Jurnal Rekayasa Elektrika

VOLUME 12 NOMOR 3 DESEMBER 2016

JRE	Vol. 12	No. 3	Hal 73–118	Banda Aceh, Desember 2016	ISSN. 1412-4785 e-ISSN. 2252-620X

Perancangan dan Penerapan Algoritme 4DES (Studi Kasus pada Keamanan Berkas Rekam Medis)

Yeni Yanti[1], Teuku Yuliar Arif [1,2], dan Rizal Munadi[1,2]
[1]Program Studi Magister Teknik Elektro, Fakultas Teknik, Universitas Syiah Kuala
[2]Jurusan Teknik Elektro dan Komputer, Fakultas Teknik, Universitas Syiah Kuala
Jl. Tgk. Syech Abdurrauf No. 7, Banda Aceh 23111
e-mail: s3ny_yy@yahoo.com

***Abstrak*—Informasi sangat penting artinya bagi kehidupan ini karena tanpa adanya informasi hampir semuanya tidak dapat dilakukan dengan baik. Masalah keamanan merupakan salah satu aspek terpenting dari sebuah berkas yang berisi informasi yang sensitif (berkas data rekam medis). Sering kali masalah keamanan kurang mendapat perhatian dari pemilik berkas, perancang dan pengelola sistem informasi tersebut. Salah satu cara mengantisipasinya adalah dengan metode kriptografi yang merupakan ilmu dan seni untuk menjaga keamanan pesan. Penelitian ini bertujuan mengevaluasi analisis kinerja dan membangun prototipe sistem keamanan berkas rekam medis menggunakan metode algoritme 4DES. Algoritme 4DES merupakan varian dari algoritme 3DES yang lebih kuat dan mampu melindungi informasi berkas dengan baik. Sistem keamanan algoritme 4DES mempunyai 4 kunci yang masing-masing kunci mempunyai panjang kunci 64 bit sehingga total panjang 4 kunci 256 bit dan K1≠K2≠K3≠K4. Berkas (*Word*, *Excel*, dan Gambar) terenkripsi/terdekripsi menggunakan kunci eksternal minimum 8 karakter (64 bit). Dalam proses enkripsi dilakukan penambahan *padding bytes* disetiap ukuran blok data untuk menimimalkan serangan dari penyerang menggunakan proses mode operasi CBC. Hasil yang didapat yaitu kecepatan waktu proses berkas terenkripsi menggunakan algoritam 4DES dalam hitungan detik terjadi selisih waktu 1 detik dibandingkan dengan kecepatan waktu proses berkas terenkripsi algoritme 3DES. Selain itu, algoritme 4DES memiliki keungulan dari segi keamanan berkas yaitu memiliki ketahanan waktu 3.45 x10^{56} tahun lebih lama terhadap serangan teknik *brute force* yang mampu mengetahui teks berkas dan kunci rahasianya.**

Kata kunci: ***berkas rekam medis, enkripsi, algoritme 3DES, algoritme 4DES, brute force***

***Abstract*—Information is necessary for life because everything can not be done properly in the absence of information. The security problem is one of the most crucial aspects of a file containing sensitive information, for example, medical record files. Often, the file owner, designer, and manager of the information systems pay less attention to the security issues. One way to anticipate this is by using a cryptographic method, which is the science and art to keep the message security. This study aimed to evaluate the performance analysis and building a security system prototype of medical record files using the 4DES algorithm. The 4DES algorithm is a variant of the 3DES algorithm that is more robust and capable of protecting information properly. The 4DES security system has four keys; each key has a key length of 64 bits so that the total length of four keys is 256 bits and K1≠K2≠K3≠K4. The encrypted / decrypted files (Word, Excel, and Image) using an external key of minimum eight characters (64 bits). During encryption, there was an addition of padding bytes in each of data block size to minimalized attack from the attacker using a CBC operation mode process.**
Results showed that the processing speed of the encrypted files using the 4DES was 1 second faster than that of using the 3DES algorithm. Also, 4DES algorithm has superiority regarding of file safety, which has time enduring 3.45 x1056 years longer to brute force attack technique which able to discover text file and the secret key.

Keywords: ***medical record file, lock password, encryption algorithm 3DES, 4DES algorithms, brute force***

I. PENDAHULUAN

Pada zaman teknologi komputer ini, masyarakat menggunakan sistem informasi yang berbasis komputer, terutama didalam *Microsoft Office* terdapat berkas yang berisi informasi. Kemajuan sistem informasi memiliki banyak keuntungan dalam kehidupan manusia, namun juga memiliki aspek negatif yang banyak terjadi pada kejahatan komputer, yang meliputi pencurian, penipuan, pemerasan, kompetitif, dan banyak lainnya. Berkas yang berisi informasi penting bila jatuh ketangan pihak yang lain atau pihak yang tidak berkepentingan/berhak dapat menimbulkan kerugian bagi pemilik berkas informasi tersebut. Oleh karena itu, salah satu cara mengantisipasinya adalah dengan menggunakan metode kriptografi yang merupakan ilmu dan seni untuk menjaga keamanan pesan. Hal ini bertujuan untuk menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak bertanggung jawab [1],[2].

Masalah keamanan merupakan salah satu aspek terpenting dari sebuah berkas yang berisi informasi yang

ISSN. 1412-4785; e-ISSN. 2252-620X
DOI: 10.17529/jre.v12i3.3271

sensitive, misalnya berkas data rekam medis. Sering kali masalah keamanan kurang mendapat perhatian dari pemilik berkas, perancang dan pengelola sistem informasi tersebut. Masalah keamanan seringkali berada di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila menggangu performansi dari sistem, seringkali masalah keamanan tidak begitu diperdulikan bahkan ditiadakan.

Beberapa algoritme yang dapat digunakan pada sistem keamanan berkas antara lain DES, 3DES, Blowfish, dan AES dari hasil studi literatur [3],[4]. Penerapan sistem keamanan 3DES untuk berkas menunjukkan bahwa proses enkripsi dan dekripsi data diimplementasikan dari algoritme DES dengan waktu yang diperlukan sesuai dengan ukuran berkas, spesifikasi dan proses yang dilakukan pada perangkat keras. Selain itu, plainteks yang diproses dengan kunci 1, kunci 2 dan kunci 3 menghasilkan cipherteks dengan jumlah karakter yang lebih besar, karena adanya proses padding dan disimpan dalam bentuk heksadesimal [5].

Dari hasil studi literatur pada penelitian yang dilakukan oleh Verma, dkk, menunjukkan bahwa *Blowfish* merupakan kinerja algoritme terbaik yang tidak hanya tercepat tetapi juga menyediakan keamanan besar melalui ukuran kunci yang kuat sehingga memungkinkan dapat digunakan dalam aplikasi yang lain. Sebaliknya, 3DES merupakan kinerja algoritme terlambat dibandingkan DES dan AES [6].

