Jurnal Ilmiah Ilmu Komputer, Vol. 2, No. 2, September 2016
Fakultas Ilmu Komputer
Universitas AL Asyariah Mandar

(P) ISSN 2442-451X
(O) ISSN 2503-3832

KRIPTOGRAFI SIMETRIS DAN ASIMETRIS DALAM PERSPEKTIF KEAMANAN DATA DAN KOMPLEKSITAS KOMPUTASI

Basri

Program Studi Teknik Informatika
Universitas Al Asyariah Mandar
Jl. Budi Utomo No. 2, Sulawesi Barat Indonesia
basri05@fikom-unasman.ac.id

ABSTRAK

Dalam suatu perusahaan keamanan data merupakan hal yang sangat penting. Masalah keamanan dan integritas data merupakan hal yang harus diperhatikan. Upaya menjaga informasi agar tidak jatuh ke tangan orang yang tidak berkepentingan menuntut perlunya diterapkan suatu mekanisme yang baik dalam mengamankan data. Ada banyak metode kriptografi yang umum dapat diterapkan, dalam klasifikasi secara umum terdiri atas dua, yaitu metode Simetris dan Asimetris. Dalam proyek ini, dilakukan suatu analisis dalam perspektif keamanan data dan kompleksitas komputasi menggunakan dua jenis metode kriptografi, untuk implementasinya dibuat suatu sistem dimana data yang dikirim (plaintext) terlebih dahulu dienkripsi oleh pengirim (*Sender*) menghasilkan data terenkripsi (*chipertext*) dan selanjutnya akan dikirim kepada penerima (*receiver*) untuk dilakukan proses dekripsi sehingga dihasilkan suatu data yang utuh seperti semula. Tentunya dalam implementasi ini dianalisis keakuratan data yang telah dienkripsi, tingkat kesulitan, keamanan dan waktu yang dibutuhkan dalam prosesnya. Dari hasil analisis penelitian terkait dalam pengujiannya terlihat bahwa kedua metode tersebut memiliki keakuratan yang sama, namun kerumitan lebih pada metode Asimetris, dan waktu yang digunakan dalam proses komputasi kriptografi Asimetris cenderung lebih kompleks, namun tingkat keamanan data lebih baik menggunakan metode Asimetris.

Kata Kunci: Simetris, Asimetris, Kriptografi, Keamanan Data.

ABSTRACT

Data security is important In an enterprise. Security and integrity of data is something that must be considered. Efforts to keep information from falling into the hands of unauthorized persons demanding the need to apply a good mechanism in security. There are many common cryptographic methods can be applied, in the classification generally consists of two, Symmetric and Asymmetric method. In this project, carried out an analysis in the perspective of data security and computational complexity using two types of cryptography methods, for its implementation, created a system where data is transmitted (plaintext) first encrypted by the sender generate encrypted data (ciphertext) and will be sent to the receiver to do the decryption process to produce a data intact as before. Of course, in this implementation analyzed the accuracy of the data that has been encrypted, the level of difficulty, security and time required in the process. From the test results of refference article shown that both methods have the same accuracy, but more complexity on Asymmetric methods, and time used in asymmetric cryptography computing process tend to be more complex, but by the level of data security using asymmetric methods is better.

Keywords: Symmetric, Asymmetric, Cryptography, Data Security.

(P) ISSN 2442-451X
(O) ISSN 2503-3832

1. PENDAHULUAN

Teknologi Informasi berkembang cukup pesat, memungkinkan keamanan data menjadi hal yang rawan. Banyaknya penyusup yang dapat melihat bahkan merusak data merupakan hal yang harus diperhatikan. sehingga diperlukan sistem komputer dengan tingkat keamanan yang dapat terjamin dan bisa terhindar dari serangan (attack), walaupun pada akhirnya akan terjadi trade off antara tingkat keamanan dan kemudahan akses. [1]

Terlebih lagi bagi sebuah perusahaan yang memiliki gudang data yang besar dibutuhkan sebuah arsitektur database yang didalamnya terdapat sistem keamanan yang berlapis. [2]

Diperlukan suatu metode pengamanan data yang efektif untuk menunjang hal tersebut. Dari beberapa metode yang telah diteliti pada dasarnya terbagi atas dua jenis yaitu metode Simetris dan Metode Asimetris. Kedua metode dengan berbagai varian banyak digunakan untuk mengamankan data, namun pada implementasinya belum pernah dilakukan suatu studi komparasi untuk menganalisis keakuratan data yang telah dienkripsi, tingkat kesulitan, keamanan dan waktu yang dibutuhkan dalam prosesnya.

