JURNAL TEKNOLOGI INFORMASI

Volume 5, Nomor 1, Pebruari 2009
ISSN 1414-9999

CyberKU

Diterbitkan oleh
Program Pascasarjana Magister Teknik Informatika
UNIVERSITAS DIAN NUSWANTORO

Jurnal Teknologi Informasi	Volume 5 Nomor 1	Halaman 533 - 659	Semarang Pebruari 2009	ISSN 1414-9999

JURNAL TEKNOLOGI INFORMASI

olume 5, Nomor 1, Pebruari 2009

SSN 1414-9999

CyberKU

DEWAN REDAKSI

Diterbitkan oleh
Program Pascasarjana Magister Teknik Informatika
UNIVERSITAS DIAN NUSWANTORO

Jurnal Teknologi Informasi	Volume 5 Nomor 1	Halaman 533 - 659	Semarang Pebruari 2009	ISSN 1414-9999

JURNAL TEKNOLOGI INFORMASI

olume 5, Nomor 1, Pebruari 2009
SSN 1414-9999

CyberKU

DAFTAR ISI

Diterbitkan oleh
Program Pascasarjana Magister Teknik Informatika
UNIVERSITAS DIAN NUSWANTORO

Jurnal Teknologi Informasi	Volume 5 Nomor 1	Halaman 533 - 659	Semarang Pebruari 2009	ISSN 1414-9999

PENYANDIAN ALGORITMA SIMETRI DENGAN KUNCI DINAMIS UNTUK FILE TEKS

Agustinus Darto Iwan Setiawan
Pascasarjana, Magister Teknik Informatika, Universitas Dian Nuswantoro Semarang

Abdul Syukur
Pascasarjana, Magister Teknik Informatika, Universitas Dian Nuswantoro Semarang

Purwanto
Pascasarjana, Magister Teknik Informatika, Universitas Dian Nuswantoro Semarang

ABSTRACT

Mostly of the cryptography method have a characteristic of static and known every people. This causes the algorithm is brittle enough to be cracked by certain ways. This new characteristic method is existence of substitution of dynamic nature. Text file has information about date and time to be created of file is always attach of the file. Date and time created file is taken information above as one of the encryption and description key.

This algorithm feature is number of possibility of key combination that very big, unbreakable by analyzing frequency of appearing character or character pair and ciphertext that a lot enough, not yet known of cryptography world, authentication existence and non repudiation by existence of key of sender name as encryption key.

There are four step of encryption process or to description of the algorithm to complicate cracking effort conducted by people unconcern. For further developing, it can add of ability to encrypts and descript of image file.

Keyword : cryptography, dynamic key, encryption, description, text file.

Pendahuluan

Perkembangan penggunaan komputer membawa perkembangan yang pesat pada berbagai macam perangkat lunak komputer. Kemajuan di bidang telekomunikasi dan komputer telah memungkinkan seseorang *cashless* dan *on-line*.

Masalah keamanan pada komputer menjadi isu penting pada era teknologi informasi ini. Banyak kejahatan cyber yang terjadi, yang beritanya bisa kita baca pada portal berita di internet dan di media massa.

Kriptografi merupakan dasar untuk memahami keamanan pada komputer. Kriptografi telah digunakan pada semua bidang kehidupan. Mulai dari penggunaan kartu ATM, penggunaan password untuk file – file dokumen kantor, transaksi dengan kartu kredit, transaksi di bank, percakapan dengan handphone, akses internet, hingga meluncurkan peluru kendali menggunakan kriptografi. Hal ini membuktikan pentingnya kriptografi dalam pengamanan informasi.

Banyak metode untuk melakukan penyandian data. Namum sebagian besar bersifat statis dan sudah dibanyak diketahui orang. Hal tersebut menyebabkan data yang ada didalamnya cukup rentan untuk bisa di-deskripsi oleh orang yang tidak berhak dengan berbagai macam metode seperti metode Differential Cryptanalisis (DC) yang telah dapat digunakan untuk memecahkan metode enkripri Data Encryption Standart (DES) 64 bit.

Kelebihan dari metode baru ini adalah adanya kunci substitusi yang bersifat dinamis , sehingga sebuah file yang sama persis bisa saja di-enkripsi menjadi beberapa file hasil enkripsi yang berbeda.