Kemudian penelitian yang dilakukan oleh Bemby Bantara Narendra, menjelaskan alasan utama mengapa algoritme cipher blok DES menjadi tidak aman lagi adalah terutama pada panjang kunci yang dipakai dalam algoritme ini masih terlalu pendek dan varian dari algoritme cipher blok 3DES masih dinilai aman karena cukup panjang untuk menjamin kompleksitas enciphering namun pemanfaatannya saat ini semakin kurang. Hal ini disebabkan oleh waktu performasi algoritme ini dan algoritme DES yang kurang baik ketika diterapkan dalam *software* [7].

Berdasarkan penelitian yang telah diteliti oleh Bemby Bantara Narendra, penelitian ini merancang algoritme 4DES varian dari algoritme 3DES yang mempunyai 4 kunci yang masing-masing kunci mempunyai panjang kunci 64 bit sehingga total panjang 4 kunci 256 bit dan K1≠K2≠K3≠K4, mampu mengamankan informasi/ berkas dengan baik dan mampu melindungi dari serangan pasif (*Chosen-plaintext attack*) yang menggunakan *Brute Force*. Simulasi pengujian penelitian ini menggunakan berkas (*Word, Excel*, dan Gambar) dienkripsi/didekripsi menggunakan kunci *eksternal* minimum 8 karakter (64 *bit*) didalam proses enkripsi dilakukan penambahan padding *bytes* disetiap ukuran blok data untuk menimimalkan serangan dari penyerangan.

Selanjutnya dilakukan proses pebandingan kecepatan waktu proses data terenkripsi dan hasil tingkat keamanan pada saat proses algoritme 3DES dan alogirtma 4DES.

II. Studi Pustaka

A. Sistem Kriptografi

Sistem kriptografi terdiri dari 5 bagian yaitu :

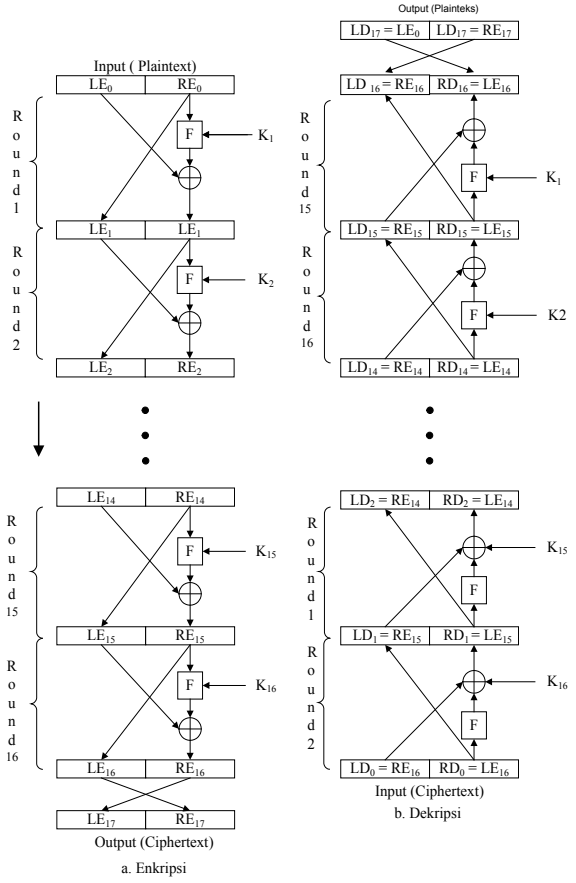
1. ***Plaintext*** : pesan atau data dalam bentuk aslinya yang dapat terbaca. Plaintext adalah masukan bagi algoritme enkripsi dan disebut dengan teks asli.
2. ***Secret Key***: *secret key* yang juga merupakan masukan bagi algoritme enkripsi merupakan nilai yang bebas terhadap teks asli dan menentukan hasil keluaran algoritme enkripsi dan digunakan istilah kunci rahasia.
3. ***Ciphertext***: keluaran algoritme enkripsi. *Cpihertext* dapat dianggap sebagai peasan dalam bentuk tersembunyi. Algoritme enkripsi yang baik akan menghasilkan *ciphertext* yang terlihat acak. Untuk selanjutnya digunakan istilah teks sandi.
4. **Algoritme Enkripsi**: Algoritme enkripsi memiliki 2 masukan teks asli dan kunci rahasia. Algoritme enkripsi melakukan transformasi terhadap teks asli sehingga menghasilkan teks sandi.
5. **Algoritme Dekripsi**: Algoritme dekrisi memiliki 2 masukan yaitu teks sandi dan kunci rahasia. Algoritme dekripsi memulihkan kembali teks sandi menjadi teks asli kunci rahasia yang dipakai algoritme dekripsi sama dengan kunci rahasia yang dipakai algoritme enkripsi [8].

B. Struktur DES

Masukkan untuk algoritme enkripsi DES adalah teks asli berukuran *w* bits dan sebuah kunci *K*. Terdapat algoritme pembangkit kunci ronde yang diturunkan dari kunci *K* menghasilkan kunci ronde $K_1,...,K_{16}$ untuk 16 ronde.Teks asli dibagi dua yang sama ukurannya disebut dengan LE_0 (*Left* Enkripsi), LD_0 (*Left* Dekripsi) dan RE_0 (*Right* Enkripsi), RD_0 (*Right* Dekripsi). Tiap ronde memiliki struktur yang sama terdiri dari *Mixer* dan *Swapper*. *Mixer* Ronde ke-*i* memiliki masukan dari ronde sebelumnya L_{i-1} dan R_{i-1} (untuk ronde pertama masukan adalah teks asli) dan kunci ronde ke-*i* (K_i). Pada tiapa ronde parush sebelah kiri masukan (L_{i-1}) disubstitusikan menggunakan *S-Box* dengan hasil operasi *XOR* antara dan L_{i-1} dan rangkaian bit hasil pengaplikasian kunci K_i dan paruh sebelah kanan masukan (R_{i-1}) terhadap sebuah fungsi ronde (sandi produk) *F* dan keluaran *F*. Setelah itu sebuah komponen swap menukar isi L_i dan R_i dan menjadi masukkan untuk ronde selanjutnya [8],[9]. Terlihat pada Gambar 1.

C. Fungsi Chiper Feistel

E merupakan fungsi yang mengambil blok 32 bit sebagai input dari hasil blok 48 bit sebagai output [10],[11]. Perhitungan dari fungsi *F(R,K*) .Terlihat pada Gambar 2.



Gambar 1. Struktur DES

III. METODE

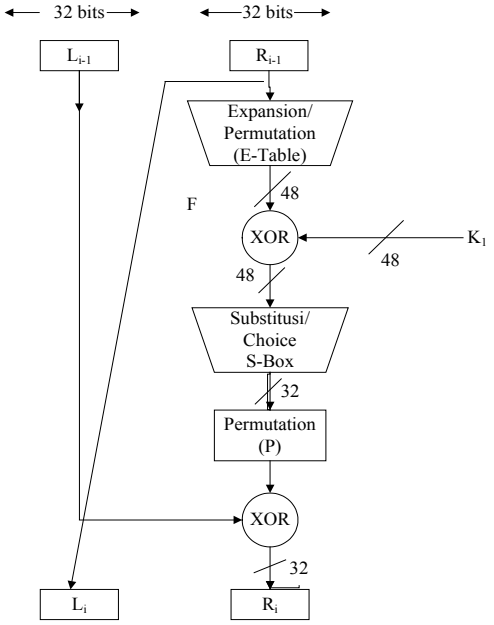
A. Penerapan Algoritme 3DES

Dalam kriptografi, *3DES* adalah sebuah *cipher* blok yang dibentuk oleh DES dengan menggunakannya tiga kali. Cara kerja dari model enkripsi ini adalah mengambil tiga kunci sebanyak 64 *bit* dari seluruh kunci yang mempunyai panjang 192 *bit* [12],[13].

