PERANCANGAN ALGORITMA SISTEM KEAMANAN DATA MENGGUNAKAN METODE KRIPTOGRAFI ASIMETRIS

Munawar

Program Studi Teknik Informatika
Fakultas Teknik dan Ilmu Komputer Universitas Komputer Indonesia
Jl. Dipati Ukur No. 112-116 Bandung
Email : munawarhfz@gmail.com

ABSTRAK

Masalah keamanan, kerahasiaan, keaslian dan integritas data merupakan aspek-aspek penting yang perlu dilakukan untuk menjaga informasi dari pihak-pihak yang tidak memiliki otoritas atau hak akses. Untuk mengatasi hal ini, penulis mencoba mengimplementasikan konsep kriptografi pada sistem keamanan data pada jaringan komputer. Data-data elektronik dapat diamankan dengan cara mengubah data menjadi sandi-sandi yang tidak dimengerti.
Banyak algoritma kriptografi yang bisa diterapkan untuk mengamankan data, namun pada kesempatan kali ini penulis akan merancang algoritma tersendiri untuk mengatasi masalah keamanan data pada jaringan komputer. Cara efektif untuk menyembunyikan data atau informasi adalah dengan cara enkripsi

Kata Kunci : A*symmetric cryptosystem*, Enkripsi, Deskripsi, Kunci *Private*, Kunci *Public*, *Cipherkey I, Cipherkey II.*

1. PENDAHULUAN

a. Latar Belakang

Pada saat ini teknologi informasi sedang berkembang dengan pesat yang memungkinkan semua orang dapat berkomunikasi dari satu tempat ke tempat lain yang berjarak ribuan kilometer. Informasi yang dikirimkman itu menggunakan jalur transmisi telekomunikasi yang belum tentu dijamin kerahasiaannya. Bisa saja informasi yang sedang dikirim melalui media transmisi itu dicuri atau diubah oleh penyadap atau *cracker* untuk kepentingan tertentu.

Hal itu sedang menjadi masalah bagi dunia telekomunikasi terutama dalam pengiriman informasi penting yang memerlukan kerahasiaan yang tinggi seperti keuangan bank, informasi rahasia negara, dan informasi penting lainnya.

b. Identifikasi Masalah

Permasalahan yang akan terjadi pada skripsi yang penulis kerjakan diantaranya:

1. Rentannya sistem keamanan data pada jaringan komputer.
2. Adanya pihak yang tidak berhak untuk mengetahui privasi atau kerahasiaan data.
3. Sistem keamanan data yang mudah dipecahkan oleh pihak lain.
4. Sulitnya dalam merancang dan menginplementasikan sistem keamanan data.

c. Batasan Masalah

Luasnya suatu bahasan mengenai kriptosistem maka pada penulisan ini, penulis hanya membahas:

1. Merancang sistem keamanan data dengan memanfaatkan algoritma kriptografi.
2. Memilih dan menentukan algoritma kriptografi yang relatif sulit untuk dipecahkan oleh pihak lain.
3. Menginplementasikan dan menguji sistem keamanan data guna mengetahui keunggulan sistem yang dibuat.

d. Maksud dan Tujuan

Maksud dalam penulisan ini adalah merancang algoritma kriptografi asimetris, sedangkan tujuannya sebagai berikut:

a. Memunculkan kepedulian bagi para perancang sistem informasi terhadap keamanan data bahwa keamanan data merupakan bagian utama sistem yang patut untuk di perhitungkan.
b. Memunculkan ide atau metode baru bagi para perancang sistem informasi dalam mengamankan data atau informasi yang di kelolahnya.
c. Memberikan warna baru dalam ilmu penyandian data atau cryptography

2. LANDASAN TEORI

A. Kriptografi

Cryptography adalah cabang ilmu matematika tentang persandian untuk menjaga keamanan data. *Cryptographic system* atau *cryptosystem* adalah suatu fasilitas untuk mengkonversikan plaintext ke *ciphertext* dan sebaliknya. *Plaintext* adalah data asli, data yang masih bisa dibaca dan dimengerti. Sedangkan *ciphertext* adalah data yang tidak bisa dibaca maupun dimengerti.

Setiap *cryptosytem* yang baik harus memiliki karakteristik sebagai berikut

a. Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
b. *Cryptosystem* yang baik memiliki ruang kunci (*keyspace*) yang besar.
c. *Cryptosystem* yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.