Dengan menggunakan metode penyandian kunci dinamis ini , pada setiap penerapan algoritma, akan dihasilkan chipertext yang berbeda-beda. Setiap kali proses enkripsi pada file yang sama akan menghasilkan cipherteks yang berbeda. Sehingga metode pembongkaran akan sangat sulit diterapkan di sini. Pada umumnya metode pembongkaran algoritma tidak memperdulikan tanggal diciptakannya sebuah file dan pembuat file, yang menjadi kunci utama di sini.

Algoritma yang akan dipergunakan pada tesis ini hanya algoritma simetri substistusi dan algoritma simetri transposisi saja.

Metode Rekayasa

Model pengembangan perangkat lunak yang digunakan adalah System Development Life Cycle (SDLC) iteratif / spiral. Beberapa tahap dalam SDLC iteratif / spiral dijabarkan di bawah ini.

1. Planning / Perencanaan : Mengumpulkan contoh – contoh file yang berisi dokumen – dokumen rahasia yang sering dikirimkan oleh narasumber. Mengumpulkan informasi dari buku dan referensi tentang teknik – teknik enkripsi dan dekripsi yang termasuk dalam kelompok simetri untuk mengetahui kelemahan dan kelebihan masing- masing teknik.
2. Analysis / Analisa : Dari informasi yang didapat dari tahap perencanaan, dipilih beberapa teknik enkripsi dan dekripsi yang paling sesuai untuk

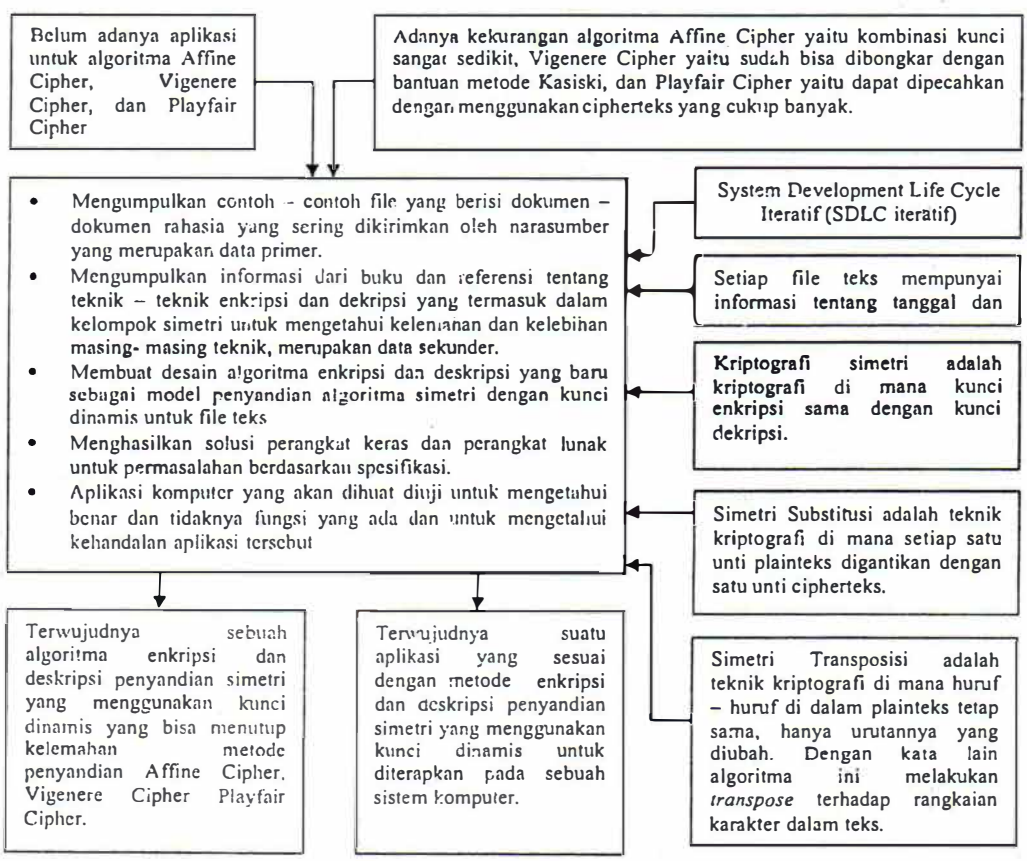
menutup kelemahan yang ditemukan. Tahap ini menggunakan studi pustaka untuk mendapatkan data.