Penelitian terkait yang menggunakan metode Simetris diantaranya yang dilakukan oleh Ashadi Kurniawan, dkk. yang menggunakan metode Enkripsi Algoritma RC-5 [1], Victor Asido Elyakim, dkk. yang menggunakan Enkripsi Simetris dengan algoritma FEAL [3], sedangkan yang menggunakan metode Asimetris diantaranya yang dilakukan oleh Putu H. Ajrana, dkk. yang menggunakan Algoritma Vigenere Chiper [4], dan yang dilakukan oleh Munawar yang merancang suatu metode kriptografi asimetris [5].

Sehingga pada penilitian akan dianalisis permasalahan tersebut, dengan suatu studi kasus yang selanjutnya akan menghasilkan sebuah kesimpulan manakah yang lebih baik antara metode Simetris atau metode Asimetris.

2. TINJAUAN PUSTAKA

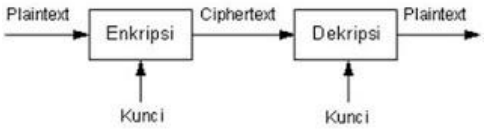
Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *cryptós* yang artinya *"secret"* (yang tersembunyi) dan *gráphein* yang artinya *"writting"* (tulisan). Jadi, kriptografi berarti *"secret writting"* (tulisan rahasia). Definisi yang dikemukakan oleh Bruce Schneier (1996), kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (Cryptography is the art and science of keeping messages secure).

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan (message). Algoritma kriptografi adalah :

- Aturan untuk enkripsi (enciphering) dan dekripsi (deciphering).
- Fungsi matematika yang digunakan untuk enkripsi dan dekripsi.

Suatu pesan yang tidak disandikan disebut sebagai *plaintext* ataupun dapat disebut juga sebagai *cleartext*. Proses yang dilakukan untuk mengubah plaintext ke dalam ciphertext disebut *encryption* atau *encipherment*. Sedangkan proses untuk mengubah ciphertext kembali ke plaintext disebut *decryption* atau *decipherment*. Secara sederhana istilah-istilah di atas dapat digambarkan sebagai berikut :

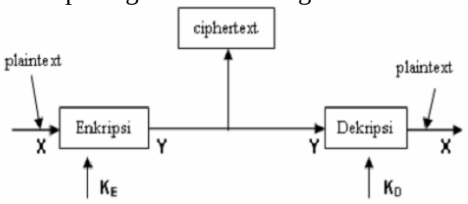


Gambar 1. Proses Enkripsi/Dekripsi Sederhana

Algoritma kriptografi berkembang terus dan terbagi atas dua bagian yaitu algoritma kriptografi klasik dan modern. Pada kriptografi klasik, kriptografer menggunakan algoritma sederhana, yang memungkinkan cipherteks dapat dipecahkan dengan mudah (melalui penggunaan statistik, terkaan, intuisi, dan sebagainya). Algoritma kriptografi modern dibuat sedemikian kompleks sehingga kriptanalis sangat sulit untuk memecahkan cipherteks tanpa mengetahui kunci. Pengelompokan algoritma juga dilakukan berdasarkan kunci enkripsi – dekripsi yang digunakan, yaitu symmetric cryptosystem atau simetris (menggunakan kunci yang sama untuk proses enkripsi – dekripsi) dan Assymmetric cryptosystem atau asimetris (menggunakan kunci yang berbeda untuk proses enkripsi – dekripsi).

