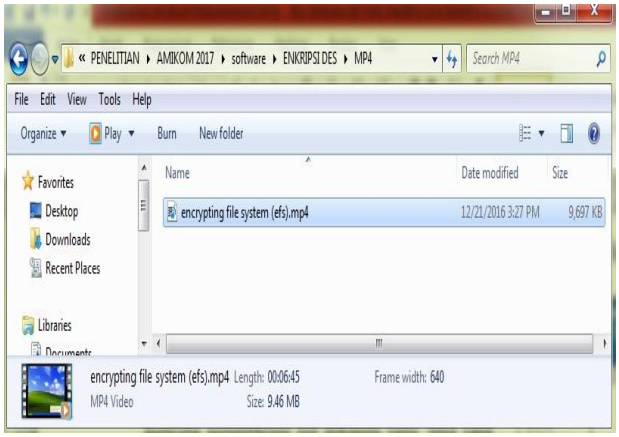
Gambar 5. *Form Login Aplikasi*

Gambar 5 merupakan form untuk login ke aplikasi pengamanan data/file dengan metode enkripsi dan dekripsi 3DES.

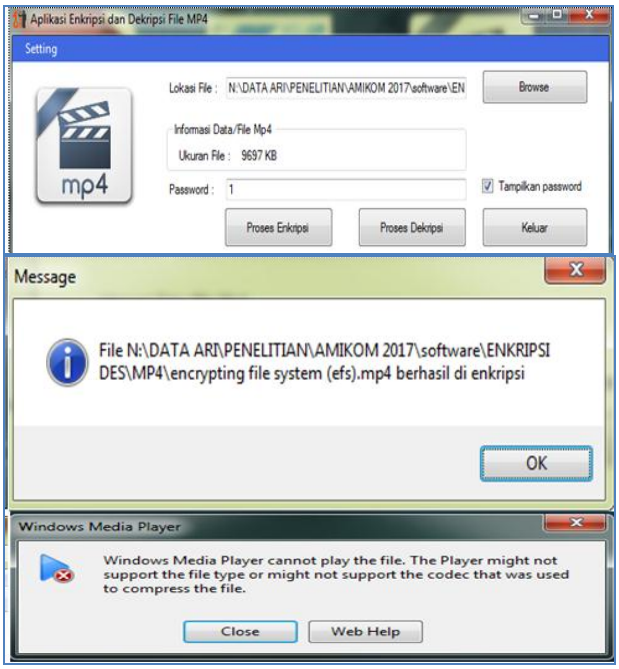
Gambar 6. *Menu Utama Aplikasi*

Gambar 6 merupakan tampilan menu utama aplikasi pengamanan data/file dengan metode enkripsi dan dekripsi seperti data (*word*, *excel*, *powerpoint*, *pdf*, *jpg*, *mp3*, *mp4*).

Salah satu contoh yang akan ditampilkan penelitian untuk menguji aplikasi ini adalah mengenkripsi file dokumen yaitu .Mp4 yang merupakan ekstensi file dari *Microsoft Windows Media Player*. Berikut adalah susunan file "**encrypting file system (efs).mp4**" untuk dienkripsi.

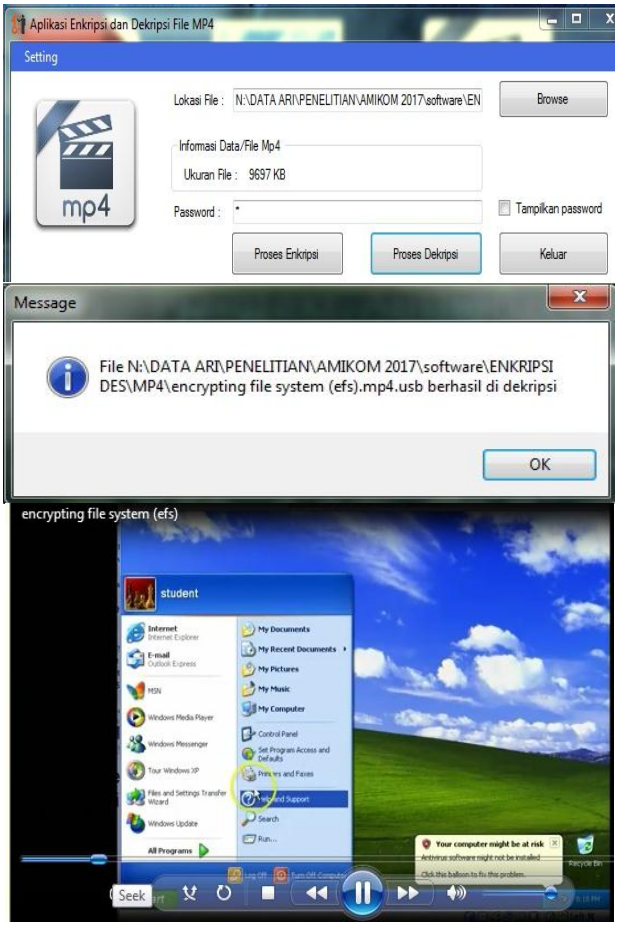


Gambar 7. *Letak File .Mp4 yang akan di enkripsi*



Gambar 8. *Contoh Uji Coba Enkripsi File .Mp4*

Pada gambar 8. terlihat pada uji coba file .Mp4 yang telah di enkripsi tidak dapat dibuka dengan aplikasi *Microsoft Windows Media Player*.



