Perancangan Perangkat Lunak Enkripsi dan Dekripsi File dengan Algoritma RSA Dan RC4

Iwan Tanto, Ricco
STMIK IBBI
Jl. Sei Deli No. 18 Medan, Telp. 061-4567111 Fax. 061-4527548
e-mail: iwntanto@yahoo.com

Abstrak

Data atau informasi merupakan salah satu elemen yang memegang peranan yang sangat besar dalam berbagai bidang kehidupan. Dengan semakin pesatnya perkembangan teknologi komputer, semakin banyak orang yang sanggup mengutak-atik data yang disimpan dengan rapi dan dijaga kerahasiaannya. Untuk mencegah terjadinya pencurian data oleh orang yang tidak berhak, maka dikembangkanlah berbagai teknik pengamanan data. Teknik untuk mengamankan data dikenal sebagai kriptografi. Metode-metode kriptografi sendiri dibagi atas metode public key dan private key. Public key memudahkan user dalam manajemen kunci sedangkan kecepatannya prosesnya lambat. Private key menawarkan proses enkripsi dan dekripsi yang cepat tetapi kunci tidak dapat saling dipertukarkan. Untuk mendapatkan kelebihan dari masing-masing metode kriptografi maka metode-metode tersebut dapat digabungkan sehingga terbentuk metode hybrid. Salah satu metode hybrid yang dapat dikembangkan adalah algoritma RSA yang merupakan kriptografi public key dan RC4 yang merupakan private key block cipher. Dengan adanya metode hybrid ini maka dapat dihasilkan suatu program pengamanan data yang dapat memanajemen kunci dan proses enkripsi dalam satu program yang sama.

Kata kunci: Kriptografi, Enkripsi, Dekripsi, RSA, RC4

Abstract

Data or information is one element that plays a very large in many areas of life. With the rapid development of computer technology, more and more people are able to tamper with the data stored neatly and kept confidential. To prevent data theft by unauthorized people, so it is developing various techniques of data security. Techniques for securing data is known as cryptography. Cryptographic methods themselves divided over the method of public key and a private key. Facilitate the user's public key in a key management process while the speed is low. Offering private key encryption and decryption keys are fast but can not interchangeable. To get the advantages of each method of cryptography that these methods can be combined to form a hybrid method. One method is a hybrid that can be developed which is a cryptographic algorithm RSA public key and private key RC4 is a block cipher. With the hybrid method, it can produce a data security program that can manage encryption keys and processes within the same program.

***Keywords**: Cryptography, Encryption, Decryption, RSA, RC4*

1. Pendahuluan

Data atau informasi merupakan salah satu elemen yang memegang peranan yang sangat besar dalam berbagai bidang kehidupan. Dengan semakin pesatnya perkembangan teknologi komputer, semakin banyak orang yang sanggup mengutak-atik data yang disimpan dengan rapi dan dijaga kerahasiaannya. Untuk mencegah terjadinya pengaksesan data oleh orang yang tidak berhak, maka dikembangkanlah berbagai teknik pengamanan data. Data yang tersimpan dalam arsip data itu dapat menyangkut kerahasiaan baik perseorangan maupun kelompok, jadi apabila komputer dan perlengkapan komunikasi dilengkapi dengan sistem pengamanan yang baik, maka komputer dan peralatan tersebut dapat menambah kepercayaan untuk menyimpan, mengolah, dan bertukar data atau informasi yang sangat penting [3]. Teknik pengamanan data yang biasanya dikenal sebagai kriptografi merupakan salah satu solusi untuk permasalahan di atas. Ada banyak metode kriptografi yang dapat digunakan untuk melakukan enkripsi data, antara lain: DES (*Data Encryption Standard*) yang dikembangkan oleh IBM, RSA (*Rivest-Shamir-Adleman Algorithm*), *Blowfish*, *Helix*, *Solitaire*, *RC4*, *Frog*, *GOST*, *SkipJack*, *TEA*, dan lain-lain. Metode-metode tersebut mempunyai tingkat keamanan yang bervariasi, kecepatan, dan kemudahan dalam hal implementasi algoritmanya. Tetapi untuk pertukaran data di Internet jika hanya menggunakan metode *symetric*, maka akan terjadi penyadapan data. Sehingga metode *symetric* dan *asymetric* harus dikombinasikan untuk mengatasi hal tersebut [4]. Sehingga kedua algoritma tersebut menjadi kuat dan dapat menahan serangan *cipher attack*. Untuk itu maka dibuat sebuah program yang dapat melakukan proses enkripsi dan dekripsi dengan *input* segala jenis *file* teks dan biner. Secara umum tujuan dari penulisan ini adalah merancang perangkat lunak untuk pengamanan data dengan metode algoritma RSA dan RC4 untuk menjaga kerahasiaan *file* atau data sehingga data tersebut tidak dapat diakses oleh orang yang tidak berkepentingan.