B. Enkripsi dan Dekripsi

Enkripsi adalah suatu proses mengubah pesan atau data menjadi sandi yang merupakan salah satu proses dari kriptografi. Data yang disandikan berupa file sebagai input dan dengan menggunakan suatu kunci, file tersebut diubah menjadi file enkripsi yang tidak bisa dibaca. Adapun tujuan dari enkripsi ini adalah menyembunyikan data atau informasi dari orang tidak berhak.

Dekripsi adalah proses sebaliknya dari enkripsi yaitu mengembalikan sandi-sandi atau informasi yang telah dilacak ke bentuk file aslinya dengan menggunakan kunci pula.

Secara umum operasi enkripsi dan dekripsi dapat diterangkan secara matematis sebagai berikut:

EK (M) = C (Proses Enkripsi)

DK (C) = M (Proses Dekripsi)

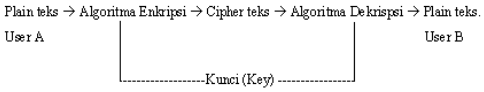
Pada saat proses enkripsi kita menyandikan pesan M dengan suatu kunci K lalu dihasilkan pesan C. Sedangkan pada proses dekripsi, pesan C tersebut diuraikan dengan menggunakan kunci K sehingga dihasilkan pesan M yang sama seperti pesan sebelumnya.

C. Penggolongan *Cryptographic system* (cryptosystem)

Suatu *cryptosystem* terdiri dari sebuah algoritma, seluruh kemungkinan plaintext, ciphertext dan kunci-kunci. Secara umum *cryptosystem* dapat digolongkan menjadi dua buah, yaitu :

a. Symmetric cryptosystem

Dalam *symmetric cryptosystem* ini, kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik, tetapi satu buah kunci dapat pula diturunkan dari kunci yang lainnya. Algoritma *symetric cryptosystem* dapat dilihat pada gambar 1.



Gambar 1. Model Symmetric cryptosystem

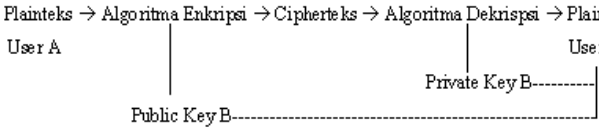
Kunci-kunci ini harus dirahasiakan. Oleh karena itulah sistem ini sering disebut sebagai *secret-key ciphersystem*. Jumlah kunci yang dibutuhkan umumnya adalah:

$$ {}_nC_2 = \frac{n(n-1)}{2} $$

dengan n menyatakan banyaknya pengguna. Contoh dari sistem ini adalah Data Encryption Standard (DES), Blowfish, IDEA.

b. *Assymmetric cryptosystem*

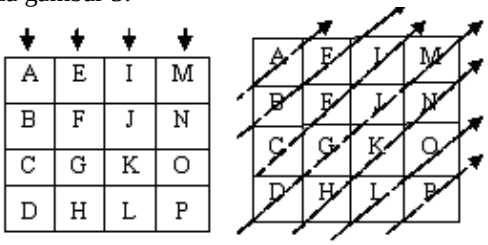
Dalam *assymmetric cryptosystem* ini digunakan dua buah kunci. Satu kunci yang disebut kunci publik (*public key*) dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (*private key*) harus dirahasiakan. Proses menggunakan sistem ini dapat diterangkan secara sederhana sebagai berikut : bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca surat tersebut, ia perlu mendekripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut, karena adanya mekanisme ini. Contoh sistem ini antara lain RSA Scheme dan Merkle-Hellman Scheme. Algoritma *assymmetric cryptosystem* dapat dilihat pada gambar 2.



Gambar 2. Model Asymmetric cryptosystem

D. Teknik substitusi

Masukan berdasarkan kolom kemudian keluarannya berdasarkan diagonal, dapat dijelaskan pada gambar 3.



Gambar 3. Model Teknik substitusi

E. Matriks

Matriks adalah kumpulan bilangan atau unsur yang disusun menurut baris dan kolom.

a. *Transpose* matriks

Transpose dari suatu matriks merupakan pengubahan baris menjadi kolom dan kolom menjadi baris. *Transpose* dari A dinotasikan dengan A^T atau A^t. Untuk lebih jelasnya dapat dilihat pada gambar 4..