3. Design / Desain : Pilihan yang didapatkan pada tahap analisa, dimunculkan dalam bentuk desain yang mempertimbangkan semua perangkat yang mendukung.
4. Implementation / Pembuatan Aplikasi : Berdasarkan perangkat lunak dan perangkat keras dan teknik yang telah dipersiapkan pada tahap desain, dibentuk sebuah aplikasi komputer yang bisa dipakai untuk menerapkan teknik yang telah dipilih.
5. Test / Pengujian : Pada tahap ini, aplikasi komputer yang sudah dibuat diuji untuk mengetahui benar dan tidaknya fungsi yang ada dan untuk mengetahui kehandalan aplikasi tersebut. Digunakan tiga buah pengujian, yaitu black box, white box, dan user acceptance.

Kerangka Pemikiran

Kerangka pemikiran ini dimulai dengan mengadakan identifikasi masalah – masalah yang berkaitan dengan penyandian yang bisa mendukung penulis untuk menguatkan judul tesis ini. Khususnya untuk sandi – sandi yang bersifat simetri.

Berdasarkan pustaka yang dipergunakan pada penyusunan tesis ini, didapat beberapa hal yang menjadi pertimbangan dalam pembuatan Penyandian Algoritama Simetri dengan Kunci Dinamis untuk File Teks.



Analisis pada Algoritma Pembanding

Berdasarkan tinjauan pustaka yang telah disajikan pada bab sebelumnya, berikut ini akan disajikan analisa mengenai kelebihan dan kekurangan masing – masing algoritma yang dijadikan pembanding.

Affine Cipher

Kelebihan : Kunci bisa sesuai dengan keinginan pengguna algoritma karena pengguna bisa dengan bebas menentukan nilai m dan nilai b.

Kekurangan : Jumlah kemungkinan kombinasi kunci yang merupakan kombinasi m dan b hanya 25 x 12 = 52. Sehingga mudah dicari kuncinya dengan exhaustive key search.

Vigenere Cipher

Kelebihan : Kekuatan dari cipher ini adalah adanya banyak huruf cipherteks untuk setiap huruf plainteks, satu untuk setiap huruf unik dari huruf kunci. Jadi, informasi frekuensi huruf menjadi tidak jelas.

Kekurangan : Sudah dikembangkan cara atau metode (Metode Kasiski) untuk membongkar algoritma ini sejak lebih dari 100 tahun yang lalu dan terbukti berhasil dibongkar.

Playfair Cipher

Kelebihan : Playfair cipher termasuk ke dalam polygram cipher yang melakukan substitusi secara bigram (kelompok yang terdiri dari dua huruf). Cipher ini mengenkripsi pasangan huruf. Analisis frekuensi menjadi sangat sulit sebab frekuensi kemunculan huruf menjadi datar .

Kekurangan : Bisa dipecahkan dengan analisa frekuensi kemunculan pasangan huruf plainteks dan cipherteks yang cukup banyak.

Algoritma Baru

Algoritma yang baru mempunyai kemampuan dan ciri yang bisa menutup kekurangan pada masing – masing algoritma yang dibandingkan di atas.

1. Jumlah kemungkinan kombinasi kunci yang merupakan kombinasi 4 langkah enkripsi adalah ± 6,835 * 10 97, metode exhaustive key search sangat lama dilakukan.
2. Tidak bisa dipecahkan dengan analisa frekuensi kemunculan huruf maupun pasangan huruf dan cipherteks yang cukup banyak. Hal ini disebabkan kunci waktu yang selalu berbeda beda untuk setiap kesempatan enkripsi. Walaupun plainteks sama cipherteks bisa berbeda untuk waktu yang berbeda
3. Gabungan dari metode substitusi dengan metode transposisi.
4. Belum dikenal pada dunia kriptografi
5. Belum pernah dikembangkan cara atau metode untuk membongkar algoritma ini
6. Tidak bisa mencari panjang kunci dengan Metode Kasiski karena adanya proses rotasi data dengan kunci yang berbeda

7. Menjamin tercapainya otentikasi dengan adanya kunci Nama Pengirim sebagai Kunci enkripsi
8. Menjamin tercapainya Non repudiation atau anti penyangkalan dengan adanya kunci Nama Pengirim sebagai Kunci enkripsi.