2. Metode Penelitian

Algoritma

Algoritma adalah program kriptografi yang digunakan untuk melakukan enkripsi. Ia bukanlah suatu kunci, tetapi menghasilkan kunci. Algoritma kriptografi selalu terdiri dari dua bagian yaitu fungsi enkripsi dan dekripsi [1]. Suatu algoritma yang kuat atau bagus akan menghasilkan kriptografi yang kuat dan bagus juga [5]. Dalam pembuatan perangkat lunak ini peneliti menggunakan metode hybrid yang mengabungkan algoritma RSA dan RC4 sehingga dihasilkan suatu program pengamanan data yang dapat memanajemen kunci dan proses enkripsi dalam satu program yang sama.

Metode RSA & RC4

Metode RSA merupakan sistem kriptografi kunci publik, dibuat pada tahun 1977 oleh Ronald Rivest, Adi Shamir, dan Leonard Adleman dari MIT. Ide dasar RSA dalam mengamankan data, adalah tingkat kesulitan dalam menemukan bilangan prima berdigit besar dan kesulitan dalam memfaktorkan bilangan bulat menjadi 2 buah bilangan prima. Cara Kerja RSA pada prinsipnya adalah perpangkatan modular. Dengan algoritma perpangkatan modular yang khusus yang digunakan untuk mengimplementasikan algoritma RSA, operasi kunci publik membutuhkan waktu $O(k^2)$, operasi kunci rahasia membutuhkan $O(k^3)$, sedangkan pembentukan kunci memiliki kompleksitas $O(k^4)$; dimana k adalah jumlah bit dalam operasi modular [2]. Kecepatan DES dan *block ciphers* yang lain jauh lebih tinggi daripada RSA. Perbandingan kecepatan DES dengan RSA ialah algoritma DES paling tidak 100 kali lebih cepat dalam *software* dan antara 100 sampai 10000 kali lebih cepat dalam implementasi *hardware*, tergantung pada implementasi. Walaupun RSA lambat tetapi tetap digunakan karena memberikan keuntungan dalam hal keamanan pertukaran kunci dan kemampuan untuk menerapkan tanda tangan digital.

Metode RC4 adalah jenis kriptografi *symmetric key*, *secret key*, dan *stream cipher* yang didesain oleh Ron Rivest. RC merupakan singkatan dari "*Ron's Code*". RC4 merupakan bagian dari protokol standar enkripsi yang umum digunakan termasuk dalam SSL (*Security Socket Layer*) yang dipakai untuk mengamankan jaringan *web browser*. (RC4, Wikipedia, 2010). RC4 diinisialisasi dari sebuah kunci rahasia. Kemudian di-*generate* sebuah "*keystream*" yang disederhanakan dengan XOR dengan *plaintext* untuk menghasilkan *ciphertext*. Proses dekripsi sama dengan proses enkripsi. Salah satu alasan untuk kepopuleran RC4 adalah kesederhanaannya. Algoritma RC4 dapat diingat dan mudah diimplementasikan. Algoritma RC4 menggunakan 256 *byte* dari memori, S[0] hingga S[255], dan menggunakan variabel integer i, j, dan k. RC4 adalah salah satu cipher yang tercepat yang dipergunakan secara luas untuk pekerjaan yang serius. RC4 menggunakan panjang kunci variabel dari 1–256 *byte* (mempunyai kemampuan antara 1−2048 bit) untuk menginisialisasi 256−*byte state table*. Algoritma RC4 dibagi menjadi dua tahap, yaitu membentuk kunci dan *ciphering* (enkripsi/dekripsi). Pembentukan kunci merupakan tahap pertama dan tersulit. Selama pembentukan kunci, kunci enkripsi digunakan untuk menghasilkan sebuah variabel enkrip menggunakan 2 *array* (*state array* & *key array*) dan sejumlah operasi penjumlahan.

