Analisis Keamanan Sistem Informasi Dengan Metode Enkripsi Menggunakan Algoritma *Blowfish*

I. Hendrawan[1] Febrianty[1], A. Eka[1], B. Irawan[1], Irzaman[2]
[1] Jurusan Teknik Informatika, FT, Jl. Dipatiukur Bandung
[2] Jurusan Fisika, FMIPA IPB, Jl. Raya Pajajaran Bogor

Abstract
Security aspect represent one of the most important aspect in information system. One of the mechanism done to do this security is by cryptography technique with encryption method using blowfish algorithm. Blowfish created to replace DES. Basically, blowfish algorithm will change an information with encription massage in order can't read by side who want to access and damage the information. Blowfish algoritm are one of simetrik cryptographt system where used the same key for encryption and decription. Blowfish algorithm are one of block cipher method in modern cryptography bit basis.

Abstrak
Dalam suatu sistem informasi Aspek keamanan merupakan salah satu aspek yang sangat penting. Salah satu mekanisme yang dilakukan untuk melakukan pengamanan ini adalah dengan teknik kriptografi dengan metode enkripsi menggunakan algoritma *blowfish. Blowfish* dirancang untuk menggantikan *DES.* Pada dasarnya, algoritma *blowfish* akan mengubah sebuah informasi dengan cara mengenkripsi pesan sehingga tidak dapat dibaca oleh pihak yang ingin mengakses dan merusak informasi tersebut. Algoritma *blowfish* merupakan salah satu sistem kriptografi simetrik dimana menggunakan kunci yang sama baik untuk proses enkripsi maupun dekripsi. Algoritma *blowfish* merupakan salah satu bentuk metode *block cipher* dalam kriptografi modern berbasis bit.

1. Pendahuluan

Kemajuan di bidang telekomunikasi dan komputer telah memungkinkan seseorang untuk melakukan transaksi dan pengiriman informasi kepada pengguna lainnya secara jarak jauh.

Kegiatan-kegiatan tersebut tentu saja akan menimbulkan resiko bilamana informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak. Misalnya, informasi mengenai nomor kartu kredit, bila informasi ini jatuh kepada orang-orang yang jahat maka informasi mengenai kartu kredit tersebut dapat diakses dan disalah gunakan oleh orang-orang tidak berhak .

Sebelum tahun 1970-an, teknologi kriptografi digunakan terbatas hanya untuk tujuan militer dan diplomatik. Akan tetapi kemudian bidang bisnis dan perorangan mulai menyadari pentingnya melindungi informasi berharga.

Dengan berkembangannya sistem komputer dan interkoneksinya melalui jaringan *on-line,* tentu saja hal ini membutuhkan sistem keamananan informasi yang handal. Untuk mengamankan informasi tersebut diperlukan teknik

kriptografi dengan metode enkripsi untuk melindungi informasi-informasi yang berharga. Tujuan dari penelitian yaitu untuk menganalisa keamanan sistem informasi menggunakan teknik kriptografi dengan metoda enkripsi algoritma *Blowfish.*

2. Metodologi

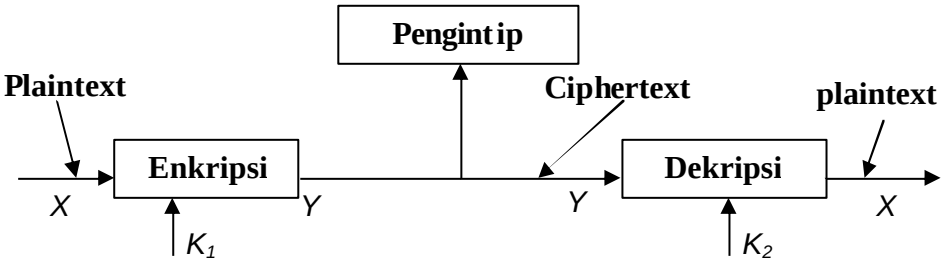
Dalam pelaksanaannya, penelitian dilakukan di jurusan teknik informatika UNIKOM, terhitung mulai bulan Januari 2004 sampai dengan bulan Juni 2004.