Prosedur untuk enkripsi sama dengan DES tetapi diulang sebanyak 3 kali. Data dienkripsi dengan kunci pertama kemudian didekripsi dengan kunci kedua dan pada akhirnya dienkripsi lagi dengan kunci yang ketiga. Dan Sebaliknya untuk proses dekripsi dimulai dari K3 lalu K2 dan K1 untuk kembali mendapat isi informasi [14]. Terlihat pada Gambar 3. Kunci algoritme 3DES yang memiliki pemilihan kunci eksternal yang berbeda antara K1 berbeda dengan K2 dan K2 berbeda dengan K3 (K1≠K2≠K3).

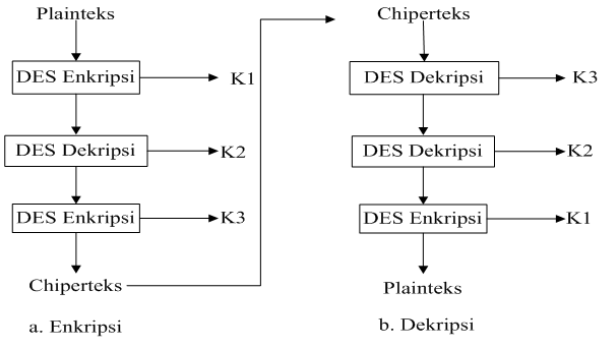
B. Penerapan Algoritme 4DES

Pada penelitian ini menerapkan algoritme 4DES yang merupakan *Chiper Blok* yang dibentuk oleh DES dan 3DES dengan menggunakan kunci *eksternal*. Algoritme 4DES membutuhkan 4 kunci sebanyak 256 *bits* dalam proses enkripsi dan dekripsi. Prosedur untuk enkripsi sama dengan DES tetapi diulang sebanyak 4 kali. Data dienkripsi

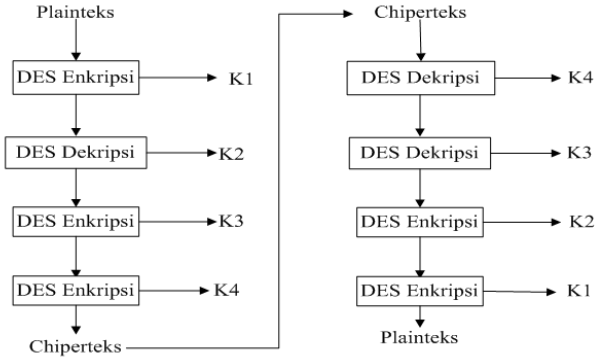


Gambar 2. Fungsi Cipher Feistel

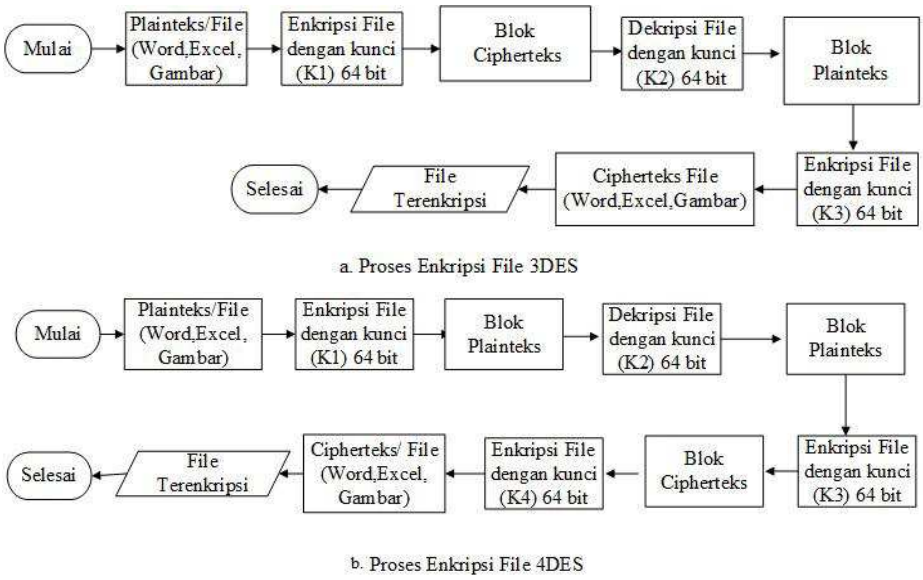
dengan kunci pertama kemudian didekripsi dengan kunci kedua lalu dienkirpsi dengan kunci ketiga dan terakhir dienkripsi dengan dengan kunci yang keempat. Dan Sebaliknya untuk proses dekripsi dimulai dari K4,K3,K2 dan K1 untuk kembali mendapat isi informasi. Pemilihan kunci untuk 4DES yaitu K1≠K2≠K3≠K4. Terlihat pada Gambar 4.



Gambar 3. Flowchat kunci 3DES



Gambar 4. Flowchat kunci 4DES



Gambar 5. Proses enkripsi berkas

C. *Proses Enkripsi*

Encode (enkripsi) adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa mengerti [15],[16]. Proses enkripsi kunci yang digunakan dalam bentuk format karakter biasa (8 karakter) dan *plainteks* yang digunakan bentuk berkas data rekam medis.

Proses berkas enkripsi 3DES, kunci yang digunakan 3 kunci *eksternal* yaitu K1 (enkripsi),K2 (dekripsi) dan K3 (enkripsi), sedangkan untuk proses berkas enkripsi 4DES, kunci yang digunakan 4 kunci *eksternal* yaitu K1 (enkripsi), K2 (dekrispsi), K3 (enkripsi) dan K4 (enkripsi).

Plainteks Berkas dilakukan proses enkripsi dengan menggunakan kunci *eksterna*l (*K*) 64 bit lalu menghasilkan blok *cipherteks* yang berisi bit teracak/tidak beraturan. Selanjutnya blok tersebut dilakukan proses dekripsi menggunakan kunci (*K*) 64 bit menghasilkan juga suatu blok yang bit yang beraturan .

Untuk proses keamanan sistem berkas menggunakan 3DES. Proses dekripsi yang menghasilkan blok plainteks dilakukan sekali lagi proses pengacakan bit didalam proses enkripsi yang mana hasil isi berkas bit tersebut semakin sulit untuk dimengerti/dibaca [14].

Sedangkan untuk proses keamanan sistem berkas menggunakan 4DES proses enkripsi yang menghasilkan blok cipherteks pada proses enkripsi 3DES dilakukan sekali lagi proses pengacakan bit didalam proses enkripsi .