Enkripsi dan Dekripsi

Proses penyandian pesan dari *plaintext* ke *ciphertext* dinamakan *enkripsi / enchipering*. Sedangkan proses mengembalikan pesan dari *chipertext* ke *plaintext* dinamakan *deskripsi /dechipering*. Proses enkripsi dan deskripsi ini dapat diterapkan pada pesan yang dikirim ataupun pesan yang disimpan. Algoritma Kriptografi dari setiap kriptografi klasik selalu terdiri dari dua bagian yaitu enkripsi dan dekripsi. Secara sederhana proses kriptografi dapat digambarkan sebagai berikut :



Gambar 2. Kriptografi secara umum[1]

Operasi enkripsi dan dekripsi dijelaskan secara umum sebagai berikut :

EK (M) = C (Proses Enkripsi)

DK (C) = M (Proses Dekripsi)

Ada dua cara yang paling dasar pada kriptografi klasik. yaitu adalah Transposisi dan Subsitusi :

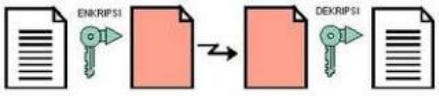
(P) ISSN 2442-451X
(O) ISSN 2503-3832

- Transposisi adalah mengubah susunan huruf pada plaintext sehingga urutannya berubah. Contoh yang paling sederhana adalah mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik.
- Substitusi yaitu setiap huruf pada plaintext akan digantikan dengan huruf lain berdasarkan suatu cara atau rumus tertentu.

Symmetric cryptosystem

Symmetric cryptosystem atau kriptografi simteris atau disebut juga algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Algoritma kriptografi simetris dibagi menjadi 2 kategori yaitu algoritma aliran (*Stream Ciphers*) dan algoritma blok (*Block Ciphers*). Pada algoritma aliran, proses penyandiannya berorientasi pada satu bit atau satu byte data. Sedang pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit atau byte data (per blok).

Ini adalah jenis kriptografi yang paling umum dipergunakan. Kunci untuk membuat pesan yang disandikan sama dengan kunci untuk membuka pesan yang disandikan itu. Jadi pembuat pesan dan penerimanya harus memiliki kunci yang sama persis. Siapapun yang memiliki kunci tersebut – termasuk pihak-pihak yang tidak diinginkan – dapat membuat dan membongkar rahasia *ciphertext*. Problem yang paling jelas disini terkadang bukanlah masalah pengiriman *ciphertext*-nya, melainkan masalah bagaimana menyampaikan kunci simetris tersebut kepada pihak yang diinginkan. Contoh algoritma kunci simetris yang terkenal adalah DES (*Data EncryptionStandard*) dan RC-4, sebagaimana ditunjukkan pada gambar 3 berikut :



Gambar 3. Kunci simetris

Ada beberapa kelebihan menggunakan kunci simetris yang sudah diketahui yaitu Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik walupun hal ini berbanding lurus dengan penambahan ukuran file [2], kecepatan proses enkripsi/dekripsi bergantung pada besarnya ukuran file, semakin besar ukuran file semakin banyak waktu yang dibutuhkan untuk enkripsi/dekripsi [7], selain itu Karena kecepatannya yang cukup tinggi, maka dapat digun akan pada sistem *real-time*. Namun terdapat pula kelemahannyya, yaitu Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut, dan Permasalahan dalam pengiriman kunci itu sendiri yang disebut *" key distribution problem".*

Dalam analisis ini digunakan Algoritma RC-5. algoritma RC-5 merupakan metode enkripsi menggunakan metode simetrik dan pengolahan dalam bentuk blok chiper, jadi kata kunci yang sama digunakan untuk proses enkripsi dan dekripsi. Parameter-parameter yang digunakan dalam RC-5 adalah sebagai berikut :

a. Jumlah putaran ini disimbolkan dengan r yang merupakan parameter untuk rotasi dengan nilai 0, 1, 2,… 255.
b. Jumlah word dalam bit disimbolkan dengan w. Nilai bit yang di support adalah 16 bit, 32 bit, dan 64 bit.
c. Kata kunci (key word) Variabel ini disimbolkan dengan b dengan range 0, 1, 2, ….255. Key word ini dikembangkan menjadi array S yang digunakan sebagai key pada proses untuk enkripsi dan dekripsi.