Metode yang digunakan dalam penelitian ini adalah dengan metode deskriptif yaitu melalui studi pustaka dan dokumenter dari berbagai buku atau literatur yang berhubungan dengan obyek penelitian yang dilakukan termasuk data dari internet. Data dan fakta yang berupa pemikiran, teori, konsep atau penelitian sebelumnya yang akan dikemukakan berbagai sumber, dianalisa sehingga tujuan dari penulisan tugas akhir ini tercapai.

Alat dan istrumen yang digunakan dalam penelitian antara lain : seperangkat komputer AMD Athlon XP 1700 MHz, Memori 256, monitor 15 inci dan printer canon BJC 210's, serta perangkat lunak menggunakan sistem operasi Windows XP Proffesional dan program simulasi dengan menggunakan teknik kriptografi algoritma *blowfish.*

3. Hasil dan Pambahasan

Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. (*Cryptography is the art and science of keeping messages secure.*) "*Crypto*" berarti "*secret*" (rahasia) dan "*graphy*" berarti"*writing*" (tulisan) [B. Raharjo, 2001].). Para pelaku atau praktisi kriptografi disebut *cryptographers*. Sebuah algoritma kriptografik (*cryptographic algorithm*), disebut *cipher*, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat.



Gambar 1 Proses Enkripsi dan Dekripsi dengan Kunci

Blowfish adalah *cipher* blok simetri yang dapat digunakan sebgai pengganti DES atau IDEA. *Blowfish* didesain pada tahun 1993 oleh Bruce

Schneier sebagai alternatif algoritma kriptografi yang cepat (*fast*) dan bebas (*free*). Algoritma ini tidak dipatenkan dan berlisensi *free*.

Enkripsi algoritma *blowfish* terdiri dari sebuah jaringan feistel dengan iterasi sebanyak 16 putaran. Setiap putaran mempunyai sebuah permutasi *key-dependent*, sebuah substitusi-*key* dan substitusi *data-dependent*. Semua operasi penjumlahan dan XOR pada karakter 32 bit.

P-array mempunyai 18 *subkey* 32-bit:

$P_1, P_2, P_3, \ldots\ldots\ldots\ldots\ldots\ldots P_{18}$

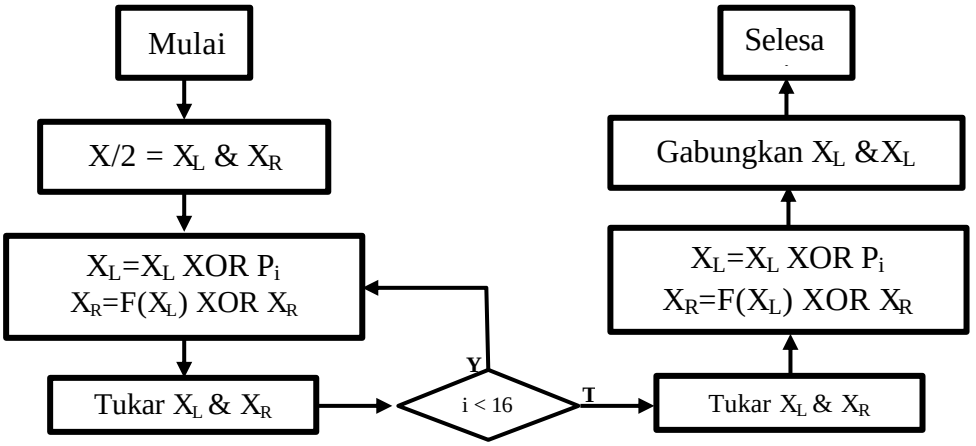
Empat S-box 32- bit mempunyai masing-masing 256 entry, yaitu:

