Algoritma DES untuk Keamanan Informasi pada Aplikasi Rekam Medis Elektronik

Yulino Sentosa- NIM : 13507046
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if17046@students.if.itb.ac.id

***Abstrak* — Sistem informasi rekam medis elektronik sudah banyak digunakan oleh rumah sakit maupun poliklinik. Aplikasi rekam medis elektronik harus memberikan jaminan kerahasiaan isi rekam medis pasien, sehingga hanya bisa dilihat dan diakses oleh pasien yang bersangkutan dan teknisi kesehatan yang berkepentingan. Untuk itu, diperlukan sebuah algoritma kriptografi untuk merahasiakan informasi yang mengandung nilai kerahasiaan di dalam rekam medis. Algoritma DES bisa diterapkan di dalam permasalahan ini, karena algoritma ini cukup kuat untuk merahasiakan informasi di dalam nya.**

Kata kunci : rekam medis, DES, enkripsi, dekripsi, kunci

I. PENDAHULUAN

Status hukum dan peraturan tentang catatan kesehatan harus dijaga oleh institusi pelayanan kesehatan. Institusi pelayanan kesehatan harus menyimpan catatan mengenai kesehatan karena hukum atau peraturan tersebut penting sebagai dokumen yang sah. Catatan kesehatan atau yang biasa disebut rekam medis tersebut minimal berisi tentang alamat pasien. Rekam medis (*medical record*) adalah data yang bersifat sangat pribadi dan menjadi salah satu informasi penting yang wajib menyertai seseorang kemanapun dia pergi. Kepemilikan informasi tersebut merupakan kepentingan dasar seseorang pasien dan tidak boleh dirahasiakan dari pasien oleh sebuah institusi kesehatan manapun, karena informasi tersebut adalah hak milik pasien. Namun data tersebut rahasia bagi orang lain yang tidak berhak. Rekam medis berisi tentang identitas data, ramalan penyakit, sejarah keluarga, tindakan yang dilakukan oleh tenaga kesehatan, laporan konsultasi, laporan laboratorium, prosedur operasi, laporan khusus, waktu tindakan, catatan perkembangan pasien, laporan asuhan perawatan, terapi, ringkasan pasien masuk, catatan untuk menemukan diagnosis akhir, komplikasi, prosedur pemeriksaan, dan tanda tangan kehadiran dokter.

Rekam medis merupakan tanda bukti rumah sakit terhadap segala upaya dalam penyembuhan pasien. Disamping itu rekam medis juga memiliki beberapa fungsi utama, diantaranya : sebagai alat komunikasi antar tenaga kesehatan (seperti: dokter, perawat, dan apoteker), sebagai dasar untuk merencanakan pengobatan atau perawatan, dan sebagai bukti tertulis atas segala tindakan pelayanan, perkembangan penyakit, dan pengobatan selama pasien dirawat

Sebagai dokumen yang sah yang dimiliki oleh rumah sakit, informasi di dalam rekam medis ada yang mengandung nilai kerahasiaan dan ada yang tidak mengandung nilai kerahasiaan. Informasi yang mengandung nilai kerahasiaan yaitu berupa laporan / catatan yang terdapat dalam berkas rekam medis sebagai hasil pemeriksaan, pengobatan, observasi, atau wawancara dengan pasien. Informasi ini tidak boleh disebarluaskan kepada pihak-pihak yang tidak berwenang karena menyangkut individu langsung si pasien. Sementara informasi yang tidak mengandung nilai kerahasiaan yaitu identitas pasien, seperti : nama dan alamat. Untuk beberapa kasus tertentu, identitas pasien tidak boleh disebarluaskan (untuk ketenangan dan keamanan rumah sakit), seperti : orang terpandang/pejabat, atas permintaan pasien, dan buronan.

II. SISTEM INFORMASI REKAM MEDIS ELEKTRONIK

Secara umum ada dua jenis rekam medis, yaitu : rekam medis kartu dan rekam medis elektronik. Sesuai dengan perkembangan teknologi, maka diterapkan suatu bentuk rekam medis berbasis komputer (elektronik) untuk mengatasi kekurangan-kekurangan pada rekam medis kartu, diantaranya : sulit menemukan data, fragmentasi : jika masing-masing unit atau instalasi menyimpan rekam medis berbeda untuk orang yang sama, untuk mengirimkan informasi data perlu disalin, dan bisa mengintegrasikan sistem pendukung keputusan klinik dengan informasi pasien yang telah dikumpulkan.