Sehingga menghasilkan isi bit pada berkas yang sangat teracak dan sulit di mengerti dan keamanan berkas lebih terjaga. Terlihat pada Gambar 5. Blok penyadian dalam proses enkripsi 3DES/4DES tiap blok perblok hingga blok terakhir, terjadi proses penambahan padding byte baik itu bila terjadi ganjil blok ataupun genap blok.

D. *Proses Dekripsi*

Decode (Dekripsi) adalah proses dengan algoritme yang sama untuk mengembalikan informasi teracak menjadi bentuk aslinya[15],[16]. Kunci yang digunakan sama dengan kunci saat dilakukan proses enkripsi menggunakan algoritme 3DES dan algoritme 4DES.

Proses dekripsi ini digunakan berkas yang telah dienkripsi atau yang sering disebut dengan chiperteks . Proses ini bertujuan untuk mengembalikan berkas yang tidak bisa dimengerti menjadi berkas yang bisa dimengerti.

Proses kerja dekripsi algoritme 3DES/4DES untuk berkas sama halnya dengan proses kerja enkripsi pada berkas rekam medis. Menggunakan kunci *eksternal* dan blok penyadian. Bila terjadi penambahan blok terakhir pada proses enkripsi, di proses dekripsi ini akan dilakukan pemisahan blok yang asli berisi isi bit berkas dengan blok penambahan *padding byte*. Terlihat pada Gambar 6.

IV. HASIL DAN PEMBAHASAN

A. *Rancangan Database*

Database yang terbentuk terdiri dari dua tabel yaitu tabel admin dan tabel pasien. Tabel pasien terdiri dari dua kolom yaitu id_pasien dan nama_dokter. Tabel ini berfungsi untuk menyimpan data pasien dan dokter.

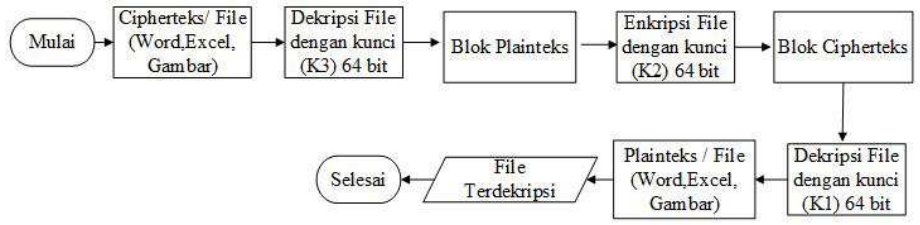
Tabel 1 menunjukkan implementasi tabel admin yang merupakan tabel *username* dan *password* admin yang

Tabel 1. Implementasi tabel admin serta tipe data penyusunnya

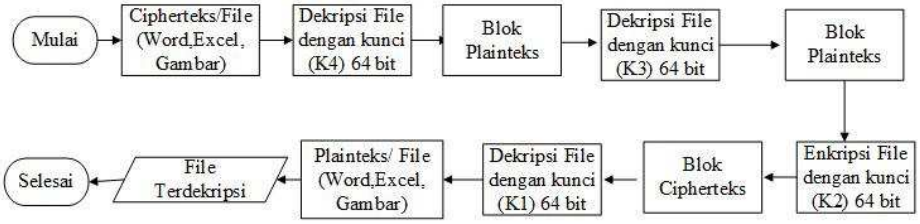
Nama Field	Tipe Data (ukuran)	Keterangan
Username	Varchar(20)	Username admin
Password	Varchar(32)	Password admin

Tabel 2. Implementasi tabel data pasien serta tipe data penyusunnya

Nama Field	Tipe Data (ukuran)	Keterangan
Id_pasien	Int (30)	ID pasien
Nama_dokter	Varchar(32)	Nama dokter



a. Proses Dekripsi File 3DES



b. Proses Dekripsi File 4DES

Gambar 6. Proses dekripsi berkas

diberi izin untuk melakukan untuk login aplikasi sistem keamanan.

Tabel 2 menunjukkan implementasi tabel data pasien yang diberikan kepada pertugas rekam medis untuk mengisi data pasien berdasarkan Id_pasien dan nama dokter .

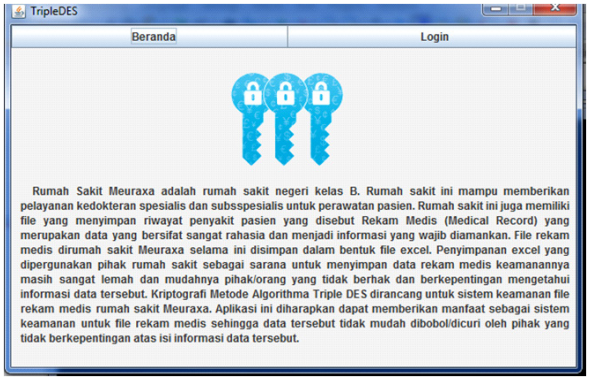
B. Implementasi Sistem

Tampilan perancangan desain program utama user perangkat lunak dimaksud untuk memberikan kemudahan dalam proses melakukan sistem keamanan untuk berkas rekam medis. Selain itu pada tampilan ini juga terdapat beranda dan *login*. Menu beranda yang memberikan keterangan tentang sistem keamanan atau kriptografi.

Adapun tampilan menu utama *user* yang dilakukan dengan konversi algoritme 3DES/4DES dalam bahasa pemograman Java. Terlihat pada Gambar 7.

Untuk dapat melanjutkan ke proses menu yang selanjut, harus lebih dahulu untuk mengisi menu admin ini sesuai dengan username dan password yang telah ditentukan.

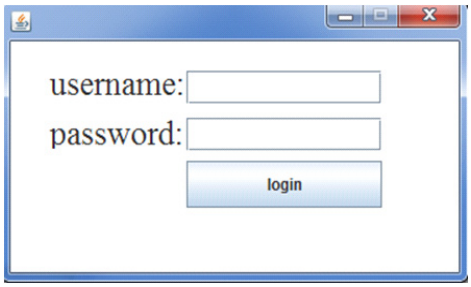
Bila dalam pengisian *username* dan *password* salah maka tidak bisa melanjutkan proses selanjutnya. Terlihat pada Gambar 8.



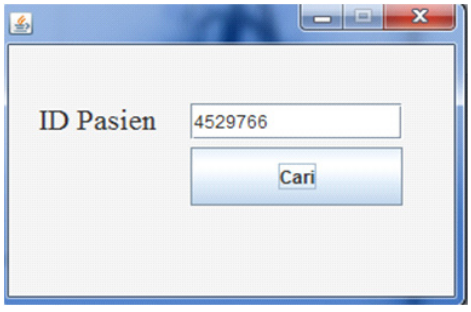
Gambar 7. Halaman depan aplikasi

Tampilan menu Id ini dibuat untuk melakukan proses pencarian data pasien untuk kemudahan mencari berkas pasien. *Id_* pasien yang digunakan berupa nomor KTP atau nomor Asuransi kesehatan pasien yang diinput. Terlihat pada Gambar 9.