Untuk mendapatkan kelebihan dari masing-masing metode kriptografi maka metode algoritma RSA yang merupakan kriptografi public key dan RC4 yang merupakan private key block cipher digabungkan sehingga terbentuk metode hybrid yang diberi nama *RSARC4 Cyrpto* sehingga dihasilkan suatu program pengamanan data yang dapat memanajemen kunci dan proses enkripsi dalam satu program yang sama.

3. Hasil dan Analisis

3.1 Analisa Sistem

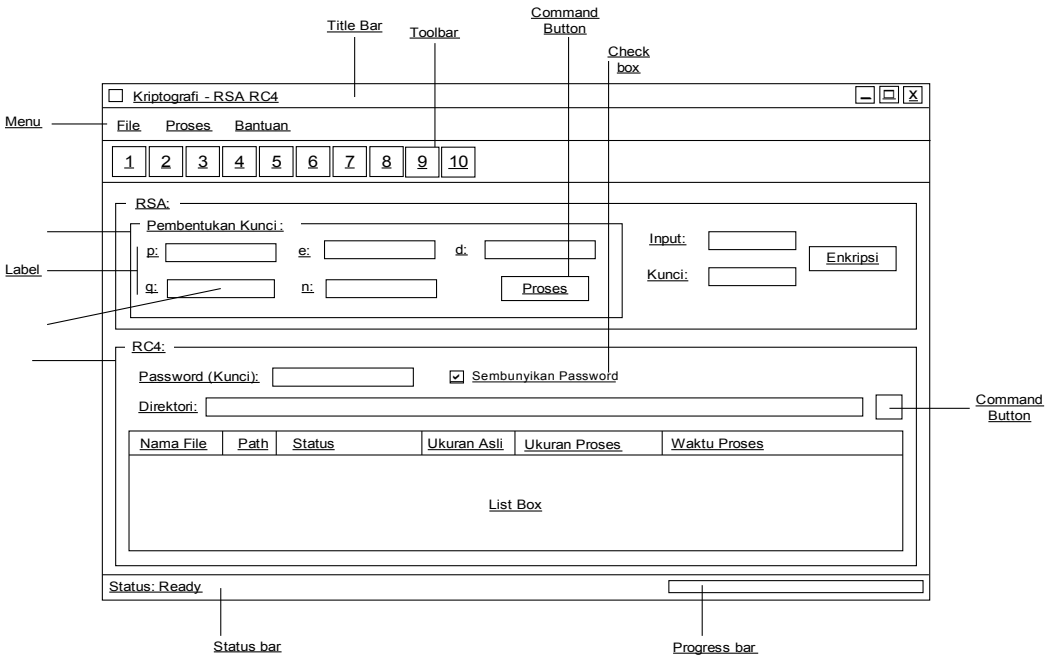
Teknik analisis data dalam perancangan perangkat lunak ini berupa analisis contoh perhitungan metode RSA dan RC4 baik untuk proses enkripsi dan proses dekripsi. Adapun pada rancangan program, *file* kunci terenkripsi akan dikirimkan bersamaan. Kunci asli yang digunakan untuk mengenkripsi *file* dengan RC4 akan diproses melalui RSA sehingga didapat kunci terenkripsi. Selanjutnya *file* dan kunci tersebut akan di-*packed* menjadi satu *file* tunggal.