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}_{mxn}$$

$$A^T = \begin{bmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & & a_{mn} \end{bmatrix}_{nxm}$$

Gambar 4. Model Transpose Matriks

b. Invers matriks

Matriks yang tidak singular mempunyai invers. Invers matriks A dinotasikan dengan A^{-1} dan secara umum dirumuskan dengan:

$$A^{-1} = \frac{1}{|A|} \text{(adjoint A)}$$

invers matriks ordo 2x2

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

jika maka

invers matriks A adalah:

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

F. Jaringan Komputer

Komunikasi merupakan masalah yang paling mendasar dalam sebuah jaringan, baik yang bentuknya suara, gambar atau data. Komunikasi adalah proses untuk menampilkan, merubah, menginterprestasikan atau mengolah sebuah informasi antara manusia atau mesin. Sedangkan jaringan komunikasi adalah suatu sistem yang terbentuk dari interkoneksi fasilitas-fasilitas yang dirancang untuk membawa trafik dari berbagai sumber telekomunikasi (komunikasi jarak jauh).

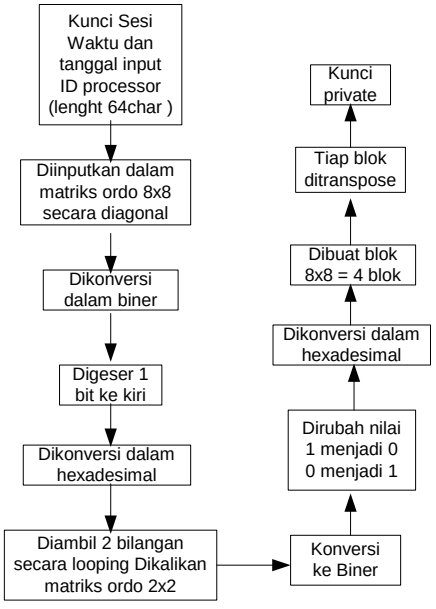
Ciri-ciri jaringan komputer:

a. Berbagi *hardware* dan *software*
b. Berbagi data dengan mudah
c. Berbagi saluran komunikasi
d. Memudahkan komunikasi antar pemakai jaringan

4. ANALISIS DAN PERANCANGAN

A. Pemrosesan kunci private

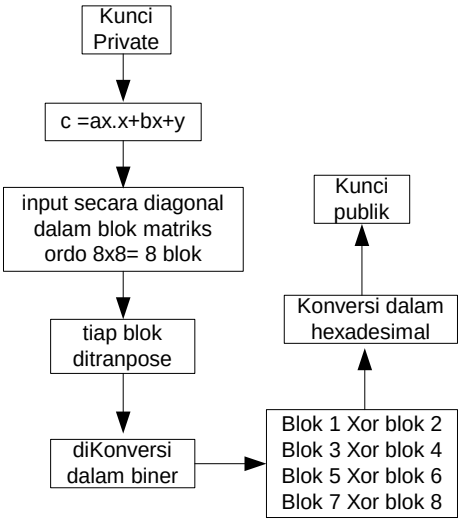
Untuk dapat memperoleh kunci *private* maka dilakukan proses algoritma *enkripsi* kunci sesi yang di *input*-kan oleh user. Kunci sesi tersebut secara otomatis digabungkan dengan waktu input, tanggal input, dan *ID Processor*. Algoritma pemangkitan kunci *private* dapat di lihat pada gambar 5.



Gambar 5. Algoritma pemrosesan kunci *private*

B. Pemrosesan kunci publik

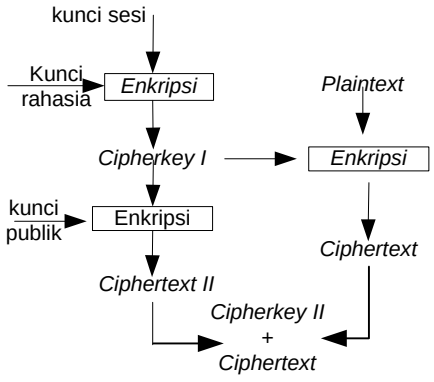
Untuk dapat memperoleh kunci *public* maka akan dilakukan Enkripsi kunci *private*, untuk algoritma Enkripsi kunci *private* dapat diketahui dalam proses algoritma dibawah ini. urutan pemrosesan kunci publik dapat dilihat pada gambar 6.



