PERANCANGAN PROGRAM APLIKASI KRIPTOGRAFI MENGGUNAKAN ALGORITMA MAGENTA DENGAN PANJANG KUNCI 128 BIT

Steffie Hugh Wibisono[1]; Djunaidy Santoso[2]

[1, 2] Jurusan Teknik Informatika, Fakultas Teknologi Informasi, Universitas Tarumanagara
Jln. S. Parman No. 1, Jakarta Barat 11440
djunaidys0533@binus.ac.id, djunsan2002@yahoo.com

ABSTRACT

Along with the development of computer technology, the growing crimes against the computer. Crimes against the computer makes people increasingly competing to make the algorithms-algorithms that can maintain the confidentiality of data. Algorithms algorithm Magenta is one of the many algorithms that exist today. Magenta algorithms have been developed since 1990 by using a simple and transparent technique that can be implemented in hardware and software. First time algorithms are analyzed using the butterfly structure - the structure of the butterfly which was then replaced by a Fast Hadamard Transform (FHT) shuffle structure which has the advantage of providing some structure in each level. In 1994 there was a slight change in the use of hardware that was not processed according to plan so that now the algorithm used by Deutsche Telekom Magenta for secure management of sensitive data with 128-bit key length. These algorithms break the 128-bit key length into 16 blocks with each block containing the 8-bit and one other advantage of this algorithm is the recursive part is calculated repeatedly at each iteration.

Keywords: *128-bit key length, cryptography, algorithms magenta*

ABSTRAK

Seiring dengan perkembangan teknologi komputer, kejahatan terhadap komputer semakin berkembang. Kejahatan terhadap komputer ini membuat orang semakin berlomba untuk membuat algortima–algortima yang dapat menjaga kerahasiaan suatu data. Algortima Magenta adalah salah satu algortima dari sekian banyak algoritma yang ada saat ini. Algortima Magenta ini telah dikembangkan sejak tahun 1990 dengan menggunakan teknik sederhana dan transparan yang dapat diimplementasikan dalam hardware dan software. Pertama kali algortima ini dianalisa menggunakan struktur kupu – kupu yang kemudian struktur tersebut diganti dengan Fast Hadamard Transform (FHT) shuffle structure yang memiliki keunggulan dalam memberikan struktur pada setiap tingkatannya. Pada tahun 1994 terjadi sedikit perubahan dalam penggunaan hardware yang tidak diproses sesuai rencana sehingga sekarang algoritma Magenta digunakan oleh Deutsche Telekom untuk mengamankan manajemen data yang sensitif dengan panjang kunci 128 bit. Algortima ini memecah kunci dengan panjang 128 bit menjadi 16 blok dengan masing–masing blok berisi dengan 8 bit dan salah satu keunggulan lain dari algoritma ini adalah bagian rekursifnya yang dihitung secara berulang–ulang pada setiap iterasi.

Kata kunci: *panjang kunci 128 bit, kriptografi, algoritma magenta*

PENDAHULUAN

Latar Belakang Masalah

Pesatnya perkembangan dunia komputer dan komunikasi saat ini telah menciptakan suatu jaringan komputer yang sangat luas dan besar ukurannya. Jaringan ini dijadikan sarana untuk menyebarkan informasi tanpa mengenal adanya batasan hukum, waktu, dan jarak, maka dari itu tindak kejahatan terhadap komputer juga semakin meningkat. Hal ini mengakibatkan adanya suatu keresahan karena data penting yang kita miliki menjadi tidak aman dan dapat disadap oleh orang lain. Untuk menghindari terjadinya tindak kejahatan komputer ini, maka diperlukan suatu sekuriti terhadap perangkat keras maupun perangkat lunak. Sekuriti komputer meliputi tiga karakter, yaitu kerahasiaan (*secrecy*), integritas (*integrity*) dan ketersediaan (*availability*). Perancangan sekuriti ini lebih difokuskan pada perangkat lunak menggunakan algortima Magenta dengan panjang kunci 128 bit.

Rumusan Rancangan

Berdasarkan latar belakang masalah di atas, maka akan dirancang suatu program enkripsi dan dekripsi yang berguna untuk keamanan data pada komputer si suatu jaringan. Algoritma Magenta ini menggunakan symmetric *key* dan panjang kunci 128 bit.