$S_{1,0}, S_{1,1}, S_{1,2}, S_{1,3}, \ldots\ldots\ldots\ldots S_{1,255}$
$S_{2,0}, S_{2,1}, S_{2,2}, S_{2,3}, \ldots\ldots\ldots\ldots S_{2,255}$
$S_{3,0}, S_{3,1}, S_{3,2}, S_{3,3}, \ldots\ldots\ldots\ldots S_{3,255}$
$S_{4,0}, S_{4,1}, S_{4,2}, S_{4,3}, \ldots\ldots\ldots\ldots S_{4,255}$

Enkripsi Algoritma *Blowfish*

Blowfish adalah sebuah jaringan *Feistel* yang mempunyai 16 *round*. masukannya adalah (X) element data 64-bit. Untuk mengenkripsi (X) yaitu :

(X) dibagi kedalam dua bagian 32-bit (X_L dan X_R).
Untuk i = 1 sampai 16 maka :
$X_L = X_L$ XOR P_i
$X_R = F(X_L)$ XOR X_R
Swap (tukar) X_L dan X_R
Swap (tukar) X_L dan X_R (mengulang *swap* yang lalu)
$X_R = X_R$ XOR P_{17}
$X_L = X_L$ XOR P_{18}
Gabungkan kembali X_L dan X_R



Gambar 2 diagram alir algoritma *blowfish*

Gambar 2 menunjukan Blok diagram Algoritma Enkripsi *Blowfish* dengan deskripsi sebagai berikut, 64-bit pesan yang pertama dibagi menjadi 2 bagian, 32-bit elemen kiri dan 32-bit elemen kanan. XOR-kan 32-bit elemen kiri yang pertama dengan sub-kunci yang pertama, kemudian kenakan elemen kiri dengan fungsi F dan hasilnya XOR-kan dengan 32-bit elemen kanan, kemudian tukarkan elemen kanan dan elemen kiri untuk melanjutkan ke-iterasi berikutnya. Seluruh proses dari algoritma ini terdiri dari 16 iterasi dengan menggunakan sub kunci P1 sampai P18, pada iterasi ke-16 terjadi dua kali pertukaran elemen kanan dan kiri, dengan kata lain pada iterasi ini tidak ada pertukaran elemen kanan dan kiri,kemudian gabungkan kembali elemen kanan dan kiri untuk menghasilkan suatu *ciphertext* 64-bit.

Dekripsi Algoritma *Blowfish*

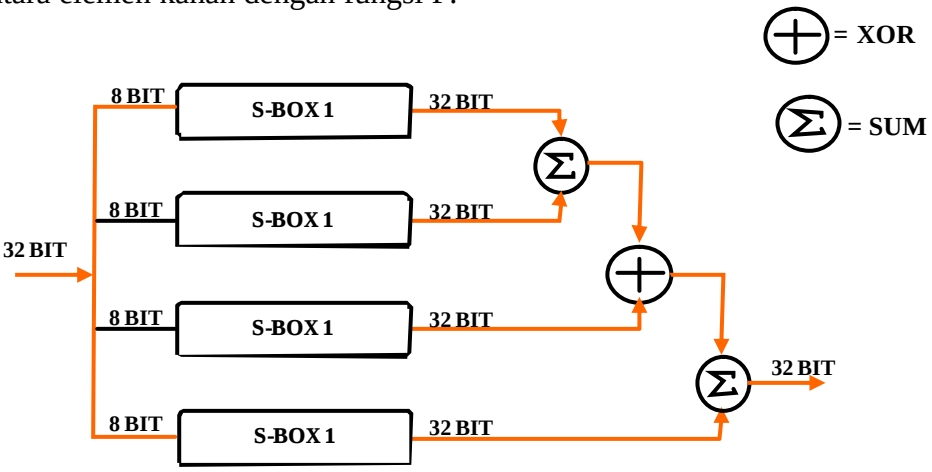
Proses dekripsi sama persis dengan proses enkripsi, kecuali bahwa P_1, P_2,…, P_{18} digunakan pada urutan yang terbalik.