Untuk memahami cara kerja RC-5, dapat dimulai dengan melihat konsep dasar bagaimana RC-5 ini bekerja. Hal ini dilakukan untuk memahami cara kerja algoritma ini lebih lanjut. RC-5 Menggunakan operasi dasar untuk proses enkripsi sebagai berikut :

a. Data yang akan dienkripsi dikembangkan menjadi 2 bagian bagian kiri dan bagian kanan dan dilakukan penjumlahan dengan key word yang yang telah diekspansi sebelumnya. Penjumlahan ditunjukan dengan tanda ``+``, dan disimpan di dua register A dan register B.
b. Kemudian dilakukan operasi EX-OR, yang ditandai dengan tanda ``⊕``.
c. Melakukan rotasi kekiri (shift left) sepanjang y terhadap x word yang ditandai dengan x<<< y. y merupakan interpretasi modulo w atau jumlah kata w dibagi 2. Dengan lg[w] ditentukan jumlah putaran yang dilakukan.
d. Tahap akhir dilakukan penggabungan untuk mendapatkan data yang telah dienkripsi.

Proses dekripsi dilakukan dengan konsep dasar sebagai berikut :

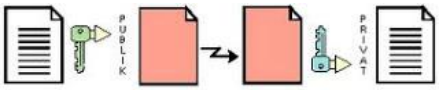
a. Data yang telah dienkripsi dikembangkan kembali menjadi 2 bagian dan disimpan di dua register A dan register B.
b. Kemudian dilakukan rotasi ke kanan sejumlah r. Satuan
c. Selanjutnya dilakukan operasi EX-OR yang ditandai dengan ``⊕``.
d. Tahap akhir dilakukan pengurangan terhadap masing-masing register dengan key word yang ditunjukan dengan tanda ``-``, untuk mendapatkan plaintext.

Assymmetric cryptosystem

Pada pertengahan tahun 70-an **Whitfield Diffie** dan **Martin Hellman** menemukan teknik enkripsi asimetris yang merevolusi dunia kriptografi. Kunci

(P) ISSN 2442-451X
(O) ISSN 2503-3832

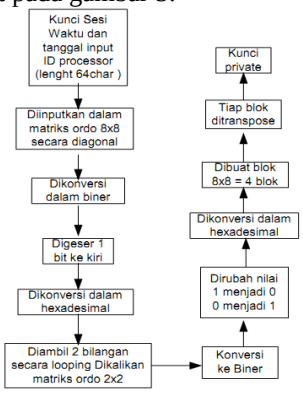
asimetris adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu dalam hal ini kunci private untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya. Sebagai contoh jika Anto mengirim pesan untuk Badu, Anto dapat merasa yakin bahwa pesan tersebut hanya dapat dibaca oleh Badu, karena hanya Badu yang bisa melakukan dekripsi dengan kunci privatnya. Tentunya Anto harus memiliki kunci publik Badu untuk melakukan enkripsi. Anto bisa mendapatkannya dari Badu, ataupun dari pihak ketiga seperti Tari.



Gambar 4. Penggunaan kunci asimetris

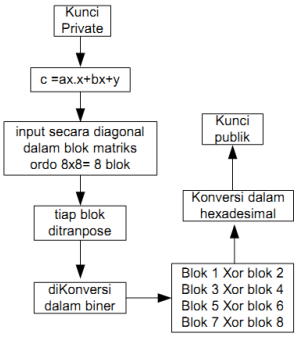
Teknik enkripsi Asimetris ini jauh lebih lambat ketimbang enkripsi dengan kunci simetris. Oleh karena itu, biasanya bukanlah pesan itu sendiri yang disandikan dengan kunci asimetris, namun hanya kunci simetrislah yang disandikan dengan kunci asimetris. Sedangkan pesannya dikirim setelah disandikan dengan kunci simetris tadi. Contoh algoritma terkenal yang menggunakan kunci Asimetris adalah RSA (merupakan singkatan penemunya yakni Rivest, Shamir dan Adleman).