Dengan adanya penyimpanan berkas rekam medis yang terkomputerisasi ini, menjadikan rekam medis tersebut mudah dan cepat diolah menjadi informasi dalam bentuk laporan-laporan maupun statistik perkembangan pelayanan kesehatan maupun statistik penyakit. Selain itu manfaat lainnya adalah : kemudahan penelusuran dan pengiriman informasi, penyimpanan lebih ringkas, integritas data serta kualitas data dan standar dapat dikendalikan.

Sistem informasi rekam medis elektronik adalah sistem penyimpanan informasi secara elektronik mengenai status kesehatan serta pelayanan kesehatan, yang diperoleh pasien sepanjang hidupnya dan tersimpan sedemikian hingga dapat melayani berbagai pengguna rekam yang sah (Shortlife, 2001).

Sistem informasi rekam medis elektronik kini telah banyak diterapkan oleh rumah sakit-rumah sakit yang ada di Indonesia sebab telah terbukti memberi kemudahan pada petugas pelayanan kesehatan, sehingga mempercepat proses yang akan diperlukan bagi pihak rumah sakit maupun bagi pihak pasien tersebut. Sistem informasi rekam medis elektronik pada era saat ini sangat membantu kinerja petugas pelayanan kesehatan karena memberi kemudahan-kemudahan dalam mendata segala sesuatu tentang pasien untuk dibutuhkan dengan cara yang tepat. Akan tetapi dalam pengoperasiannya, sistem informasi rekam medis elketronik membutuhkan biaya yang tidak sedikit dan diperlukan sistem jaringan keamanan yang kuat.

Dengan aplikasi rekam medis elektronik yang ada sekarang memungkinkan untuk ditambahkan unsur keamanan informasi. Unsur keaman informasi ditambahkan dengan menerapkan algoritma kriptografi kepada data atau informasi pasien terutama terhadap data yang mengadung nilai kerahasiaan dan tidak boleh disebarluaskan seperti yang telah dijelaskan sebelumnya.

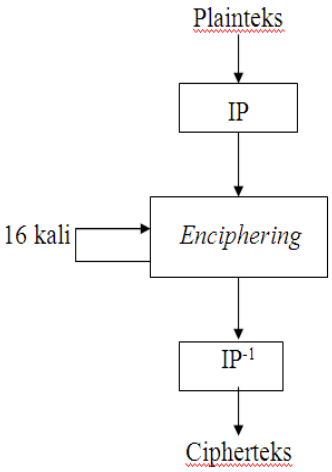
III. ALGORITMA DES

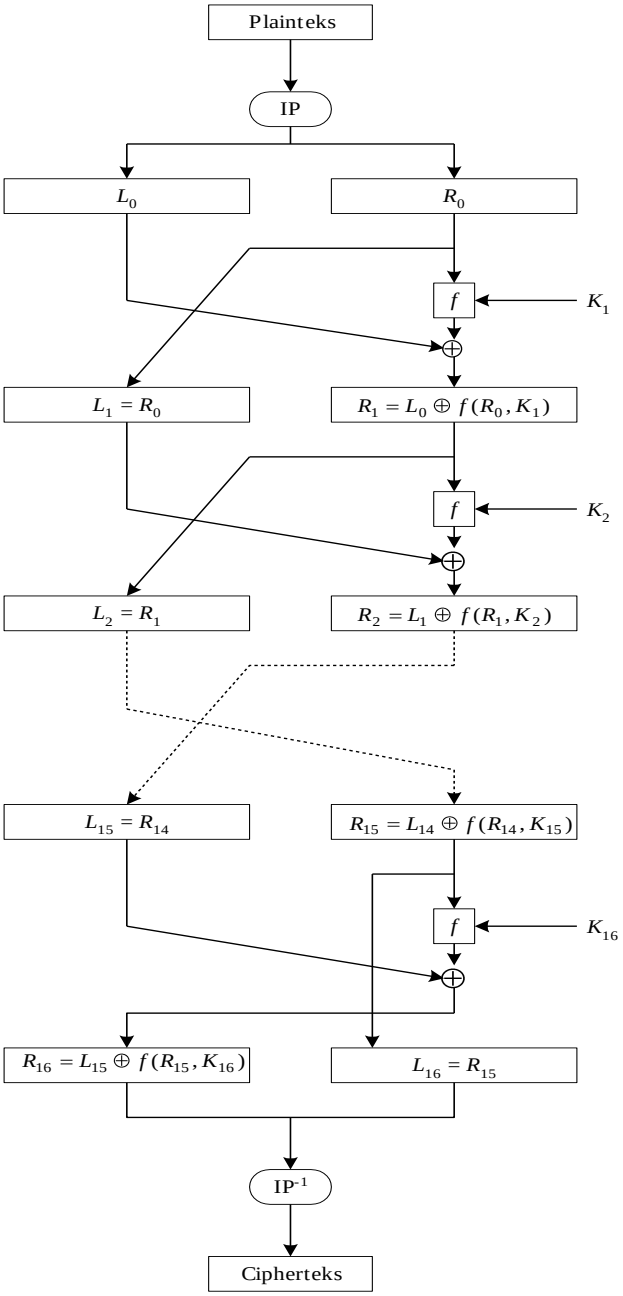
Algoritma DES (*Data Encryption Standard*) dapat diterapkan pada aplikasi sistem informasi rekam medis elektronik karena algoritma ini telah disetujui oleh *National Bureau of Standard* (NBS) setelah penilaian kekauatannya oleh *National Security Agency* (NSA) Amerika Serikat. DES termasuk ke dalam algoritma kriptografi simetri dan tergolong jenis *cipher block*.

DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (*internal key*) atau upa-kunci (*subkey*). Kunci internal dibangkitkan dari kunci eksternal (*external key*) yang panjangnya 64 bit.

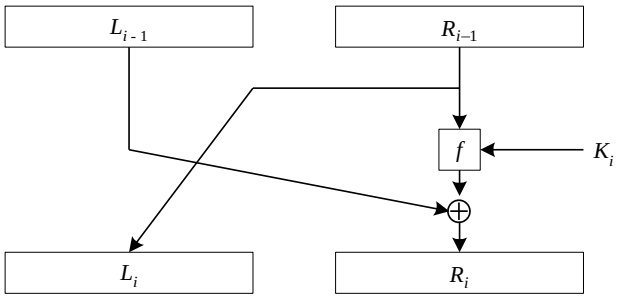
Skema global dari algoritma DES adalah sebagai berikut :

1. Blok plainteks dipermutasi dengan matriks permutasi awal (*initial permutation* atau IP).
2. Hasi permutasi awal kemudian di-*enciphering* sebanyak 16 kali (putaran). Setiap putaran menggunakan kunci internal yang berbeda.
3. Hasil enciphering kemudian dipermutasi dengan dengan matriks permutasi balikan (*invers initial permutation*) menjadi blok cipherteks.





Untuk menambah kerumitan dari algoritma DES, bisa ditambahkan jaringan Feistel. Setiap putaran pada DES merupakan jaringan Fesitel



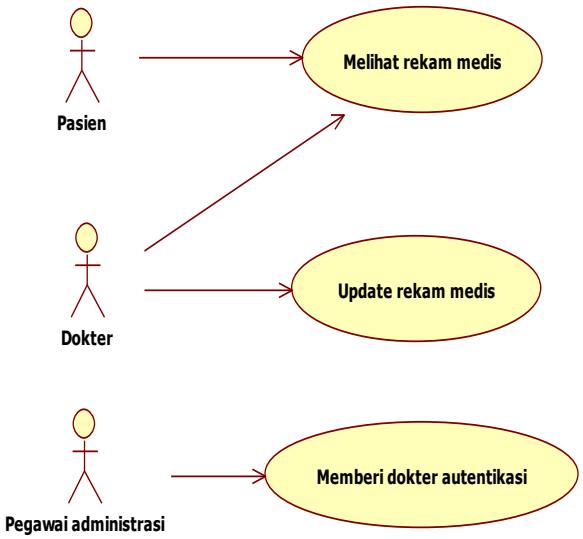
Karena ada 16 putaran, maka dibutuhkan kunci sebanyak 16 buah, yaitu : K1,K2,..K16. Kunci-kunci internal ini dapat dibangkitkan sebelum proses enkripsi atau bersamaan dengan proses enkripsi. Kunci internal dibangkitkan dari kunci eksternal (64 bit /8 karakter), yang dalam kasus aplikasi sistem informasi rekam medis elektronik merupakan password yang dimiliki oleh pasien.