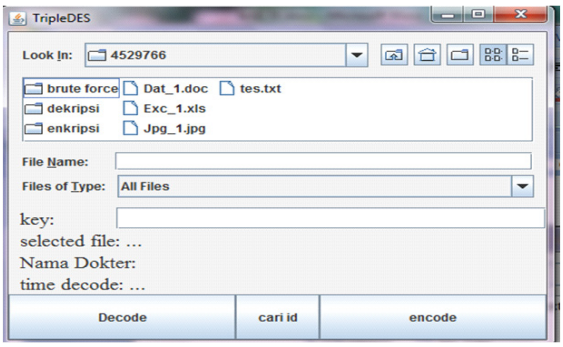
Kemudian untuk tampilan menu berkas ini merupakan program yang dibuat untuk melakukan proses enkripsi dan dekripsi . Menu berkas ini berdasarkan folder *Id_*Pasien didalam folder Id-Pasien berisi berkas data pasien (*Word, Excel*, dan Gambar) dan nama dokter sesuai riwayat penyakit pasien setelah itu dan terdapat berkas yang akan dienkripsi/dekripsi. Berkas tersebut berupa berkas *Word, Excel*, dan Gambar cukup mengklick *doubell* pada salah satu berkas tersebut. Lalu masukan key eksternalnya sebanyak 8 bytes untuk melakukan proses keamanan dengan menggunakan pilihan encode.



Gambar 8. Menu *Login*



Gambar 9. Menu *ID_Pasien*



Gambar 10. Menu berkas

Data yang di hasilkan tidak dapat dimengerti oleh orang yang tidak berhak sedangkan decode data yang dihasilkan menghasilkan data asli atau data yang akan dimengerti/dibaca. Terlihat pada Gambar 10.

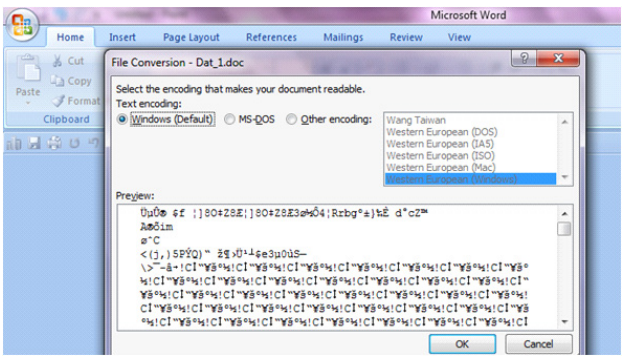
C. *Hasil Pengujian Keamanan Berkas Data Rekam Medis*

Pengujian keamanan berkas data rekam medis dalam penelitian ini dilakukan menggunakan berkas (*Word,Excell*,Gambar) untuk hardware menggunakan *Processor Intel(*R) *Core* (TM) *i3*-5005U (2.00 *GHz*).

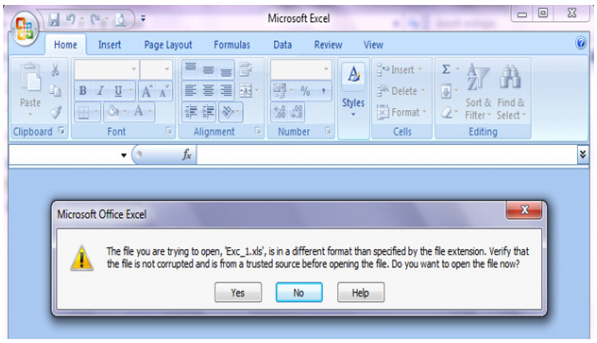
Berkas data rekam medis dikonversi ke dalam suatu urutan *digit biner* (*bits*) yaitu 0 dan 1, yang umumnya digunakan untuk *Schema Encoding* dalam *America Standar Code for Information Interchange (ASCII)* [13].

Hasil pengujian keamanan berkas rekam medis (Plainteks) dilakukan proses enkripsi yang berasal dari algoritme 3DES dan algoritme 4DES. Terlihat pada Gambar 11, Gambar 12, dan Gambar 13.

Setiap bit plainteks dan bit kunci yang digunakan untuk membangkitkan kunci acak semu melalui *Pseudo-Random Sequence Generator Domnness* yang merupakan suatu nilai yang terlihat seperti diacak, tetapi sebenarnya nilai tersebut merupakan suatu urutan bit . lalu pada saat proses enkirpsi *Pseudo-Random Sequence Generator* menghasilkan urutan bit yang sama secara berulang-ulang pada penempatan yang berbeda yang mengakibatkan plainteks tidak dapat dimengerti/dibaca. Kemudian untuk mendapatkan cipherteks atau untuk mendapatkan informasi yang dapat di mengerti dilakukan proses operasi *XOR* pada kunci acak semu dengan plaintext tersebut.



Gambar 11. Hasil berkas Dat_1 Enkripsi



Gambar 12. Hasil berkas Exc_1 Enkripsi

D. *Hasil Pengujian Perbandingan Ukuran Berkas Data Asli Sebelum dan Sesudah Menggunakan Sistem Keamanan* .

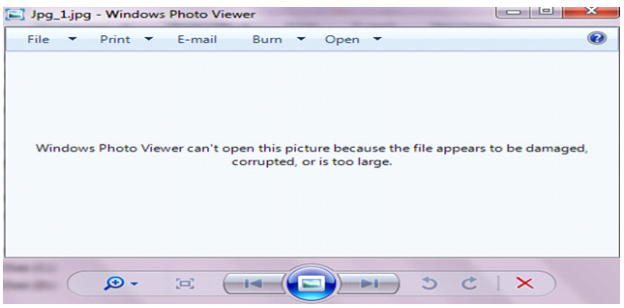
Simulasi dari beberapa berkas jenis *word,excell* dan gambar dengan ukuran yang berbeda. Kolom ukuran berkas asli (*bytes*) merupakan kolom yang belum dilakukan sistem kemanan dan ukuran berkas yang akan digunakan untuk ukuran yang akan dilakukan proses.

Kolom ukuran berkas terenkripsi (*bytes)* dan kolom ukuran terdekripsi (*bytes*) merupakan ukuran berkas yang menggunakan sistem keamanan algoritme 3DES/4DES. menghasilkan penyusunan blok-blok data yang berukuran sama.

Proses enkripsi melakukan pembagian dan penyusunan setiap jumlah plaintext (ukuran berkas) menjadi blok-blok yang telah ditentukan 64 bits (8 *bytes*) yang

Terlihat pada Tabel 3. Sebagian ukuran blok data tidak memiliki ukuran ukuran blok yang sama sehingga di butuhkan padding byte sebagai pengganjal untuk menggenapi data agar sesuai dengan ukuran blok yang telah ditentukn. Namun sebagian ukuran data yang lain sudah genap dengan ukuran blok yang ditentukan juga terjadi proses penambahan padding karena sesuai dengan PKCS (*Public Key Crytography Standard*) data tetap harus ditambahakan minimal 1 byte dan maksimal 8 byte dan menggunakan proses mode operasi CBC (*Cipher Block Chaining*) untuk meminimalkan serangan terhadap blok maka diperlukan beberapa cara agar posisi dan ukuran yang ada tidak sama.