Komponen Rancangan

Unit-unit yang akan digunakan diantaranya unit text editor yang didalamnya terdapat sebuah text field dan beberapa menu item. Unit yang kedua adalah unit enkripsi dan dekripsi, di mana dalam unit ini terdapat tombol *set key*, tombol *encrypt*, dan tombol *decrypt*.

Spesifikasi Rancangan

Spesifikasi dari rancangan ini adalah: pertama, unit text editor. Program aplikasi ini memiliki text editor yang *built-in* (telah disediakan bersama dengan program aplikasi tersebut), artinya user dapat langsung memasukkan text yang diinginkan tanpa harus membuka *text editor* yang baru; kedua, unit enkripsi dan dekripsi. Unit enkripsi dan dekripsi ini menggunakan algoritma Magenta dengan metode operasi *Electronic Code Book* (ECB). Untuk *key*-nya digunakan *symmetric key*, artinya *key* pengirim dan *key* penerima pesan harus sama. Bahasa pemrograman yang digunakan adalah Visual Basic 6.0. Teks yang ingin dienkripsi adalah teks biasa (karakter ASCII); ketiga, unit pengiriman dan penerimaan file dalam jaringan. Sistem pengiriman dan penerimaan file ini hanya bias dilakukan di dalam Local Area Network (LAN).

Kegunaan Rancangan

Perancangan ini dapat digunakan oleh bank-bank atau perusahaan-perusahaan yang membutuhkan banyak pengamanan ekstra terhadap data dan distribusi melalui jaringan, contoh yang biasa digunakan adalah penggunaan PIN. Hasil dari rancangan ini diharapkan dapat memberikan suatu sekuriti yang lebih baik pada LAN untuk menjamin keamanan serta menghindari terjadinya tindak kejahatan komputer.

Studi Pustaka

Sistem yang Dirancang

Seperti yang telah dijelaskan dalam latar belakang masalah, untuk menghindari terjadinya tindak kejahatan komputer seperti pencurian, sabotase atau pengrusakan data, maka diperlukan suatu sekuriti komputer agar data yang ada pada komputer lebih aman. Pada suatu system komputer

terdapat empat macam kegagalan, yaitu: pertama, interupsi. Interupsi dalam sekuriti komputer mempunyai arti suatu aset dari system hilang, tidak tersedia atau tidak berguna; kedua, pencegatan. Pencegatan berarti ada pihak yang tidak berkepentingan yang berhasil mengakses suatu aset; ketiga, modifikasi. Modifikasi berarti ada sekelompok orang yang tidak berkepentingan, yang mengadakan perubahan atau modifikasi pada suatu aset; keempat, fabrikasi. Fabrikasi mempunyai arti sekelompok orang yang tidak berkepentingan berhasil menambahkan sesuatu ke dalam suatu aset sehingga sistem menjadi kacau.

Sekuriti dalam Jaringan Komputer

Jaringan komputer adalah kumpulan komputer-komputer yang saling terhubung yang dapat bertukar informasi. Tujuan dari penggunaan jaringan komputer salah satunya adalah untuk mendapatkan reliabilitas yang tinggi dengan memiliki sumber-sumber alternatif persediaan. Sekuriti komputer adalah istilah umum dari pengumpulan alat-alat yang dirancang untuk melindungi data dan menghalanginya dari hacker (pencuri atau pelaku tindak kejahatan komputer)

Kriptografi

Ada tiga istilah yang berkaitan dengan proteksi data, yaitu kriptografi, kriptologi, dan kriptanalisis. Di mana ketiganya memiliki arti yang kurang lebih sama. Kriptografi merupakan seni untuk menyembunyikan informasi dari sebuah pesan sehingga pesan itu terlihat tidak memiliki arti. Kriptologi adalah ilmu yang mempelajari tentang komunikasi pada jalur yang tidak aman beserta masalah-masalah yang berhubungan dengan itu. Kriptanalisis adalah orang yang memecahkan sistem tersebut.

Enkripsi dan Dekripsi

Enkripsi adalah suatu upaya agar data yang rahasia tidak bergantung atau terganggu pada lingkungan yang tidak aman atau suatu proses untuk menyandikan suatu pesan sehingga pesan tersebut tidak nyata. Sedangkan dekripsi adalah proses kebalikan dari enkripsi. Cryptosystem adalah sistem yang mengatur atau melakukan enkripsi dan dekripsi.