Gambar 6. Algoritma pemrosesan kunci publik

C. Proses Enkripsi data 2048 bit

Data atau *plaintext* sebesar 256 digit karakter atau 2048 bit akan dienkripsi melalui proses algoritma enkripsi *plaintext* seperti yan\g terlihat pada gambar 7.

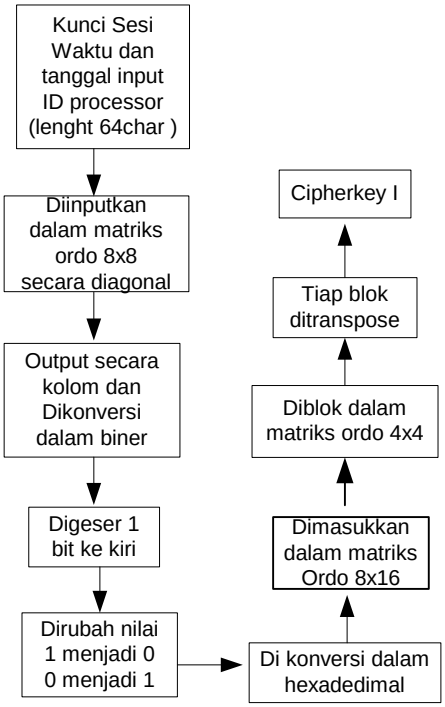


Gambar 7. Model Enkripsi data 2048 bit

Dari proses enkripsi *plaintext* tersebut dibagi menjadi beberapa proses lagi, diantaranya proses algoritma pembangkitan *cipherkey I*, *cipherkey II* dan proses algoritma enkripsi *plaintext.* Ketiga algoritma tersebut akan diuraikan secara rinci pada pembahasan berikut.

1. Pembangkitan *Cipherkey I*

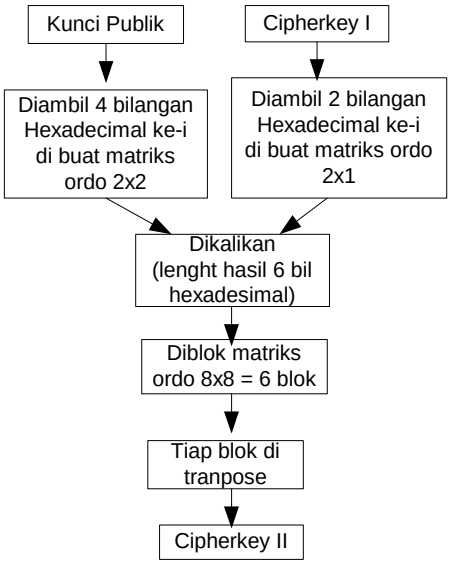
Algoritma proses pembangkitan *cipherkey I* dapat dilihat pada gambar 8.



Gambar 8. Algoritma Pembangkitan *Cipherkey I*

2 . Enkripsi Cipherkey I

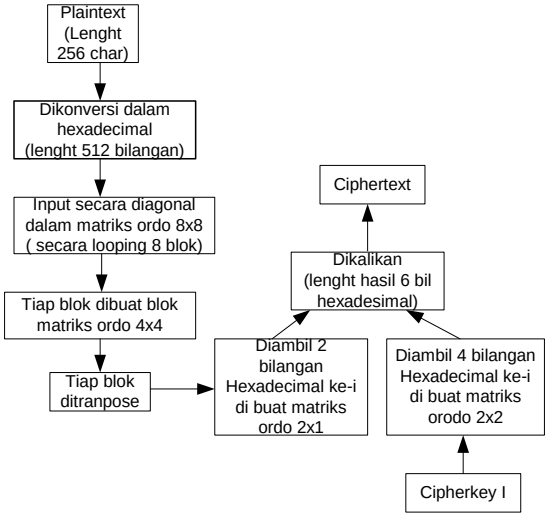
Algoritma proses enkripsi *cipherkey I* untuk menghasilkan *cipherkey II* dapat dilihat pada gambar 9.