Salah satu contoh metode kriptografi asimetris adalah yang dikembangkan oleh Munawar [5]. Pada prinsipnya akan dilakukan sebuah proses untuk mendapatkan kunci private dan kunci publik. Untuk dapat memperoleh kunci private maka dilakukan proses algoritma enkripsi kunci sesi yang di input-kan oleh user. Kunci sesi tersebut secara otomatis digabungkan dengan waktu input, tanggal input, dan ID Processor. Algoritma pemangkitan kunci private dapat di lihat pada gambar 5.



Gambar 5. Algoritma pemrosesan kunci private[5]

Selanjutnya untuk mendapatkan kunci public maka akan dilakukan Enkripsi kunci private, untuk algoritma Enkripsi kunci private dapat diketahui dalam proses algoritma dibawah ini. Urutan pemrosesan kunci publik dapat dilihat pada gambar 6.

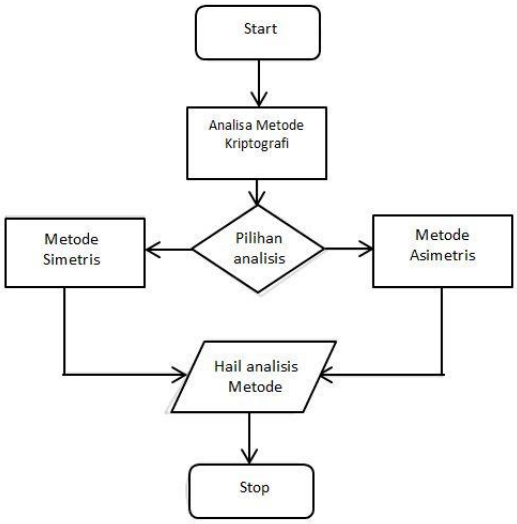


Gambar 6. Algoritma pemrosesan kunci publik[5]

METODE PENELITIAN

Perancangan Analisis

Pada analisis ini menggunakan pendekatan studi pustaka dengan beberapa hasil penelitian sebelumnya. Analisis pertama dengan menggunakan metode kriptografi Simetris kemudian dilakukan analisis metode Kriptografi Asimetris. Dalam analisis ini selanjutnya akan mengumpulkan informasi bagaimana tingkat keakuratan data yang telah dienkripsi, tingkat kesulitan, keamanan dan waktu yang dibutuhkan dalam prosesnya. Proses kerja yang dilakukan sebagaimana terlihat pada gambar flowchart di bawah ini. Pada metode Simetris digunakan Algoritma Asimetri RC-5, sedangkan pada metode Asimetri digunakan Algoritma yang dikembangkan oleh Munawar [5].



Gambar 7. Flowchart Analisis Kriptografi

Proses implementasi yang dilakukan untuk metode Simetri dengan Algoritma RC-5, dengan cara dibuat interaksi antara 2 buah PC (Personal Computer). Untuk PC pertama (client) akan menyiapkan data / plaintext yang akan diberikan ke PC kedua (server) dan data tersebut dienkripsi terlebih dahulu menggunakan metode RC-5 menjadi sebuah data chipertext sebelum dikirim ke jaringan internet. Setelah itu data ciphertext akan didekripsi

(P) ISSN 2442-451X
(O) ISSN 2503-3832

disisi server (PC2) sehingga data yang diterima oleh server akan kembali lagi seperti data awal atau kembali ke plaintext lagi.

Sementara itu pada Metode asimetri yang dikembangkan oleh Munawar dimulai dengan proses Enkripsi plaintext dengan menggunakan kunci publik. Dari proses enkripsi plaintext tersebut dibagi menjadi beberapa proses lagi, diantaranya proses algoritma pembangkitan cipherkey I, cipherkey II dan proses algoritma enkripsi plaintext. Kemudian dilanjutkan dengan proses dekripsi, tentunya dengan kunci yang berbeda (kunci private). Dalam proses dekripsi dari hasil enkripsi melewati beberapa tahapan algoritma dekripsi kunci. Sebelumnya hasil enkripsi berupa gabungan cipherkey II dan Ciphertext diuraikan menjadi komponen data yang terpisah, selanjutnya cipherkey II didekripsi dengan menggunakan kunci private. Ouput dari hasil dekripsi kunci private tersebut berupa cipherkey I. Cipherkey I digunakan untuk Dekripsi ciphertext, output dari hasil dekripsi tersebut berupa plaintext yang kita inginkan.