Spesifikasi dan Instalasi Aplikasi

Spesifikasi Perangkat Lunak

1. Aplikasi yang terbentuk merupakan hasil dari kompilasi file dari Visual Basic.
2. Berjalan di bawah sistem operasi Microsoft Windows

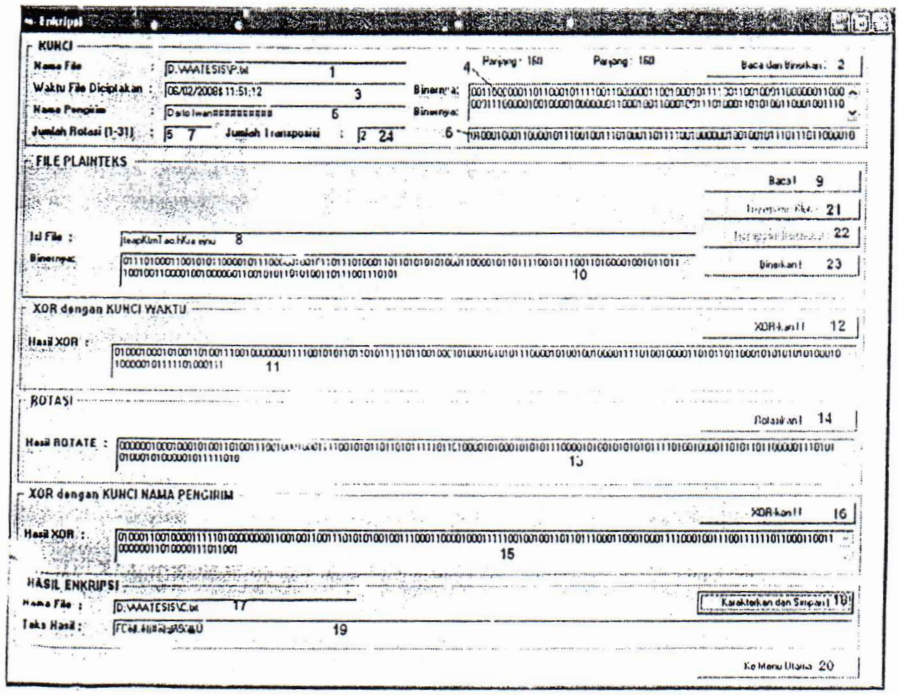
Spesifikasi Perangkat Keras

1. Dari uji coba dihasilkan bahwa kebutuhan hardware minimal adalah Prosesor Intel Pentium II, Memori 64 Mb, VGA 4 Mb
2. Sedangkan besar ruang kosong yang harus disediakan dalam harddisk untuk paket installer dan folder hasil proses instalasi hanya sekitar 400 Kb.
3. Penggunaan keyboard 104 key dan mouse 3 tombol akan sangat membantu dapat menjalankan aplikasi ini.

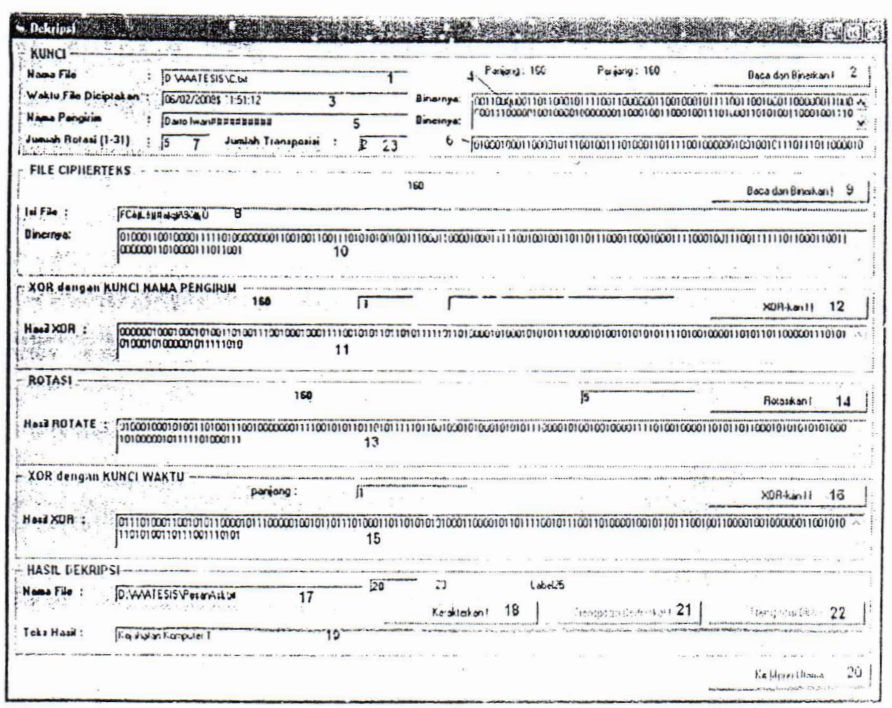
Contoh Tampilan Aplikasi :