Algoritma Magenta

Perancangan algoritma Magenta (Multifunctional Algorithm for General-purpose Encryption and Network Telecommunication) dimulai pada tahun 1990. Pada bulan Agustus 1998 algoritma ini dikembangkan oleh Michael Jacobson Jr., Klaus Huber. Proses perancangan aplikasi program kriptografi ini akan menggunakan algoritma Magenta dengan panjang kunci 128-bit. Input yang dimasukkan berupa *plaintext* dengan panjang 128-bit dan *ciphertext* yang dihasilkan juga memiliki panjang yang sama, yaitu 128-bit.

Fungsi-fungsi dalam Algoritma Magenta

$f(x) = \alpha^x \quad x \neq 255$
$0 \quad x=255$
$A(x,y) = f(x \oplus f(y))$
$PE(x,y) = (A(x,y), A(y,x)) = (f(x \oplus f\ y)), f(y \oplus f(x))$
$T(x_0, ..., x_{15}) = \Pi(\Pi(\Pi(\Pi(x_0, ..., x_{15}))))$
$\Pi(x_0, ..., x_{15}) = (PE(x_0, x_8), PE(x_1, x_9), ..., PE(x_7, x_{15}))$
$C^{(j+1)}(x_0, ..., x_{15}) = T((x_0, ..., x_7) \oplus C_e^{(j)}, (x_8, ..., x_{15}) \oplus C_o^{(j)}))$
$E^{(r)}(x_0, ..., x_{15}) = C_e^{(r)}$
$F_y(x) = ((x_8, ..., x_{15}), (x_0, ..., x_7) \oplus E^{(3)}(x_8, ..., x_{15}), (y_0, ..., y_7)$
$Enc_K(M) = F_{K1}(F_{K1}(F_{K2}(F_{K2}(F_{K1}(F_{K1}(M))))))$
$Enc_K(M) = V(Enc_K(V(M)))$

Keterangan fungsi algoritma di atas adalah sebagai berikut.

f(x) : fungsi untuk mencari nilai (x) di dalam S-box.
A : variabel bebas untuk menjalankan proses penghitungan dan pencarian nilai *plaintext* dari dalam S-box.
PE : *Portable Execution*, tempat untuk mengeksekusi *plaintext*.
T : variabel bebas untuk menerima hasil iterasi Π.
Π : variabel bebas yang melakukan iterasi untuk mengacak *plaintext.*
C : *ciphertext* yang dihasilkan.
C_e : *ciphertext index even* (genap).
C_o : *ciphertext index odd* (ganjil).
E : *encryption.*
$F_y(x)$: Fungsi Feistel, dengan y digantikan *key* (K_1 atau K_2), dan x digantikan dengan *plaintext* (M).
Enc_K : fungsi untuk melakukan enkripsi.
Dec_K : fungsi untuk melakukan dekripsi.
M : *plaintext.*
V : variabel bebas untuk membalik *plaintext*, hasil *encrypt* atau hasil *decrypt*.
K_1 : 8 byte *key* pertama.
K_2 : 8 byte *key* kedua.
r : *rounds*.
⊕ : fungsi Xor.
X : *byte plaintext*.
Y : *byte key*.

METODE PENELITIAN

Proses Enkripsi Algoritma Magenta

Pengerjaan proses enkripsi dengan algoritma Magenta, perhitungannya dilakukan mundur mulai dari *point* 9, *point* 8 sampai dengan *point* 1. Berikut ini merupakan penjelasan cara kerja perhitungan enkripsi algoritma Magenta.

Pertama, proses enkripsi pada algoritma Magenta dimulai dengan memasukkan plaintext (M) yang di pecah menjadi 16 *byte* ($X_0, X_1, \ldots, X_{15}$), ke dalam fungsi:

$Enc_K\ (M) = F_{K1}(\ F_{K1}(\ F_{K2}(\ F_{K2}(\ F_{K1}(\ F_{K1}(\ M\ ))))))$; dan memasukkan *key* sebesar 16 *byte* ($Y_0, Y_1, \ldots, Y_{16}$), yang kemudian dipecah menjadi 2 *key* (K_1, K_2), di mana K_1 adalah 8 *byte* pertama dari *key* ($Y_0 \ldots Y_7$) dan K_2 terdiri dari 8 *byte key* kedua ($Y_8 \ldots Y_{15}$).