Gambar 9. Algoritma Enkripsi *Cipherkey I*

3. Enkripsi Plaintext

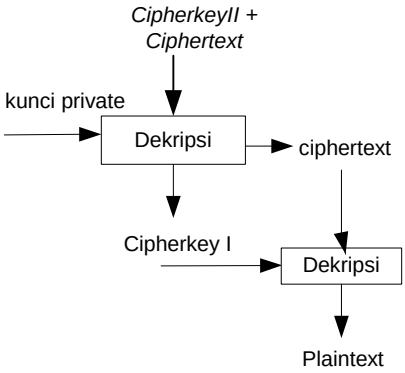
Algoritma proses enkripsi *plaintext* untuk menghasilkan *ciphertext* dapat dilihat pada gambar 10.



Gambar 10. Algoritma Enkripsi *Plaintext*

D. Proses Dekripsi

Proses dekripsi merupakan kelanjutan dari proses enkripsi, proses dekripsi merupakan kebalikan dari proses enkripsi yaitu merubah ciphertext yang dihasilkan oleh proses enkripsi menjadi plaintext yang diinginkan. Alur proses dekripsi dapat dilihat pada gambar 11.



Gambar 11. Model propses deskripsi

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.

Urutan algoritma dekripsi gabungan *cipherkey II* dan *Ciphertext* adalah sebagai berikut:

1. Dekripsi kunci private
2. Pengujian kunci public, dengan cara membandingkan hasil enkripsi kunci private dengan kunci public yang di gunakan user dalam melakukan enkripsi *plaintext.*
3. Dekripsi cipherkey II
4. Dekripsi ciphertext.

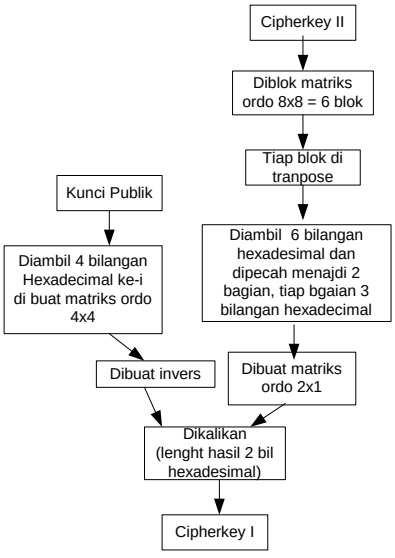
1. Dekripsi Kunci *Private*

Algoritma dekripsi kunci *private* dapat dilihat pada gambar 11.

Gambar 11. Algoritma Deskripsi Kunci *Private*

2. Dekripsi *Cipherkey II*

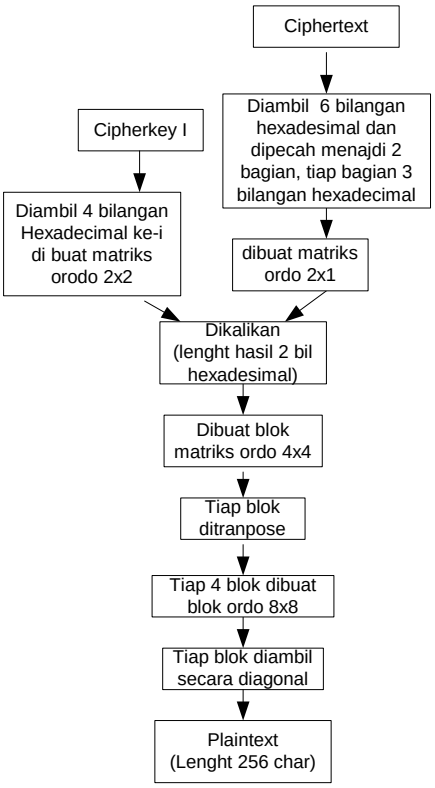
Algoritma proses dekrispi *cipherkey II* dapat dilihat pada gambar 12.



Gambar 12. Algoritma deskripsi *ciphertext II*

3. Dekripsi Ciphertext

Algoritma dekripsi ciphertext dapat dilihat pada gambar 13.



Gambar 13. Algoritma Deskripsi Ciphertext

5. PENGUJIAN PROGRAM

Dengan program aplikasi yang dibuat penulis mencoba beberapa file dokumen, file gambar, suara, video dan lain-lain, dengan kapasitas berbeda dari yang terkecil sampai yang terbesar.