HASIL PENELITIAN

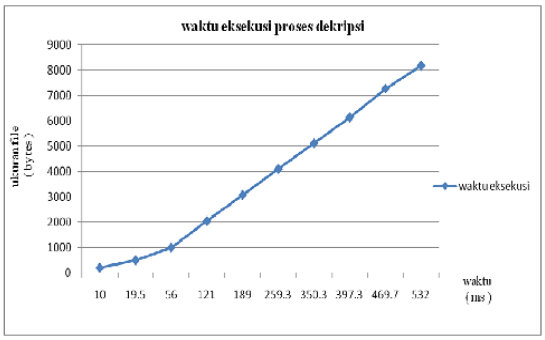
Implementasi Metode Simetris (Algoritma RC-5)

Pada tahap implementasi dilakukan pengujian analisis waktu, keberhasilan proses enkripsi dan dekripsi, dan keberhasilan pengembalian file yang telah dienkripsi (chiphertext) menjadi file semula (plaintext). Pada tahap pembangkitan kunci membutuhkan waktu antara 9 – 10 nano second, sedangkan waktu eksekusi pada proses enkripsi dilakukan 10 kali pengujian dengan menggunakan *file.txt* yang memiliki ukuran file yang berbeda beda. Sehingga hasil percobaannya dapat dilihat pada tabel 1 di bawah ini :

Tabel 1. Waktu eksekusi pada proses enkripsi [1]

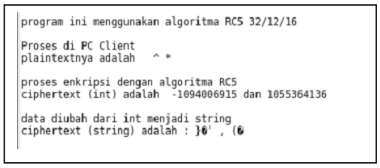
No	Nama file (.txt)	ukuran file (bytes)	Waktu Eksekusi Proses Enkripsi dalam millisecond										
		plaintext	1	2	3	4	5	6	7	8	9	10	average
1	data1	200	10	15	15	10	10	15	10	10	10	10	11.5
2	data2	500	20	15	20	20	20	20	15	20	20	20	19
3	data3	1000	46	50	50	50	60	50	50	50	50	50	50.6
4	data4	2049	140	110	120	110	120	130	110	130	110	130	121
5	data5	3076	171	180	190	190	180	198	175	187	180	171	182.2
6	data6	4104	234	250	250	240	270	230	250	270	256	245	249.5
7	data7	5121	296	343	343	335	302	330	331	320	312	320	323.2
8	data8	6144	353	358	375	365	379	382	383	370	378	388	373.1
9	data9	7275	420	440	456	455	482	477	457	423	455	470	453.5
10	data10	8189	479	510	483	540	468	508	512	475	458	480	491.3

Untuk proses dekripsi pengujiannya dilakukan cara yang sama dengan proses enkripsi, sehingga dari data tabel bisa digambarkan grafiknya sebagai berikut ini :

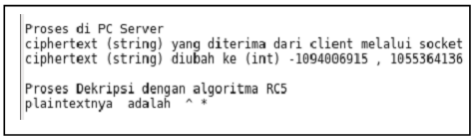


Gambar 8. Grafik waktu eksekusi proses dekripsi[1]

Pada pengujian keberhasilan enkripsi dan dekripsi file, karakter yang akan dikirimkan ke server, akan di enkripsi terlebih dahulu dengan sebuah kunci menjadi suatu ciphertext yang berupa data interger. Ketika akan dikirin ke server melalui jaringan internet menggunakan socket, data integer akan diubah terlebih dahulu menjadi data bertipe string.