Kedua, setelah diketahui plaintext dan *key* yang akan digunakan, maka *plaintext* dan *key* tersebut dimasukkan ke dalam fungsi:

$F_y(x) = ((x_8, \ldots, x_{15}), (x_0, \ldots, x_7) \oplus E^{(3)}\ (x_8, \ldots, x_{15}), (y_0, \ldots, y_7))$. Dengan *Plaintext* ($X_0, X_1, \ldots, X_{15}$) dimasukkan ke dalam fungsi Fy(x) dengan penempatan yang dibalik $((x_8, \ldots, x_{15}), (x_0, \ldots, x_7))$, kemudian *plaintext* tersebut di ⊕ (XOR) dengan 8 byte plaintext yang kedua dan 8 byte *key* yang pertama, $(E^{(3)}\ (x_8, \ldots, x_{15}), (y_0, \ldots, y_7))$.

Ketiga, untuk mencari $E^{(3)}$, maka digunakan fungsi $C_e^{(r)}$ dengan r sebanyak tiga kali, di mana $(E^{(3)}\ (x_8, \ldots, x_{15}), (y_0, \ldots, y_7))$ akan dianggap sebagai:
$E^{(r)}\ (\ x_0, \ldots, x_{15}) = C_e^{(r)}$.

Keempat, penjabaran fungsi untuk mencari $C_e^{(r)}$ dengan r = 3, adalah:

$Ce^{(r)} = C^{(j+1)}(X_0 \ldots X_{15}) = T((X_0 \ldots X_7) \oplus Ce^{(j)}, (X_8 \ldots X_{15}) \oplus Co^{(j)})$, dengan:
$C^{(3)}$ didapat dari $C^{(2+1)} = T(X_0 \ldots X_7) \oplus Ce^{(2)}, (X_8 \ldots X_{15}) \oplus Co^{(2)})$,
$C^{(2)}$ didapat dari $C^{(1+1)} = T(X_0 \ldots X_7) \oplus Ce^{(1)}, (X_8 \ldots X_{15}) \oplus Co^{(1)})$,
$C^{(1)}$ didapat dari $C^{(0+1)} = T(X_0 \ldots X_7) \oplus Ce^{(0)}, (X_8 \ldots X_{15}) \oplus Co^{(0)})$.
(Ce adalah *ciphertext* dengan *index even*, $X_e = (x_0, x_2, ..., x_{14})$ sedangkan Co adalah *ciphertext* dengan *index odd*, $X_o = (x_1, x_3, ..., x_{15})$).

Kelima, untuk menghitung fungsi di atas, T yang belum diketahui, dicari dengan menggunakan fungsi $T(x_0, ..., x_{15}) = \Pi (\Pi (\Pi (x_0, ..., x_{15}))))$.

Keenam, untuk masing-masing $\Pi (x_0, ..., x_{15})$, pengerjaannya menggunakan fungsi $\Pi (x_0, ..., x_{15}) = (PE(x_0, x_8), PE(x_1, x_9), ..., PE(x_7, x_{15}))$.

Ketujuh, fungsi PE(x,y) di dapat dari penjabaran fungsi:
$PE(x,y) = (A (x,y), A (y,x)) = (f (x \oplus f\ y)), f (y \oplus f (x))$

Kedelapan. dengan penjabaran fungsi $A (x,y) = f (x \oplus f (y))$. Kesembilan. nilai f(x) sendiri dapat diperoleh dari S-box (256):
$f(x) = \alpha^x \quad x \neq 255$
$0 \quad x=255$

Proses Dekripsi Algoritma Magenta

Untuk proses dekripsi, *key* (K) yang akan digunakan sama dengan *key* yang digunakan dalam proses enkripsi. Dimulai dengan menggunakan fungsi:

$Dec_K (M) = V (Enc_K (V(M))$
di mana $V(X_0 \ldots X_{15}) = (X_8, X_9, \ldots, X_{15}, X_0, X_1, \ldots, X_7)$
yang kemudian dilanjutkan kembali dengan menjalankan fungsi enkripsi seperti di atas sehingga akhirnya didapatkan hasil deskripsi.