3.2 Hasil Perancangan

3.2.1 Perancangan Sistem Perangkat Lunak

3.2.1.1 Perancangan *Form*

Form pada program ini hanya terdiri atas dua buah *form* utama saja yaitu *form* utama dan *form* about. Bentuk rancangan dari *form utama* dapat dilihat pada Gambar 1.



Gambar 1 Rancangan *Form* Utama

Gambar di atas merupakan bentuk rancangan pada *form* utama. Terdiri atas beberapa *frame* yaitu *frame* bagian RSA dan RC4. Komponen utama penyusun *form* tersebut adalah *command button*, *frame*, menu, *list box*, *progress bar*, *label*, *status bar*, dan *toolbar*. Bagian dari *toolbar* ini mempunyai 10 buah *button* yang fungsinya dapat dijabarkan sebagai berikut:

 digunakan untuk keluar dari program ini.

 digunakan untuk menginput *file* tunggal ke dalam list.

 digunakan untuk menginput seluruh *file* dalam *folder* ke dalam list.

 digunakan untuk menghilangkan *file* yang ditandai dari list.

 digunakan untuk menghilangkan seluruh *file* dari list.

 digunakan untuk menandai semua *file* dari list.

 digunakan untuk menghilangkan semua tanda cek dari list.

 digunakan untuk proses enkripsi *file* yang dipilih.

 digunakan untuk proses dekripsi *file* yang dipilih.

 digunakan untuk menampilkan *form about*.

Berikutnya adalah rancangan dari *form about*. Bagian ini hanya digunakan untuk menampilkan suatu *form* yang berisi *label* keterangan nama penulis selaku pembuat program. Semua objek *visual* yang digunakan pada *form* ini adalah *label* ditambah dengan sebuah *command button*.

3.2.1.2 Perancangan *Class Module*

Perancangan *Class Module* bertujuan agar objek *class* yaitu berisi fungsi-fungsi utama proses enkripsi / dekripsi dengan algoritma dapat dipakai dengan mudah dan dapat dipakai kembali (*reuseable*) untuk pembuatan program lain yang memakai algoritma enkripsi RSA ataupun RC4. Selain itu fungsi yang dideklarasikan berupa objek *class* akan lebih cepat dalam hal pemrosesan.

Class Module yang dibuat diberi nama clsHybrid (singkatan dari *Class Hybrid*). *Class* ini berisi rutin-rutin dari algoritma RSA dan RC4 serta seperti fungsi untuk enkripsi *file*, dekripsi *file*, operasi *path*, serta suatu fungsi untuk mengecek keberadaan suatu *file* pada lokasi *folder* tertentu.

3.2.1.3 Perancangan *Module Function*

Module Function berguna untuk mendeklarasikan semua fungsi yang berhubungan dengan operasi pada *file*, mengambil *path* pada *file*, mengambil nama *file*, ekstensi *file*, mengecek tanggal pembuatan *file*, ukuran *file*, jenis atribut *file*, dan lain-lain. Kebanyakan fungsi yang dideklarasikan tersebut merupakan fungsi yang dikompilasi dalam *library* atau pustaka pada sistem operasi Windows. Jadi fungsi tersebut sebenarnya tidak dibuat lagi sendiri oleh penulis melainkan langsung menggunakannya melalui *Visual Basic*.

3.3 Implementasi Program

Implementasi sistem program ini mencakup spesifikasi kebutuhan perangkat keras (*hardware*) dan spesifikasi perangkat lunak (*software*).