III. PERANCANGAN APLIKASI

Secara umum ada lima pihak utama yang ada di rumah sakit atau poliklinik, yaitu : pasien, pegawai administrasi, dokter, perawat, dan apoteker. Pada beberapa rumah sakit atau poliklinik juga terdapat laboratorium kesehatan. Akan tetapi yang terlibat di dalam sistem informasi rekam medis untuk mengimplementasikan algoritma DES adalah : pasien, dokter, dan pegawai administrasi. Untuk mengimplementasikan algoritma DES pada sistem informasi rekam medis elektronik, perlu diperhatikan hak akses dari masing-masing pihak tersebut terhadap informasi rekam medis pasien.
Berikut adalah penjelasan hak akses dari masing-masing pihak yang terlibat dalam sistem informasi rekam medis:

1. Pasien. Pasien berhak untuk melihat atau mengetahui tindakan yang dilakukan oleh teknisi kesehatan di rumah sakit, seperti : pemeriksaan yang dilakukan, obat dan perawatan yang diberikan, dsb pada tanggal tertentu.
2. Pegawai administrasi. Pegawai administrasi bertugas untuk pengelolaan data pasien dan merujuk pasien ke dokter tertentu.
3. Dokter. Dokter yang dirujuk melalui pegawai administrasi bisa melihat riwayat (*history*) kesehatan atau pemeriksaan pasien yang dilakukan sebelumnya. Setelah melakukan pemeriksaan, dokter berkewajiban untuk mengisi rekam medis pasien dengan jenis perawatan, pemeriksaan, dan obat yang diberikan. Selain itu dokter juga mengisi hasil cek laboratorium pasien yang didapatkan dari pegawai laboratorium.

Berikut adalah *use case diagram* dari penggunaan aplikasi rekam medis elektronik :



Cara kerja dari penerapan algoritma DES pada sistem informasi rekam medis elektronik dapat dijelaskan sebagai berikut :

1. Masing-masing pasien memiliki password untuk melakukan log in ke dalam sistem informasi rekam medis yang telah terdaftar sebelumnya di basis data administrasi. Password ini sekaligus sebagai kunci dalam melakukan enkripsi maupun dekripsi. Dengan password ini, pasien dapat melihat hasil rekam medis melalui proses dekripsi.
2. Pegawai administrasi. Pegawai administrasi memberikan hak akses kunci eksternal kepada dokter.
3. Dokter. Di sisi dokter kunci yang diterima akan diproses dan menghasilkan 16 kunci internal (K1,K2...K16). Dengan menggunakan kunci ini, proses enkripsi rekam medis dilakukan. Hasil dari pemeriksaan yang sudah terenkripsi ini akan masuk ke dalam basis data pasien dan pasien bisa melihatnya dengan melakukan proses dekripsi dengan password yang dimilikinya.

Berdasarkan metoda (cara) ini, proses enkripsi dilakukan oleh dokter dan proses dekripsi dilakukan oleh pasien melalui aplikasi yang ada. Dokter mengenkripsi hasil pemeriksaan menjadi hasil pemeriksaan yang terenkripsi, sementara pasien mendekripsi hasil pemeriksaan yang terenkripsi menjadi hasil pemeriksaan (rekam medis).

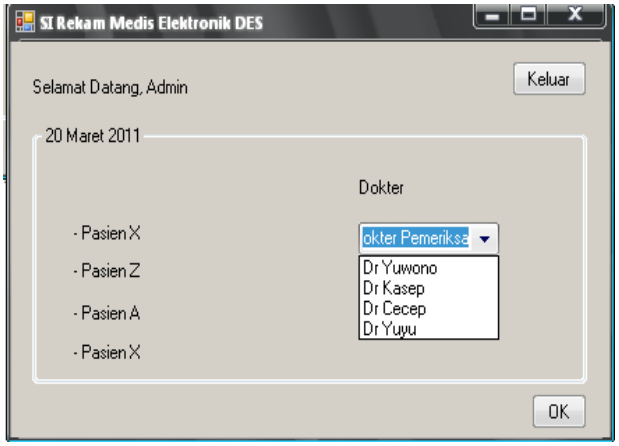
Untuk mempermudah pamahaman mengenai cara kerja algoritma DES pada rekam medis elektronik, berikut adalah rancangan tampilan (*interface*) dari aplikasi sistem

informasi rekam medis elektronik yang menerapakan algoritma kriptografi DES :

1. Tampilan (*User Interface*) untuk pasien

Jika tombol (*button*) Lihat diklik oleh pasien, maka sistem akan otomatis melakukan dekripsi dengan algoritma DES. Berikut contoh hasil yang ditampilkan :

2. Tampilan (*User Interface*) untuk pegawai administrasi



Pegawai administrasi memilih dokter yang akan menangani masing-masing pasien. Dokter yang dipilih akan mendapatkan kunci eksternal atau password dari pasien untuk melakukan enkripsi rekam medis.