Fungsi F

Bagi X_L dalam empat kuarter 8-bit (a, b, c dan d)

$$F(X_L) = ((S_{1,a} + S_{2,b} \bmod 2^{32}) \oplus S_{3,c}) + S_{4,d} \bmod 2^{32}$$

Gambar 3 menunjukan fungsi F dengan deskripsi sebagai berikut, 32-bit elemen kiri dibagi menjadi 4 X 8 bit, fungsi F merupakan array 2 dimensi yang ditunjukan pada algoritma diatas, dimana S-BOX 1 menjadi elemen x dan 8-bit pertama menjadi elemen y, S-BOX 2 menjadi elemen x dan 8-bit kedua menjadi elemen y, dan seterusnya sampai elemen ke-4, empat bagian tersebut menghasilkan keluaran masing-masing 32-bit, 32-bit pertama dijumlahkan dengan 32-bit bagian kedua, keluarannya di-XOR-kan dengan 32-bit bagian ketiga, dan keluarannya dijumlahkan lagi dengan 32-bit bagian keempat menghasilkan 32-bit keluaran. Keluaran tersebut digunakan untuk masukan pada operasi pengXOR-an antara elemen kanan dengan fungsi F.



Gambar 3 Diagram Fungsi F

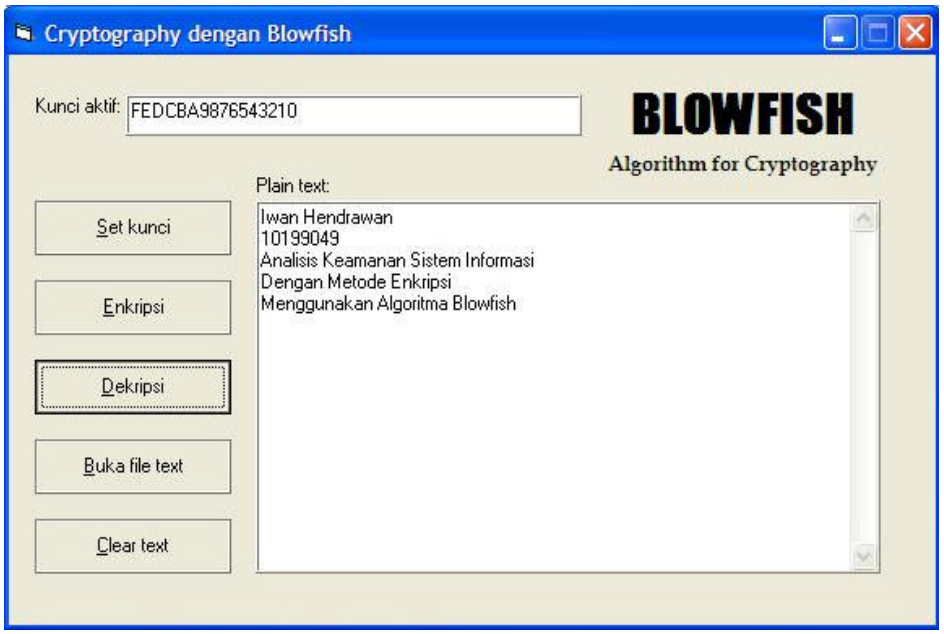
Untuk melakukan simulasi sistem keamanan informasi ini hanya dibatasi dengan memakai sebuah program kriptografi pada sebuah komputer otonom yang dirancang menggunakan *Visual Basic* 6.0 dengan menggunakan metode enkripsi/dekripsi algoritma *blowfish*. Program tersebut digunakan untuk mengubah sebuah plainteks (text yang dapat dibaca) menjadi sebuah cipherteks (text yang tidak dapat dibaca) dan sebaliknya, proses pengubahan plainteks menjadi cipherteks disebut enkripsi, sedangkan proses pengubahan cipherteks menjadi plainteks disebut dekripsi Pada program simulasi tersebut menggunaan kunci simetrik atau kunci konvensional dimana kunci yang digunakan untuk mendekripsi sama dengan kunci yang digunakan untuk mengenkripsi.

Program simulasi

Program simlasi ini dirancang dengan menggunakan *Visual Basic* 6.0, dan digunakan sebagai alat (*tools*) untuk keperluan penelitian dalam tugas akhir ini. Program tersebut menggunakan teknik kriptografi dengan metode enkripsi/dekripsi menggunakan algoritma *blowfish*.