3.3.1 Spesifikasi Perangkat Keras dan Perangkat Lunak

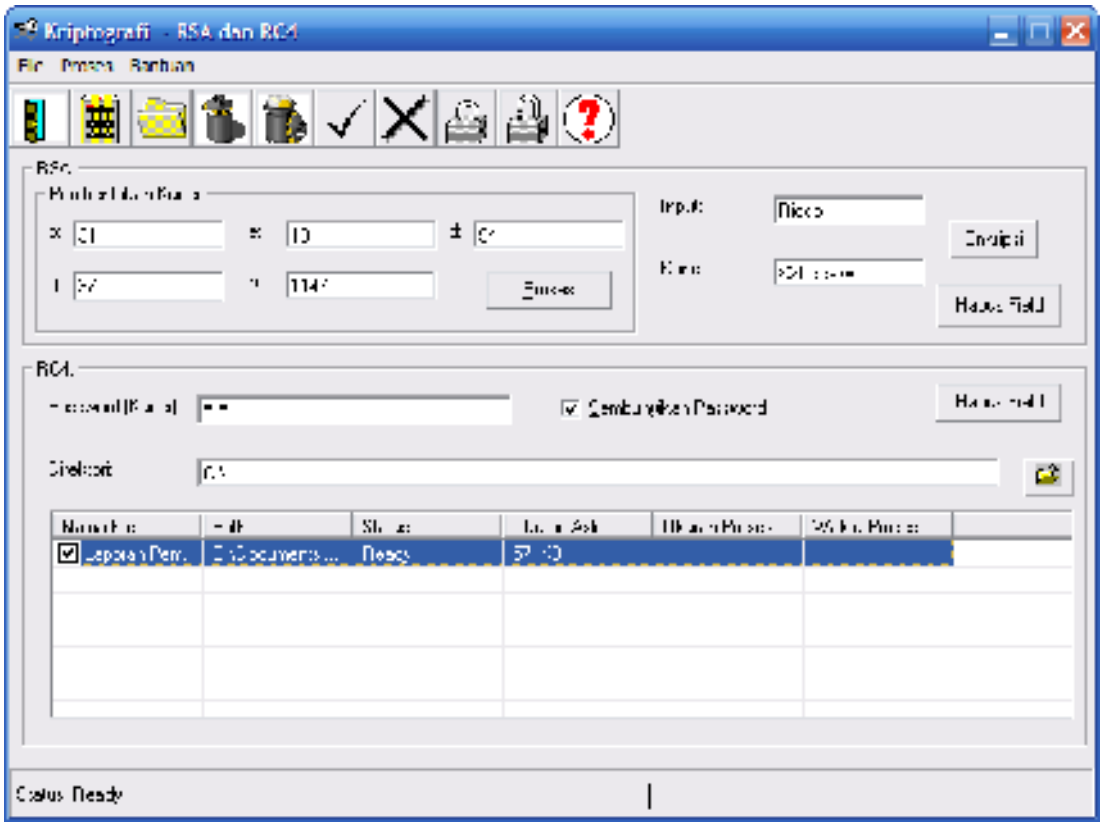
Program ini dijalankan dengan menggunakan perangkat keras (*hardware*) yang mempunyai spesifikasi minimal adalah sebagai berikut :

- *Prosesor Intel Pentium* Core i3 2.13 GHz.
- *Memory* 2 GB.
- *Harddisk* 250 GB.
- Monitor dengan resolusi 1366 × 768 *pixel*.
- Intel HD Graphics
- *Mouse*
- *Keyboard*

Adapun perangkat lunak (*software*) yang digunakan untuk menjalankan aplikasi ini adalah lingkungan sistem operasi *MS-Windows 98* atau *MS-Windows NT/2000/XP*.

3.3.2 Pengujian Program

Setelah program dikompilasi dan dijalankan, maka tampilan dari program ini diperlihatkan pada Gambar 2.



Gambar 2 Tampilan Program

Pada tampilan di atas bagian dari *toolbar* di atas digunakan untuk keluar dari program menambah dan membuang *file* yang akan diproses dari *list*. Dua bagian selanjutnya adalah bagian pembentukan kunci dan bagian enkripsi dengan menggunakan RC4.