Gambar 9. *Contoh Uji Coba Dekripsi File .Mp4*

Pada gambar 9. hasil ujicoba dekripsi file .Mp4 telah berhasil di dekripsi dan file dapat dibuka dengan aplikasi *Microsoft Windows Media Player*.

Hasil evaluasi terhadap penerapan aplikasi pengamanan data/file dengan metode enkripsi dan dekripsi seperti data (*word, excel, powerpoint, pdf, jpg, mp3, mp4*) setelah di ujicoba akan dijelaskan pada tabel 1 berikut:

Tabel 1. *Hasil Evaluasi File yang di Enkripsi dan Dekripsi*

Nama File	Kapasitas File	Kinerja Enkripsi	Kapasitas File Terenkripsi	Kinerja Dekripsi
Konsep Keamanan sistem informasi berbasis internet.docx	110 KB	Berhasil Terenkripsi	110 KB	Berhasil Terdekripsi
Superstore sales.xlsx	2957 KB	Berhasil Terenkripsi	2957 KB	Berhasil Terdekripsi
Kelompok 6 enkripsi.ppt	285 KB	Berhasil Terenkripsi	285 KB	Berhasil Terdekripsi
Northwind. mdb	3344 KB	Berhasil Terenkripsi	3344 KB	Berhasil Terdekripsi
Windows server 2003 expire.pdf	180 KB	Berhasil Terenkripsi	180 KB	Berhasil Terdekripsi
Ada band – haruskah ku mati.mp3	2187 KB	Berhasil Terenkripsi	2187 KB	Berhasil Terdekripsi
Logo uniat.jpg	21 KB	Berhasil Terenkripsi	21 KB	Berhasil Terdekripsi
Encrypting file system (efs).mp4	9697 KB	Berhasil Terenkripsi	9697 KB	Berhasil Terdekripsi

3. Kesimpulan

Berdasarkan hasil pembahasan dari bab sebelumnya, maka dapat ditarik kesimpulan sebagai berikut:

1. Aplikasi pengamanan data dengan teknik enkripsi dan dekripsi dirancang menggunakan Bahasa Pemrograman *Microsoft Visual Studio .Net*.
2. Cara kerja pengenkripsian pada kirim dan terima data yaitu pengguna mengirimkan data melalui jaringan lokal area lalu penerima data menginstal membuka file dengan memperoleh hak aksesnya (password) dari pengirim agar ketika dekripsi file berhasil dilakukan dan file akan dapat dibuka.
3. Aplikasi yang dirancang setelah diujikan berhasil mengembalikan file seperti*: Word, Excel, Powerpoint, Access, PDF, Mp3, Jpeg* dan *Mp4* yang sudah diolah dengan teknik dekripsi menjadi data yang orisinal tanpa mengalami cacat sedikitpun dan file hasil dekripsi sama dengan file asli sebelum dienkripsi.

Daftar Pustaka

[1] Jogiyanto, Hartono., "Analisis dan Desain Sistem Informasi". Edisi iii. Yogyakarta: Andi, 2010.
[2] Sanusi. Muzammil, "The Genius: Hacking Sang Pembobol Data". Jakarta: PT. Elex Media Komputindo, 2010.
[3] Susanto, Joko., Ilhamsyah., Tedy Rismawan, "Aplikasi Enkripsi dan Dekripsi Untuk Keamanan Dokumen Menggunakan Triple Des Dengan Memanfaatkan USB Flashdisk Drive", J. Coding Siskom Untan, vol. 4, no. 2, pp. 1-12, Des. 2016.
[4] Aulia, Nasta. (2016-May-20). "Aplikasi Enkripsi dan Dekripsi Menggunakan Visual Basic 2012 dengan Metode Triple Des". [Online]. Available: https://www.researchgate.net/publication/303376082_jurnal_aplikasi_enkripsi_dan_dekripsi_menggunakan_visual_basic_2012_dengan_metode_triple_des.
[5] Chan, Adhytio Sasmita., Munthe., Permanan Ginting, "Perancangan Aplikasi Pengamanan File dengan Memanfaatkan USB Flashdisk Sebagai Kunci Menggunakan Algoritma Triple Des", J. Pelita, vol. viii, no. 3, pp. 30-36, Des. 2014.
[6] Sitorus, Lamhot, "Algoritma dan Pemrograman". Yogyakarta : CV Andi Publisher, 2015.

Biodata Penulis

Arisantoso, memperoleh gelar Sarjana Teknik (S.T), Universitas Islam Attahiriyah (UNIAT) Jakarta, lulus tahun 2005. Memperoleh gelar Magister Komputer (M.Kom), Universitas Budi Luhur Jakarta, lulus tahun 2013. Saat ini menjadi Dosen di Universitas Islam Attahiriyah Jakarta.

Mochamad Sanwasih, memperoleh gelar Sarjana komputer (S.Kom), Sekolah Tinggi Ilmu Komputer Bina Niaga Bogor, lulus tahun 2005. Memperoleh gelar Magister Sistem Informasi (M.Msi), Universitas Guna Darma Jakarta, lulus tahun 2013. Saat ini menjadi Dosen di Universitas Islam Attahiriyah Jakarta.

Moh. Reza Pahlevi, memperoleh gelar Sarjana Teknik (S.T), Universitas Islam Attahiriyah (UNIAT) Jakarta, lulus tahun 2016. Saat ini menjadi Tentara Nasional Indonesia (TNI) bidang Persandian.