Pada form utama program simulasi seperti yang ditunjukan pada gambar 4 menampilkan fungsi fungsi dari tombol untuk megoperasikan program smulasi tersebut, diantaranya adalah:

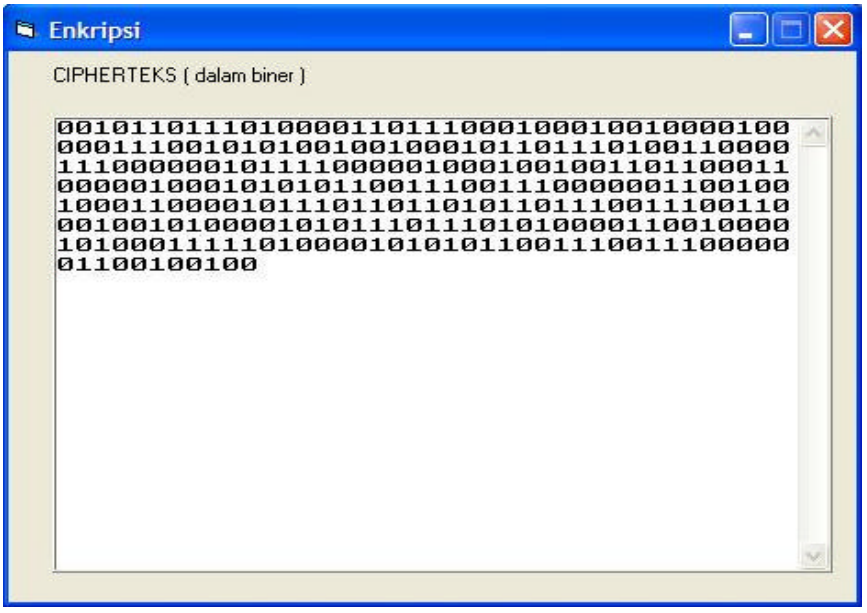
a. *Text box* kunci, *Text box* kunci ini digunakan untuk memasukan kunci yang akan digunakan dalam proses enkripsi dan dekripsi pesan.
b. *Text box* kunci aktif, text box ini merupakan sebuah kunci masukan yang akan digunakan pada proses enkripsi dan dekripsi.
c. *Text Box* Plainteks, *text box* ini digunakan untuk menyimpan tulisan atau *file* yang akan dienkripsi
d. tombol set kunci digunakan untuk mengaktifkan kunci yang dimasukan pada *text box* kunci yang kmudian akan ditampilkan pada *text box* kunci aktif.
e. Tombol Enkripsi, tombol ini digunakan untuk memulai proses enkripsi, hasil proses enkripsi akan ditampilkan pada *form* enkripsi (gambar 4.2)
f. Tombol Dekripsi, tombol ini digunakan untuk memulai prosse dekripsi, hasil proses dekripsi akan ditampilkan pada *form* dekripsi (gambar 4.3)
g. Tombol Buka *File*, tombol ini digunakan untuk membuka *file* yang berekstensi .txt untuk dienkripsi.
h. Tombol *Clear Text*, tombol ini digunakan untuk menghapus tulisan atau file yang ada pada *text box* Plainteks.