Menu Utama

Enkripsi



Dekripsi



Penutup

Algoritma penyandian simetri dengan kunci dinamis ini dapat menutup kelemahan metode penyandian :

1. Affine Cipher, karena penyandian simetri dengan kunci dinamis ini mempunyai ± 6,835 * 10^{97} kemungkinan kunci yang dipergunakan sehingga dengan metode exhaustive key search akan memerlukan waktu yang 5,4 * 10^{50} tahun.
2. Vigenere Cipher, karena penyandian simetri dengan kunci dinamis ini tidak bisa mencari panjang kunci dengan Metode Kasiski karena adanya 3 (tiga) buah kunci yang berbeda – beda dan adanya perbedaan kunci yang dipakai pada tiap file yang berbeda.
3. Playfair, karena penyandian simetri dengan kunci dinamis ini tidak dapat dipecahkan dengan analisa frekuensi kemunculan huruf maupun pasangan huruf walaupun dengan 'mencuri' cipherteks yang cukup banyak. Hal ini disebabkan kunci waktu yang selalu berbeda beda untuk setiap kesempatan enkripsi. Walaupun plainteks sama cipherteks bisa berbeda untuk waktu yang berbeda.

Aplikasi yang terbentuk merupakan hasil dari kompilasi file dari Visual Basic 6.0 yang bisa langsung dijalankan di bawah sistem operasi Microsoft Windows XP, Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows 2000. Kebutuhan hardware minimal untuk menjalankannya adalah Prosesor Intel Pentium II, Memori 64 Mb, VGA 4.

Dalam pengembangan selanjutnya diharapkan terciptanya kemampuan tersebut di atas sehingga algoritma dan aplikasi ini semakin baik, mampu untuk menyandikan file Microsoft Word yang didalamnya terdapat obyek berupa gambar atau obyek lain.

DAFTAR PUSTAKA

[1] http://hadiwibowo.wordpress.com/2008/01/17/melindungi-data-dalam-media-portabel.htm di download tanggal 25 April 2008 jam 10.05 wib.

[2] Nur Cahyo Hendro Wibowo (2004). *Aplikasi Algoritma DC untuk Membongkar DES 64 bit.* Tesis Magister Teknik Informatika. Universitas Dian Nuswantoro.

[3] Jeffrey A Hoffer, Joey F George dan Joseph S Valacich (2008) *Modern Systems Analysis and Design,* Prentice HallNew Jersey.

[4] Rinaldi Munir (2006) *Kriptografi* , Penerbit Informatika, Bandung.

[5] Yusuf Kurniawan (2004) *Kriptografi, Keamanan Internet dan Jaringan Komunikasi*, Penerbit Informatika, Bandung.

[6] W Stalling (1998) *Cryptography and Network Security, Principle and Practice 2 nd Edition,* Pearson Education Inc.

[7] Bruce Schneier(1996) *Aplied Cryptography 2 nd* , John Wiley & Sons.

[8] Alfred J Menezes, Paul C van Oorschot, dan Scott A Vanstone (1996) *Handbook of Aplied Cryptography,* CRC Press

[9] Dony Ariyus (2006) *Computer Security*, Penerbit Andi Yogyakarta, Yogyakarta.

[10] Tim Penyusun Kamus Pusat Pembinaan dan Pengembangan Bahasa (1990) *Kamus Besar Bahasa Indonesia*, Balai Pustaka, Jakarta

[11] John Lewis (2006) *Computer Science Illuminated,* Jones and Bartlett.

[12] Endang PG, Sugi Guritman dan Ahmad Ridha (2005) *Analisis Algoritma dan Waktu Enkripsi Versus Deskripsi pada Advanced Encryption Standard (AES),* Jurnal Ilmiah Ilmu Komputer Vol.3 No.1 Departemen Ilmu Komputer FMIPA IPB, Bogor

[13] Sony HArtono Wijaya, Sugi Guritman, dan Wisnu Ananta Kusuma (2005) *Analisis Algoritma Triple DES untuk Penyandian Pesan,* Jurnal Ilmiah Ilmu Komputer Vol.3 No.2 Departemen Ilmu Komputer FMIPA IPB, Bogor