Gambar 9. Proses enkripsi disisi client [1]



Gambar 10. Proses dekripsi disisi server [1]

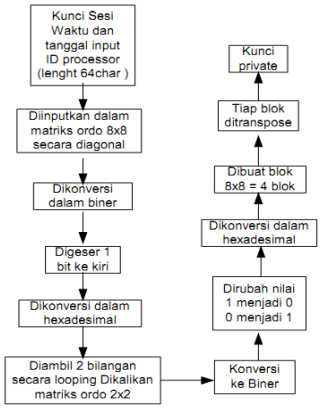
Pada pengujian keberhasilan proses enkripsi dan dekripsi RC-5 dengan metode operasi file, pengujiannya dilakukan dengan cara melakukan enkripsi file.txt yang berisi beberapa karakter dan akan menghasilkan file ciphertext.txt yang berisi beberapa karakter yang susah untuk dibaca. Sedangkan di proses dekripsi, file ciphertext.txt tadi didekripsi sehingga dapat menghasilkan file.txt kembali.

Implementasi Metode Asimetris (Algoritma Munawar)

Pemrosesan kunci private

Untuk dapat memperoleh kunci private maka dilakukan proses algoritma enkripsi kunci sesi yang di input-kan oleh user. Kunci sesi tersebut secara otomatis digabungkan dengan waktu input, tanggal input, dan ID Processor. Algoritma pembangkitan kunci private dapat di lihat pada gambar 11.

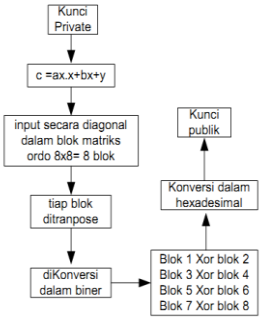
(P) ISSN 2442-451X
(O) ISSN 2503-3832



Gambar 11. Algoritma pemrosesan kunci private[5]

Pemrosesan kunci publik

Untuk dapat memperoleh kunci public maka akan dilakukan Enkripsi kunci private, untuk algoritma Enkripsi kunci private dapat diketahui dalam proses algoritma dibawah ini. urutan pemrosesan kunci publik dapat dilihat pada gambar 12.



Gambar 12. Algoritma pemrosesan kunci publik[5]

Pada pengujian program pada aplikasi yang dibuat dengan mencoba beberapa file dokumen, file gambar, suara, video dan lain-lain, dengan kapasitas berbeda dari yang terkecil sampai yang terbesar. di dapatkan data sebagai berikut :

Tabel 2. Pengujian program[5]

No	Nama file	Tipe file	Size KB	Waktu enkripsi (ms)	Size *cipher file* (KB)	Waktu Deskripsi (ms)
1	File 1	.txt	1	10	8	70
2	File 2	.txt	3	40	17	151
3	File 3	.wav	5	621	30	280
4	File 4	.jpg	11	9003	66	861
5	File 5	.doc	20	40188	188	1883
6	File 6	.doc	40	176213	239	2734
7	File 7	.doc	56	47197	338	4726
8	File 8	.bmp	87	1112480	521	32637
9	File 9	.doc	95	1113461	572	40619
10	File 10	.doc	111	189542	667	73656

Analisis Metode Simetris dan Asimetris

Dari implementasi yang dijelaskan sebelumnya untuk metode Simetris dan Asimetris maka berikut tabel analisis untuk kedua metode tersebut.

Tabel 3. Analisis metode Simetris dan Asimetris

Data	Metode											
	Enkripsi						Dekripsi					
	Simetris			Asimetris			Simetris			Asimetris		
	Size	Time (ms)	Time (byte)	Size	Time (ms)	Time (byte)	Size	Time (ms)	Time (byte)	Size	Time (ms)	Time (byte)
1	200	11.5	0.058	1024	10	0.01	0	0	0	8192	70	0.009
2	500	19	0.038	3072	40	0.013	1000	19.5	0.02	17408	151	0.009
3	1000	50.6	0.051	5120	621	0.121	2000	56	0.028	30720	280	0.009
4	2049	121	0.059	11264	9003	0.799	3000	121	0.04	67584	861	0.013
5	3076	182.2	0.059	20480	40188	1.962	4000	189	0.047	192512	1883	0.01
6	4104	249.5	0.061	40960	176213	4.302	5000	259.3	0.052	244736	2734	0.011
7	5121	323.2	0.063	57344	471979	8.231	6000	350.3	0.058	346112	4726	0.014
8	6144	373.1	0.061	89088	1112480	12.49	7000	397.3	0.057	533504	32637	0.061
9	7275	453.5	0.062	97280	1113461	11.45	8000	469.7	0.059	585728	40619	0.069
10	8189	491.3	0.06	113664	1895425	16.68	9000	532	0.059	683008	73656	0.108
	average		0.057	average		5.605	average		0.042	average		0.031