Selanjutnya pengujian yang dilakukan oleh penulis atas program ini menggunakan dua spesifikasi komputer yaitu *Pentium IV 3.2 GHz* dan *Pentium Core i3 2.13 GHz* untuk menunjukkan proses enkripsi dan dekripsi program. Adapun spesifikasi komputer yang digunakan dapat dilihat pada Tabel 1 berikut ini.

Tabel 1 Spesifikasi Komputer Pengujian

Spesifikasi	A	B
Processor	Intel Pentium IV 3.2 Ghz	Intel Pentium core i3 2,13 GHz
Memori	SDRAM 256 MB	DDR 256 MB
Harddisk	120 GB	250 GB
Sistem Operasi	Windows XP Professional	Windows XP Professional

Tabel 2 Hasil Pengujian Enkripsi RC4

Jenis	File	Ukuran (byte)	Waktu (KB/Detik) I	II	III	Rata
A	*.DOC	12.546	52,23	53,20	52,68	52,70
	*.WAV	25.640	101,24	102,25	103,50	102,33
	*.BMP	84.265	250,68	252,46	253,57	252,34
	*.TXT	1.254	5,22	5,35	5,78	5,45
B	*.DOC	12.546	17,41	18,52	17,60	17,84
	*.WAV	25.640	33,45	35,60	32,25	33,76
	*.BMP	84.265	83,56	85,68	83,47	82,24
	*.TXT	1.254	1,26	1,25	1,30	1,27

Tabel 3 Hasil Pengujian Dekripsi RC4

Jenis	File	Ukuran (byte)	Waktu (KB/Detik) I	II	III	Rata
A	*.DOC	12.549	53,32	54,30	53,87	53,83
	*.WAV	25.643	104,46	105,54	104,35	104,78
	*.BMP	84.268	252,87	254,66	254,76	254,09
	*.TXT	1.257	6,42	6,52	6,55	6,49
B	*.DOC	12.549	19,53	19,32	18,32	19,05
	*.WAV	25.643	35,59	36,53	33,58	35,23
	*.BMP	84.268	84,75	86,13	84,26	85,04
	*.TXT	1.257	2,42	1,95	2,15	2,17

Dari hasil diatas terlihat bahwa keunggulan metode hibrida dengan menggunakan RSA dan RC4 adalah mengenkripsi data sebenarnya secara simetris, tetapi kuncinya secara asimetris.

4. Kesimpulan

Rancangan perangkat lunak metode hybrid dengan nama *RSARC4 Cyrpto* dirancang dengan menggabungan antara algoritma RSA yang merupakan kriptografi public key dan RC4 yang merupakan private key block cipher sehingga dapat memanajemen kunci dan proses enkripsi dalam satu program yang sama. Algoritma RSA pada program dipergunakan untuk tujuan pertukaran kunci. Sedangkan RC4 digunakan untuk mengenkripsi dan mendekripsi *file*. Dengan adanya perangkat lunak ini maka dapat dilakukan proses pertukaran data dan kunci secara langsung. Adapun keunggulan metode hibrida dengan menggunakan RSA dan RC4 adalah mengenkripsi data sebenarnya secara simetris, tetapi kuncinya secara asimetris.

Daftar Pustaka

[1] Ariyus, D, 2006, *Kriptografi Keamanan Data dan Komunikasi*, Graha Ilmu, Yogyakarta.
[2] Arryawan, E & Smitdev Community, 2010, *Password is Nothing*, Gramedia, Jakarta.
[3] Collberg, C., Nagra, J., *Surreptitious Software: Obfuscation,Watermarking, and Tamperproofing for Software Protection*, Upper Saddle River, NJ: Addison-Wesley, 2010.
[4] Patterson, Wayne., "Mathematical Cryptology for Computer Scientiests and Mathematicians", Rowman & Littlefield Publishers, The United States of America, 1987.
[5] Scheiner, B., *Applied Cryptography*, 2nd ed., John Wiley & Sons, 1996.