3. Tampilan (*User Interface*) untuk dokter

Untuk menjaga informasi kerahasiaan password pasien, password yang didapatkan oleh dokter dari basis data pasien melalui persetujuan pegawai administrasi dalam bentuk karakter-karakter asterix. Berikut contoh tampilan (interface) dokter menerima password dari pasien :

Jika Dokter meng-klik Edit rekam medis, makadokter melakukan pengeditan terhadap rekam medis pasien yang telah ada sebelumnya dengan meng-copy kunci yang telah didapat.

Jika Dokter mengklik enkripsi, maka sistem akan melakukan enkripsi dan menyimpan hasil enkripsi tersebut ke dalam basis data. Informasi ini akan tersimpan dalam *record* pasien yang bersangkutan pada tanggal tertentu dan pasien bisa mengaksesnya.

Aplikasi rekam medis elektronik, selain menyimpan data teks berupa hasil pemeriksaan, juga harus dapat menyimpan informasi lainnya, seperti : gambar (komputer grafik, gambar yang di-scan), hasil foto rontgen digital, suara (suara jantung, suara paru), dan video (proses operasi).

Semua jenis informasi pasien tersebut harus data dirahasiakan. Berikut adalah contoh hasil rontgen pasien (rontgen.jpg) :

Hasil gambar yang telah dienkripsi tidak akan bisa dibuka karena header dari file juga akan terenkripsi. Hal ini akan sangat menguntungkan karena file gambar akan bisa dilihat oleh pasien dan dokter saja. Berikut adalah contoh file hasil rontgen yang telah didekripsi kembali dengan menggunakan aplikasi DES sederhana oleh pasien (rontgen1.jpg) :

Berdasarkan pemaparan dan contoh tampilan (*interface*) di atas, terlihat bahwa syarat utama dari penggunaan aplikasi ini adalah tersedianya jaringan internet yang memadai di rumah sakit atau poliklinik. Jaringan internet bisa menggunakan LAN yang meungkinkan dokter dan pegawai terhubung di dalamnya. Sementara pasien, dengan aplikasi ini bisa mengakses informasi rekam medis nya dimanapun dia berada, jika perancangan aplikasi rekam medis elektronik ini dengan menggunakan prinisip *web based*.

IV. KESIMPULAN

Penerapan atau pengimplementasian algoritma DES untuk kerahasiaan isi dari rekam medis pada aplikasi rekam medis elektronik membantu instansi kesehatan untuk merahasiakan informasi pasiennya. Dengan algoritma enkripsi dan dekripsi yang rumit, dapat menghindari pihak-pihak tertentu untuk mencoba mengakses informasi rahasia dari pasien. Akan tetapi untuk mengimplementasian sistem informasi rekam medis yang dilengkapi algoritma DES ini, di rumah sakit atau poliklinik harus tersedia akses internet yang bagus, agar dapat terhubung antara instansi kesehatan dan proses *update* rekam medis pasien juga bisa dilakukan dengan *real time*. Algoritma DES bisa diterapkan pada berbagai Informasi rekam medis, sepeti : file teks, file gambar, file suara, dan file video.

V. REFERENSI

[1] Aspek hukum rekam medis (http://yoyoke.web.ugm.ac.id/download/aspekhukumrekammedis.pdf), diakses 22 Maret 2011 pukul 23.00

[2] Sistem informasi rekam medis (http://sundari-sisteminformasirekammedis.blogspot.com/2009/02/rekam-medis-elektronik.html), diakses 22 Maret 2011 pukul 23.00

[3] Patah sendi tulang tangan (http://priyadi.net/archives/2007/08/21/patah-sendi-tulang-tangan/), diakses 23 Maret 2011 pukul 10.00

[4] Asmaripa Ainy. Rekam Medik & sistem pelaporan rumah sakit. FKM Unsri

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 29 April 2010

Yulino Sentosa
13507046