Didalam proses dekripsinya semua ukuran data dilakukan proses pemisahan byte mana yang berupa data (plainteks) dan *byte* mana yang berupa padding byte



Gambar 13. Hasil berkas Jpg_1 Enkripsi

Tabel 3. Hasil pengujian ukuran berkas menggunakan 3DES/4DES

Ukuran File Asli *(bytes)*	Ukuran File Terenkripsi *(bytes)*	Selisih Ukuran File Asli dengan File Terenkripsi *(bytes)*	Ukuran File Terdekripsi *(bytes)*	Selisih Ukuran File Asli dengan File Terdekripsi *(bytes)*
File *Word*				
153.600	153.608	8	153.600	8
272.896	272.894	8	272.896	8
334.848	334.856	8	334.848	8
434.176	434.184	8	434.176	8
555.520	555.527	8	555.520	8
673.280	673.288	8	673.280	8
713.848	713.848	8	713.848	8
881.664	881.671	7	881.664	7
967.680	967.688	8	967.680	8
1.050.112	1.050.120	8	1.050.112	8
File *Excel*				
123.392	123.400	8	123.392	8
231.424	231.432	8	231.424	8
334.848	334.856	8	334.848	8
491.008	491.016	8	491.008	8
565.248	565.264	8	565.248	8
620.544	620.552	8	620.544	8
731.135	731.144	8	731.135	8
863.744	863.760	8	863.744	8
957.952	957.960	8	957.952	8
1.111.552	1.111.560	8	1.111.552	8
File Gambar				
102.266	102.272	6	102.266	6
210.084	210.088	4	210.084	4
339.880	339.888	8	339.880	8
416.988	416.992	4	416.988	4
515.154	515.160	6	515.154	6
613.459	613.464	5	613.459	5
721.485	721.488	3	721.485	3
820.879	820.880	1	820.879	1
921.925	921.928	3	921.925	3
1.025.849	1.025.856	7	1.025.849	7

menggunakan *XOR*, tetapi pada proses ini pemisahan data dan padding hanya bisa dilakukan bila hasil dekripsinya mengandung *byte padding* yang *valid* atau menggunakan kunci yang sesuai saat melakukan proses enkripsi. Sehingga menghasilkan ukuran blok asli sebelum digunakan proses sistem keamanan disemua jenis ukuran data.

E. Pengujian Kunci Eksternal 12ab13cd Proses Enkripsi/ Deskripsi

Kehandalan suatu sistem diketahui melalui proses perhitungan nilai kecepatan waktu (detik) ukuran berkas dalam proses enkripsi/dekripsi menggunakan algoritme 3DES dan algoritme 4DES. Kurva distribusi /grafik antara berkas asli. Berkas terenkripsi/terdekripsi terdiri dari sumbu x untuk ukuran berkas (*Word, Excell*,Gambar) dengan skala 100 KB sampai 1100 KB dan sumbu y merupakan jumlah kecepatan waktu (detik) yang terjadi berkas asli dengan berkas terenkripsi/ berkas terdekripsi.

Distribusi nilai kecepatan waktu dari berkas asli/ awal dan berkas terenkripsi dibangkitkan /ditentukan berdasarkan eksperimen. Grafik yang bergaris warna merah dalam grafik distribusi merupakan nilai kecepatan waktu berkas terenkripsi dan berkas terdekripsi yang menggunakan algoritme 3DES, sedangan garis grafik yang berwarna hijau merupakan nilai kecepatan waktu berkas terenkripsi dan berkas terdekripsi yang mengggunakan algoritme 4DES. Garis sumbu x merupakan ukuran berkas dan garis sumbu y merupakan kecepatan waktu (detik).

Distribusi dalam penelitian ini dipentingkan nilai proses berkas terenkripsi 3DES dan nilai berkas terenkripsi 4DES yang artinya semakin lama kecepatan waktu proses yang dilakukan untuk berkas yang terenkripsi menggunakan 3DES/4DES semakin sulit juga waktu yang dibutuhkan untuk mengetahui isi berkas tersebut.

Untuk kecepatan waktu dalam proses berkas terenkripsi/terdekripsi pada jenis berkas (*Word, Excell*, Gambar) dan untuk satu jenis berkas yang sama tidak menghasilkan nilai kecepatan waktu yang berbeda karena jenis berkas tersebut sama-sama yang mengandung isi nilai bilangan binary 0 dan 1 yang kemudian komputer akan mengkonversian menjadi bilang string menggunakan kode ASCII.

Beda halnya bila ukuran berkas tersebut mempunyai ukuran yang berukuran berkas besar dan berukuran berkas kecil akan menghasilkan kecepatan waktu proses berkas terenkripsi/terdekripsi berbeda karena semakin besar ukuran berkas isi bit memiliki jumlah yang banyak dan membutuhkan waktu lama dalam proses dilakukan pengacakan bit dalam jumlah yang besar dan semakin kecil ukuran berkas isi binary memiliki jumlah yang sedikit sehingga saat proses pengacakan bit menghasilkan waktu kecepatan yang sangat cepat dalam proses enkripsi dan dekripsi.

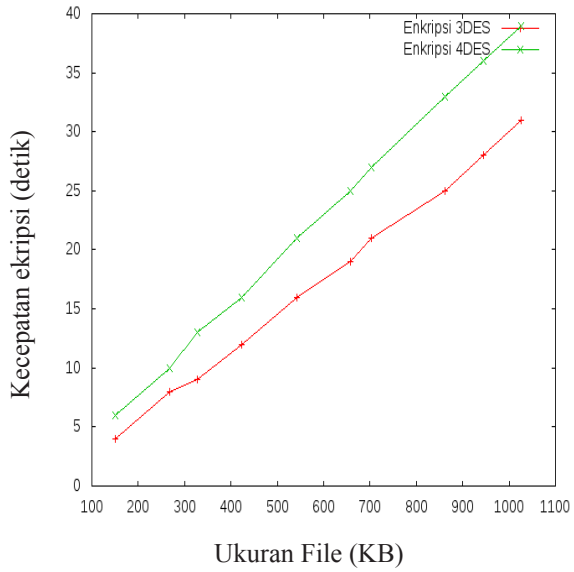
Selain itu, proses kecepatan waktu saat menggunakan berkas terenkripsi/terdekripsi menggunakan algoritme 3DES dan algoritme 4DES hasil yang didapat dan dibutuhkan sangat berbeda. Untuk proses berkas terenkripsi algoritme 3DES harus melalui pengacakan bit sebanyak 98 ronde sedangkan untuk proses berkas terenkripsi algoritme 4DES harus melalui pengacakan bit sebanyak 114 ronde.

Dari perbedaan pengacakan bit yang dimiliki oleh algoritme 3DES dan algoritme 4DES menghasilkan kecepatan waktu proses terenkirpsi/terdekripsi cepat menggunakan algoritme 3DES dari pada menggunakan algoritme 4DES lama kecepatan waktu yang digunakan. Tetapi, jika dilihat dari segi serangan yang datang dari penyerang mengambil isi kandung berkas tersebut.