Pada saat melakukan pengujian program, program yang diaktifkan bersamaan dengan program aplikasi kriptografi adalah program *Winamp* dan program *windows explorer*.
Waktu pembangkitan kunci *private* dan publik adalah 10 ms dengan size 1 KB.

Tabel 1. Pengujian program

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	1895425	667	73656

Dari data table 1 dapat disimpulkan bahwah:

1. Semakin besar size *plainfile* (file asli yang akan dienkripsi) semakin lama waktu enkripsi dan dekripsi dibandingkan dengan size *plainfile* yang lebih kecil.
2. Size kunci atau panjang kunci selalu tetap.
3. Size *cipherfile* (file hasil enkripsi) lebih besar beberapa kali lipat dari size *plainfile*.
4. Waktu enkripsi relatif lebih lama dibandingkan dengan waktu dekripsi.
5. Secara umum beban kerja komputer juga memperngaruhi lamanya pemrosesan enkripsi atau dekripsi suatu file.
6. Selain itu konfigurasi komputer, seperti *processor*, *hardisk*, dan *random access memory* (RAM) merupakan perangkat yang sangat mempengaruhi proses. Seemakin tinggi teknologi yang digunakan semakin cepat pula proses enkripsi dan dekripsi dilakukan.

6. KESIMPULAN

Aplikasi yang penulis buat berfungsi utnuk merubah sebuah data elektronik menjadi sandi-sandi yang tidak dapat dibaca sehingga kerahasiaannya dapat dijaga. Berdasarkan hasil analisa, perancangan, implementasi dan pengujian program, maka dapat diambil beberapa kesimpulan diantaranya:

1. Algoritma kriptografi ini dibuat dan dirancang sendiri oleh penulis untuk dapat diterapkan pada program aplikasi, sehingga memiliki kelebihan dalam pengamanan data atau informasi. Hal ini dikarenakan data hasil enkripsi sangat sulit untuk dimengerti dan diterjemahkan, karena banyaknya operasi logika yang harus dilewati serta algoritma yang dibuat masih belum terpublikasi secara umum.
2. Kerahasiaan kunci lebih terjaga karena menggunakan konsep kriptografi asimetris, memiliki kunci private dan kunci publik yang memiliki fungsi yang berbeda. Dan juga didukung oleh panjang kunci *private* yang relatif lebih panjang yaitu 1024 bit
3. Algoritma yang dibuat mengunakan kombinasi kunci yang sulit terprediksi, dikarenakan dalam membuat kunci *private* dan kunci publik menggunakan kombinasi

kunci sesi yang diinputkan user, waktu dan tanggal input serta *ID processor*. Sehingga pada waktu akses serta pada komputer yang berbeda dapat menghasilkan kunci yang berbeda pula meskipun dengan inputan kunci sesi yang sama.

4. Program dibuat sesederhana mungkin, sehingga user bisa dengan mudah mengenali setiap fungsi dari tombol-tombol yang digunakan dalam aplikasi ini.
5. Program kriptografi ini bisa digunakan untuk melakukan enkripsi semua file misalnya gambar, dokumen, audio maupun video dan juga jenis file yang lain.
6. Program yang dibuat dapat diimplementasikan pada sebuah jaringan (LAN). Sehingga program ini bisa dipakai untuk melindungi data, baik yang ada dikomputer server maupun di komputer client.

DAFTAR PUSTAKA

[1] Y. Kurniawan, (2004). "Kriptografi Keamanan Internet dan Jaringan komunikasi," Informatika, Bandung.
[2] Kristanto, (2003). "Keamanan Data Pada Jaringan Komputer," Gava Media, Yogayakarta.
[3] B Schneier, (1996). "Applied Cryptography," john Wiley and Sons, Inc. New York.
[4] T. Juhana "Cryptrography," Telematics Laboratory EE Dept. ITB, Bandung.
[5] T. Heriyanto, (1999). "Pengenalan Kriptografi," Internet.
[6] L.E. Nugroho, "Keamanan Sistem Informasi," Jurusan Teknik Elektro
[7] Fakultas Teknik UGM, Yogyakarta.
[8] J. Yuliantoro Dan O. W. Purbo "PGP sebagai Pengaman E-Mail Anda," Computer Network Research Group ITB, Bandung..
[9] J. Chai, M. Leung, M. Ducott, W. Yuen, (2001). "Cryptography on the Internet," Computer Communications and Networking ENG SC546.