Rata-rata waktu yang dibutuhkan, untuk metode Simetris pada 1 byte data melakukan enkripsi sebesar 0.057 milisecond dan dekripsi 0.042 milisecond, sementara itu pada metode Asimetris pada 1 byte data melakukan enkripsi sebesar 5.605 milisecond dan dekripsi 0.031. Dengan rata-rata proses Kriptografi (enkripsi dan dekripsi) untuk metode Simetris sebesar 0.05 milisecond dan metode Asimetris sebesar 2.82 milisecond.

KESIMPULAN

Dari data hasil analisis dapat disimpulkan bahwa waktu komputasi antara enkripsi dan dekripsi berbanding lurus dengan penambahan besarnya file yang dioperasikan baik metode Simetris maupun Asimetris, namun menggunakan metode Simetris cenderung membutuhkan waktu komputasi yang lebih baik sehingga menjadi alternatif untuk sistem yang membutuhkan sistem distribusi data yang cepat, walaupun untuk metode Simetris akan sangat kompleks ketika terdapat banyak user untuk tiap pengiriman pesan karena dibutuhkan kunci yang berbeda pula, sehingga untuk masalah keamanan akan sangat merugikan dibanding menggunakan metode Asimetris.

Sistem pengamana data yang baik adalah ketika memiliki tingkat kompleksitas pemecahan kunci yang rumit. Penggunaan metode Simetris dan Asimetris secara sepihak pastinya memiliki kelebihan dan kelemahan, untuk itulah dalam pengembangan selanjutnya sebaiknya diterapkan suatu metode yang menggabungkan kedua konsep Kriptografi (*hybrid*) tersebut sehingga didapatkan suatu sistem keamanan data yang lebih baik, namun tentunya dengan penggabungan metode, waktu komputasi akan lebih lama, sehingga tantangan pengembangan selanjutnya adalah menghasilkan suatu penggabungan metode dengan waktu komputasi yang relatif kecil.

(P) ISSN 2442-451X
(O) ISSN 2503-3832

DAFTAR PUSTAKA

[1] Kurniawan A., Yuliana. M, Samsono .M.Zen., Hadi. Analisis dan Implementasi Sistem Keamanan Data dengan Menggunakan Metode Enkripsi Algoritma RC-5. Karya tidak diterbitkan. Surabaya : Jurusan Teknologi Telekomunikasi Politeknik Elektonika Negeri Surabaya.

[2] QUASIM, MD.TABREZ. 2013. Security Issues in Distributed Database System Model. COMPUSOFT. Vol II-XII : 396-399.

[3] Elyakim, Victor Asido., Utama, Afen Prana., Sitio, Arjon Samuel., Simbolon, John P., 2010. Pengamanan Database Menggunakan Metoda Enkripsi Simetri dengan Algoritma Feal: Studi Kasus Pemko Pematangsiantar. SNIKOM2010. 43-45.

[4] Arjana, Putu H., Rahayu, Tri Puji., Hariyanto, Yakub. 2012. Implementasi Enkripsi Data Dengan Algoritma Vigenere Chiper. SENTIKA. 2089-9815 : 164-169.

[5] Munawar. 2012. Perancangan Algoritma Sistem Keamanan Data Menggunakan Metode Kriptografi Asimetris. *KOMPUTA.* Vol I : 11-17.

[6] Suyanto. Metode Enkripsi Untuk Multiple Database Format Berbasis XML. Karya tidak diterbitkan. Palembang : Universitas Bina Darma.

[7] Sitinjak, Suriski., Fauziah, Yuli., Juwairiah. 201. Aplikasi Kriptografi File Menggunakan Algoritma Blowfish. semnasIF UPN "Veteran". C: 78-86.