Rancangan Sistem

Perancangan program Magenta yang bekerja di dalam jaringan ini secara umum ditujukan kepada semua orang yang memerlukan peningkatan sekuriti dan kepercayaan di dalam pengiriman data antar komputer di dalam suatu jaringan. Perancangan program aplikasi ini menggunakan bahasa pemrograman Visual Basic 6.0 yang bisa bekerja di dalam *platform* Windows 98/98SE, Windows ME, Windows 2000, bahkan Windows XP.

Prosedur Pembuatan Program Aplikasi

Langkah-langkah pembuatan program Magenta yang bekerja dalam jaringan ini adalah sebagai berikut. Pertama, mempersiapkan dan melakukan instalasi perangkat keras komputer berupa 2 buah komputer yang terhubung dengan jaringan *Peer to Peer* degan spesifikasinya, yaitu prosesor Intel Pentium IV 2 GHz dan Prosesor Intel Pentium 3 850MHz, harddisk 40 GB dan 20 GB, memori DDR PC 2700 256 MB dan SDRAM PC 133 256 MB, dua monitor 15", dua mouse standar, dua *keyboard* standar, dua kartu jaringan LANPRO 10/100, dan kabel UTP yang terpasang pada konektor RJ-42 sepanjang 5m. Kedua, mempersiapkan dan melakukan instalasi perangkat lunak pada kedua komputer sebagai berikut: sistem operasi Windows XP Professional dan program aplikasi Microsoft Visual Basic 6.0 Enterprise Edition.

Proses Pembuatan Program Aplikasi

Proses pembuatan program aplikasi Magenta yang bekerja di dalam jaringan ini dilakukan setelah selesai mempersiapkan perangkat keras dan lunak. Langkah-langkah proses pembuatannya, yaitu mengumpulkan materi-materi yang dibutuhkan, melakukan pembatasan materi dari hasil pengumpulan materi, membuat alur program dengan *State Transition Diagram*, melakukan coding dengan menggunakan Microsoft Visual Basic 6.0 Enterprise Edition, membuat dokumennya serta membuat program kriptografi dengan algoritma Magenta

HASIL DAN PEMBAHASAN

Cara dan Hasil Pengujian

Cara pengujian perancangan program aplikasi ini menggunakan metode black-box, yaitu program diberikan sejumlah input dan kemudian outputnya dibandingkan, apakah telah sesuai dengan spesifikasi rancangannya. Pengujian perancangan program aplikasi kriptografi menggunakan algoritma Magenta ini dilakukan pada form-form yang terdapat pada program. Dengan menggunakan Algoritma Magenta dengan kunci bit 128 akan semakin cepat dan aman dalam hal pengamanan data, sesuai dengan implementasinya atau sesuai dengan aplikasi yang dirancang.

SIMPULAN

Adapun simpulan yang diperoleh dari pembuatan program aplikasi ini adalah sebagai berikut. Perancangan program aplikasi kriptografi dengan menggunakan Algortima Magenta ini dapat diimplementasikan sesuia dengan spesifikasi yang dirancang. Kelebihan dari program ini, cepat, aman, dan telah digunakan oleh Deutsche Telekom di Jerman untuk mengamankan manajemen data yang sensitif, sedangkan kekurangan program ini tidak dilengkapi dengan fungsi hashing. Adapun saran yang dapat diberikan untuk pengembangan lebih lanjut dari program aplikasi kriptografi ini adalah sebagai berikut. Untuk memberikan jaminan keamanan data yang lebih baik, dapat digunakan kunci dengan bit yang lebih panjang. Selain itu, juga menggunakan modus operasi selain ECB, yaitu Chiper Block Chaining (CBC), Chiper FeedBack (CFB), atau Output FeedBack (OFB).

DAFTAR PUSTAKA

Jacobson Jr, M. J., and Huber K. The Magenta Block Cipher Algorithm. Retrieved on August 10, 2004 from http://www.madchat.org/crypto/magenta.pdf.

Pfleeger, C. P. (1989). *Security in computing*, Englewood Cliff: Prentice Hall.

Soplanit, S. (2004). *Bahan kuliah security computer*, Jakarta: Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Tarumanagara.

Stallings, W. (1995). *Network and internetwork security*, New York: Prentice Hall Inc.

Tannenbaum, A. S. (1989). *Computer network*, New York: Prentice Hall Inc.