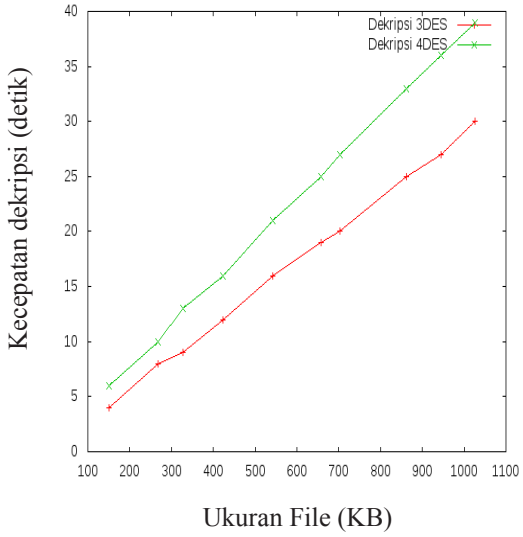
Penyerang membutuhkan kecepatan waktu yang berbeda bila berkas terenkripsi menggunakan algoritme 3DES waktu kecepatan yang dibutuhkan cepat dibandingkan berkas terenkripsi menggunakan algoritme 4DES waktu kecepatan yang dibutuhkan sangat lama untuk mengatur pengacakan bit yang tidak beraturan akibat dari proses berkas yang sudah terenkripsi menjadi pengacakan bit beraturan atau tersusun yang dapat dibaca/ dimengerti.

Terlihat pada Gambar 14 ,Gambar 15, Gambar 16, Gambar 17, Gambar 18 dan Gambar 19. Sampel Hasil proses waktu berkas terenkripsi/terdekripsi menggunakan algoritme 3DES dan algoritme 4DES dengan jenis berkas (*word,excell* dan gambar) dan ukuran berkas yang berbeda.

Selisih kecepatan waktu yang didapat untuk jenis



Gambar 14. Berkas Word enkripsi 3DES/4DES 12ab13CD



Gambar 15. Berkas Word Dekripsi 3DES/4DES 12ab13CD

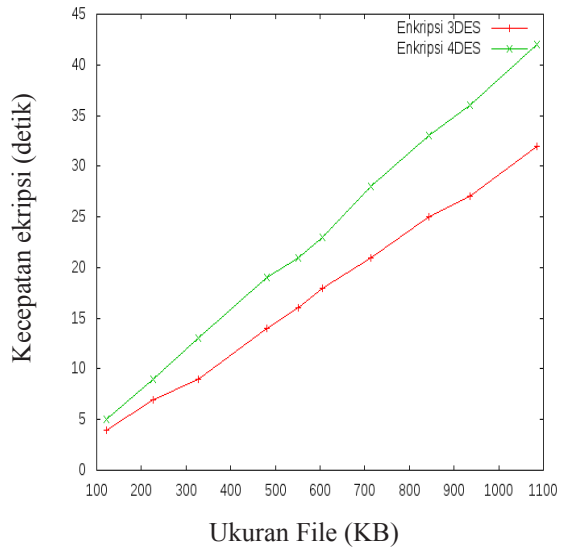
berkas *word, excell* dan gambar dan ukuran berkas 100 KB menggunakan proses enkripsi/dekripsi algoritme 3DES dan algoritme 4DES sebesar 1 detik sedangkan kecepatan waktu yang didapat untuk *word, excell* dan gambar ukuran berkas 1024 KB menggunakan proses enkripsi/dekripsi algoritme 3DES dan algoritme 4DES sebesar 1 detik.

F. Kekuatan Keamanan Brute Force

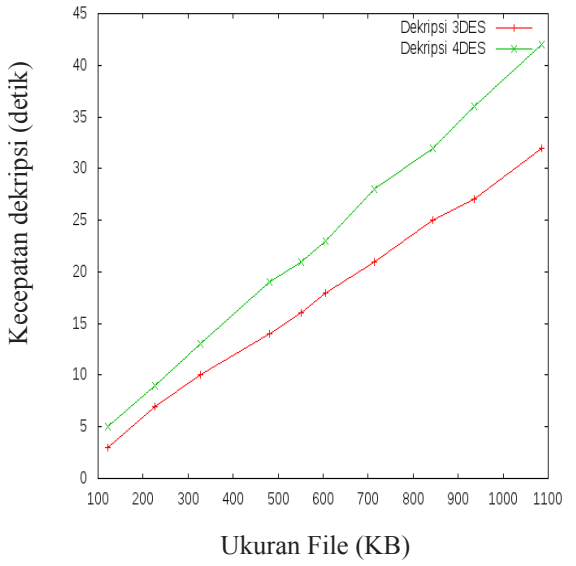
Brute force merupakan teknik yang mencoba untuk satu persatu kemungkinan kunci untuk mengetahui isi informasi (plaintext). Waktu yang diperlukan untuk mencoba kemungkinan kunci oleh serangan *brute force* [17].

Kecepatan *faster super computer* sekarang:

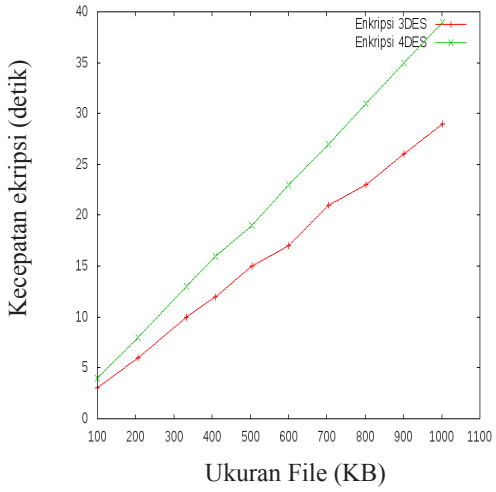
10.51 Pentaflops = 10.51 x 10^{15} *Floating point operations per second* (Flops) Jumlah Flops yang dibutuhkan untuk setiap kombinasi pengecekan: = 1000 Flops



Gambar 16. Berkas *Excel* Enkripsi 3DES/4DES 12ab13CD



Gambar 17. Berkas *Excel* dekripsi 3DES/4DES 12ab13CD



Gambar 18. Berkas Gambar Enkripsi 3DES/4DES 12ab13CD

Tabel 4. Waktu Memecahkan Kunci

Algoritme	Panjang Kunci (bits)	Waktu Serangan Tahun
3DES (K1≠K2≠K3)	192	1.89 x 10 37
4DES (K1≠K2≠K3≠K4)	256	3.45 x 1056

Jumlah kombinasi percobaan per detik
= (10.51 x 10^{15}) / 1000 = 10.51 x 10^{12}
Jumlah detik dalam 1 tahun
= 365 x 24 x 60 x 60 = 31536000

Jumlah untuk memecahkan 4DES dengan panjang kunci 256 bit
= (1.156 x 10 ^{77}) / (10.51 x 10^{12}) x 31536000
= (0.109 x 10^{65}) / 31536000
= 3.45 x 10^{56} tahun
Adapun waktu yang dibutuhkan untuk memecahkan panjang kunci ditunjukkan pada Tabel 4.