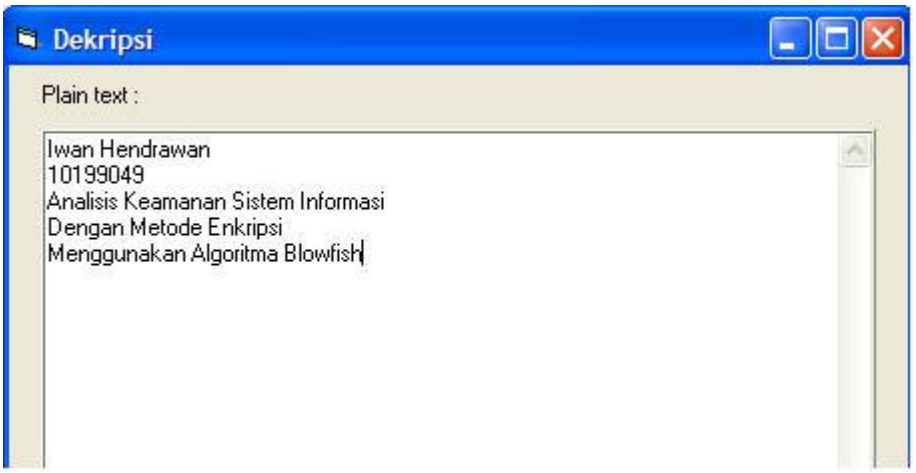
Gambar 4 Form Utama dari Program Simulasi

Pada *Form* Enkripsi program simulasi akan menampilkan hasil keluaran dari proses enkripsi yang dilakukan, hasil keluaran yang dikeluarkan, *form* ini mempunyai dua bentuk keluaran, seperti yang ditunjukan pada gambar 5 yaitu:

a. Cipherteks, yaitu hasil keluaran enkripsi dengan format data enkripsi yang dikonversikan kedalam bentuk yang tidak dapat dimengerti.
b. Hexadesimal, yaitu hasil keluaran proses enkripsi dengan format data enkripsi dalam bentuk hexadesimal.



Gambar 5 *Form* Enkripsi Algoritma *Blowfish*



Gambar 6 *Form* Dekripsi Algoritma *Blowfish*

Pada *Form* Dekripsi program simulasi akan menampilkan data hasil keluaran dekripsi dalam bentuk plainteks, seperti yang ditunjukan oleh gambar 6.

4. Kesimpulan

Adapun kesimpulan yang dapat penulis ambil diantaranya kekurangan dan kelebihan dari algoritma *blowfish*, diantaranya :

1. Kelebihan
   a. Masukan dari plainteks terdistribusi merata dalam beberapa simbol cipherteks. Sebuah blok cipherteks dapat mewakili beberapa kemungkinan plainteks.
   b. Karena yang dienkripsikan berupa blok-blok, maka tidak mungkin untuk dilakukan penyisipan terhadap bagian blok karena akan menyebabkan panjang blok berubah atau akan terjadi kesalahan pada proses dekripsi.
2. Kekurangan
   a. Proses enkripsi lambat, Cipher blok harus menunggu sampai seluruh blok simbol plainteks telah diterima untuk dilakukan proses enkripsi.
   b. Suatu *error* pada proses enkripsi akan mengimbas terhadap seluruh karakter pada blok yang sama sehingga akan mengubah makna dari cipherteks yang dihasilkan. Pada proses dekripsi, plainteks yang dihasilkan akan berubah karena cipherteks yang dihasilkan pada proses enkripsi terjadi eror dan akan mengubah makna dari cipherteks tersebut sehingga pada waktu proses dekripsi, plainteks yang dihasilkan tidak akan kembali seperti plainteks awal.

Daftar Pustaka

Anonymous, Memahami Kriptografi, 2003.

Anonymous. *Sekilas Tentang Enkripsi*, NeoTek, halaman 30, 2002.

B. Galtiff, "Encrypting data With The Blowfish Algorithm", 2003.

B. Raharjo, " Keamanan sistem informasi Berbasis Internet " PT Insan komunika/Infonesia Bandung, 2001.

B. Schneier, A short summary of Blowfish Algorithm : Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) by Bruce Schneier, 2001

B. Schneier, The Blowfish Encryption Algorithm - - One Year Later, Dr. Dobb's Journal, September 1995

B. Schneier,"Applied Criptography: Protocols, Algoritms, and Source Code in C," second edition, John Wiley & Sons, Inc., 1996.

B. Sukmawan, "Keamanan Data dan Metode Enkripsi", edisi Jan. 1998.

T. Hariyanto, "Pengenalan Kriptografi", edisi Juni 1999.

W. Stallings, Network and Internetwork Security Principles and Practice, New Jersey, Prectice-Hall, 1995.