V. KESIMPULAN DAN SARAN

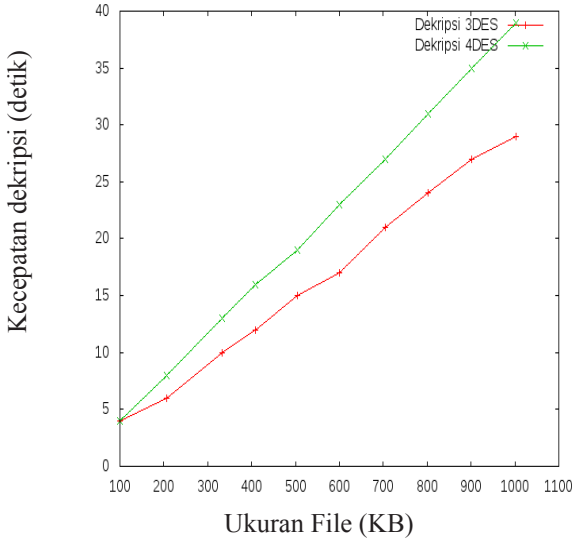
A. *Kesimpulan*

Adapun Kesimpulan dari penelitian ini yaitu :

1. Penelitian ini telah menghasilkan metode algoritme 4DES yang mempunyai 4 kunci yang masing-masing kunci mempunyai panjang kunci 64 bit sehingga total panjang 4 kunci 256 bit dan K1≠K2≠K3≠K4.
2. Hasil pengujian memperlihatkan algoritme 4DES mempunyai metode kerja yang dapat mengamankan berkas sensitif (berkas data rekam medis) dengan baik.
3. Untuk meminimalkan serangan dari penyerang proses enkripsi algoritme 4DES tambahkan padding minamal 1 byte dan makasimal 8 byte.
4. Hasil pengujian memperlihatkan proses enkripsi/ dekripsi 4DES dengan ukuran berkas 100-1024 KB hanya memiliki selisih waktu 1 detik dibandingkan dengan 3DES.
5. Algoritme 4DES memiliki keungulan dari segi keamanan berkas memiliki waktu 3.45 x10^{56} tahun lebih lama serangan *Brute Force* mengetahui teks berkas dan kunci rahasia yang digunakan.

B. *Saran*

Dalam penelitian ini masih hanya sebatas melakukan pengujian menggunakan algoritme 3DES dan algoritme 4DES dan berkas yang digunakan berkas rekam medis dengan jenis berkas word, excell dan gambar. Untuk selanjutnya disarankan bagi penelitian-penelitian lain dapat mengembangkan penggunaan algoritme diatas 4DES dan melakukan pengujian berkas yang berjenis lain.



Gambar 19. Berkas Gambar dekripsi 3DES/4DES 12ab13CD

REFERENSI

[1] C. Putra, B. Setiawan, R. P. Wibowo, "Implementasi Kriptografi untuk Pengamanan Data Sensitif Pada Aplikasi Rekam Medis". Tugas Akhir. 2011. Available: http://digilib.its.ac.id/implementasi-kriptograsi-untuk-pengamanan-data-sensitif-pada-aplikasi-rekam-medis 17478.html01/07/2011.

[2] V. Vathanophas, dan T. Pacharapha, "Information Technology Acceptance in healthcare service: The study of Electronic Medical Record (EMR) in Thailand", In Proc. Technology Management for Global Economic Growth (PICMET), 18-22 Juli 2010, pp.1-5.

[3] T. K. Patrick, "The data encryption standard thirty four years later: An overview", African Journal of Mathematics and Computer Science Research Vol. 3(10), pp. 267-269, October 2010.

[4] M. Zen Samsono Hadi, Nanang S, F. Nadziroh, Norma Ningsih. "Perbandingan Algoritma Enkripsi 3DES dan BlOWFISH Pada Aplikasi E-Hospital". The 15th Industrial Electronics Seminar (IES), Surabaya, 23 Oktober 2013.

[5] A. Hidayat, "Enkripsi Dan Dekripsi Data Dengan Algoritma 3DES (Triple Data Encryption Standard)". [online]. Available. http://repository.unpad.ac.id/2005/1/enkripsi_dan_dekripsi_data_dengan_algoritma_3_des.pdf

[6] Verma, O.P., Agrawal, R, Dafouti, D, Tyagi, S., Performance analysis of data encryption algorithms, In proceeding of 3rd International Conference on Electronics Computer Technology, Vol. 5, pp. 399-403, Kanyakumari, India, 8-10 April 2011.

[7] B.B. Narendra."Analisis Kelemahan Algoritma Cipher Blok DES dan Kekuatan Triple DES Sebagai Varian Pengganti DES". [online]. Available. http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2006-2007/Makalah1/Makalah1-080.pdf

[8] Rifki S. "Kriptografi untuk Keamanan Jaringan dan Implemetasi dalam Bahasa Java". Penerbit Andi. 2012.

[9] Stallings W. "Cryptography and Network Security: Principles and Practices, 2nd ed". Prentice Hall. 2011.

[10] Wahana Komputer. "Memahami Model Enkripsi & Security Data". Penerbit Andi. Yogyakarta. 2003.

[11] Z. Yingbing, dan L. Yongzhen, The design and implementation of a symmetric encryption algorithm based on DES, IEEE 5th International Conference on Software Engineering and Service Science, pp. 517 - 520, Beijing, 27-29 Juni 2014.

[12] Rasheed, I., Amin, A., Chaudhary, M., Bukhari, S., Rizwan, M, Ali, K., Analyzing the security techniques used in LTE Advanced and their evaluation, Eighth International Conference on Digital Information Management (ICDIM 2013), pp: 11 - 13, Islamabad, 10-12 September 2013.

[13] Wu, W., Jin, J., Cheng, J., The Research and Design of ATM PIN Pad Based on Triple DES, IEEE International Conference on Information and Automation, pp. 443 - 447, 6-8 Juni 2011.

[14] Emmy A.Br, Bangun, Gamaliel N. S. "Perbandingan Metode Modifikasi 3DES Dengan Metode 3DES". Jurnal Telematika. Vol. 7., No.11, Mei 2011. [online]. Available: http://journal.ithb.ac.id/index.php/telematika/article/view/52/50

[15] J. Pan, S. Li, Z. Xu, "Security mechanism for a wireless-sensor-network based healthcare monitoring system", IET Communications. Vol. 6, Issues: 18, 2012, pp. 3274-3280.

[16] G. Hu, "Study of file encryption and decryption system using security key", 2nd International Conference on Computer Engineering and Technology, Vol. 7, pp. V7-121 - V7-124, 16-18 April 2010.

[17] M. Arora. How Secure Is AES against brute force attack? Freescale Semiconductor. USA. [online]. Available. http://www.eetimes.com/document.asp?doc_id=1279619 Juli 2012.

Penerbit:
Jurusan Teknik Elektro, Fakultas Teknik, Universitas Syiah Kuala
Jl. Tgk. Syech Abdurrauf No. 7, Banda Aceh 23111
website: http://jurnal.unsyiah.ac.id/JRE
email: rekayasa.elektrika@unsyiah.net
Telp/Fax: (0651) 7554336