ISSN : 2548-6985

Analisa Perancangan Aplikasi Penyandian Pesan Pada Email Menggunakan Algoritma Kriptografi Blowfish

Achmad Fauzi
STMIK KAPUTAMA, Jl. Veteran No. 4A-9A, Binjai, Sumatera Utara, Indonesia
Email : fauzyrivai88@gmail.com

ABSTRAK

Teknologi informasi dan komunikasi yang cepat banyak memberikan keuntungan bagi setiap orang untuk saling tukar-menukar informasi terlebih lagi dalam dunia bisnis. Seperti dalam mengirim data-data yang penting, sedemikian sehingga untuk mengirim data tidak perlu lagi datang langsung ke tempat yang ingin dituju, melainkan cukup dengan menggunakan pengiriman dengan fasilitas internet menggunakan email. Kriptografi merupakan teknik yang dapat melindungi kerahasiaan dari orang yang tidak bertanggung jawab. Pada skripsi ini dibentuk suatu aplikasi yang bertujuan mengamankan data yang dikirim melalui email dari gangguan penyadap yang berniat merusak data atau informasi. Adapun dalam penelitian ini penulis menggunakan algoritma blowfish dimana algoritma tersebut merupakan sebuah algoritma kunci simetri blok kode dengan panjang blok tetap 64 bit, dan algoritma blowfish dibagi menjadi dua subalgoritma utama yaitu ekspansi kunci dan bagian enkripsi-dekripsi. Sehingga proses pengiriman file yang di lakukan dengan menggunakan email dapat terjaga kerahasiannya.

Kata kunci: Security, Kriptografi, Blowfish, Email.

PENDAHULUAN

Teknologi informasi dan komunikasi yang cepat banyak memberikan ke untungan bagi setiap orang untuk saling tukar-menukar informasi terlebih lagi dalam dunia bisnis. Seperti dalam mengirim data-data yang penting, sedemikian sehingga untuk mengirim data tidak perlu lagi datang langsung ke tempat yang ingin dituju, melainkan cukup dengan menggunakan pengiriman dengan fasilitas internet menggunakan email[5].

Akan tetapi, perlu disadari bahwa dalam proses pengiriman data yang dilakukan dengan menggunakan email, pada dasarnya melakukan pengiriman data tanpa melakukan pengamanan terhadap data tersebut. Sehingga ketika dilakukan penyadapan pada jalur pengiriman data tersebut, maka data yang disadap dapat langsung dilihat dan dibaca serta dapat dimanipulasi keaslian datanya.

Untuk menghindari kemungkinan penyadapan data dari pihak yang tidak bertanggung jawab, sehingga data tersebut dapat langsung dilihat dan dibaca serta dapat dimanipulasi keaslian datanya oleh penyadap, maka data yang akan dikirim terlebih dahulu diacak dengan metode penyandian. Sehingga ketika data yang dikirim tersadap oleh penyadap, maka seorang penyadap tidak dapat melihat dan membaca serta memanipulasi data tersebut.

Teknik kriptografi merupakan teknik yang dapat melindungi kerahasian data agar terhindar dari orang yang tidak berhak. Teknik ini memiliki dua konsep utama yaitu enkripsi dan dekripsi. Enkripsi merupakan proses menyandikan plaintext menjadi chipertext dengan mengubah pesan menjadi bentuk yang lain agar tidak dikenali secara langsung, sedangkan dekripsi merupakan proses mengembalikan ciphertext menjadi plaintext. Proses enkripsi dan dekripsi juga membutuhkan kunci sebagai parameter yang digunakan untuk transformasi. Salah satu metode dalam kriptografi yaitu metode *Blowfish*.

Kriptografi berasal dari bahasa yunani, menurut bahasa dibagi menjadi *kripto* dan *graphia,* kripto berarti rahasia dan graphia berarti tulisan. Sehingga kata kriptografi dapat diartikan sebagai “tulisan yang tersembunyi”. Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain[1].

Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu:

1. Enkripsi: merupakan pesan asli disebut juga *plaintext*, yang diubah menjadi kode-kode yang tidak dimengerti atau disebut juga *chipertext*.
2. Dekripsi: merupakan kebalikan dari enkripsi, yaitu pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks asli).
3. Kunci : adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci juga terbagi menjadi dua bagian, yaitu

ISSN : 2548-6985

kunci rahasia (*private key*) dan kunci umum (*public key*)[1], seperti yang terlihat pada Gambar 1 berikut.

Gambar 1. Konsep Enkripsi dan Dekripsi[1]

Algoritma Blowfish

Blowfish merupakan algoritma kunci simetri blok kode yang dirancang untuk menggantikan DES. Pada saat itu banyak sekali rancangan algoritma yang ditawarkan, namun hmpir semua terhalang oleh paten atau kerahasiaan pemerintah Amerika. Schneier menyatakan bahwa blowfish bebas hak paten dan akan diletakan pada domain publik. Dengan pernyataan Schneier tersebut blowfish telah mendapatkan tempat di dunia kriptografi, khususnya bagi masyarakat yang membutuhkan algoritma kriptografi yang cepat, kuat dan tidak terhalang oleh lisensi[7].

Keberhasilan blowfish dalam menembus pasar telah terbukti dengan diadopsinya blowfish sebagai Open Cryptography Interface (OCI) pada kernel linux versi 2.5 ke atas. Dengan diadopsinya blowfish berarti dunia opern source menganggap blowfish adalah salah satu algoritma yang terbaik.

a. Cara kerja Algoritma Blowfish

Adapun cara kerja algoritma blowfish pertama dilakukan pengekspansian kunci terhadap P-box sehingga P-box menjadi termodifikasi dengan kunci. Setelah pengekspansi kunci selesai maka dilakukan proses enkripsi dan dekripsi terhadap data yang ingin kita enkripsikan maupun didekripsikan. Data yang ingin di enkripsikan maupun didekripsikan diambil perblok dari setiap data dan memiliki panjang blok tetap 64 bit. Kemudian, data tersebut dibagi menjadi 2 bagian, bagian kiri(xl) dan bagian kanan(xr) dengan besaran masing-masing 32 bit. dalam proses enkripsi dan dekripsi ada yang dinamakan fungsi F dimana fungsi F tersebut membagi (xl) 32 bit menjadi 4 bagian masing-masing 8 bit. Adapun proses enkripsi dan dekripsi dilakukan dengan menXorkan data plainteks dan data chiperteks dengan p-box yang sudah termodifikasi dengan kunci.

b. Ekspansi kunci

Pengekspansian kunci dilakukan pada saat awal dengan masukan sebuah kunci dengan panjang 32 bit hingga 448 bit, dan keluaran adalah sebuah larik upa-kunci dengan total 4168 byte. Adapun langkah-langkah pembangkit kunci blowfish adalah sebagai berikut:

1. Terdapat kotak permutasi (P-box) yang terdiri dari 18 buah dan 32 bit upa-kunci: P1, P2, P3, ...P18. P-box ini telah ditetapkan sejak awal, 4 buah P-box awal sebagai berikut:
   P1 = 0x243f6a88
   P2 = 0x85a308d3
   P3 = 0x1319812e
   P4 = 0x03707344
2. XOR-kan P1 dengan 32 bit awal kunci, Xor-kan P2 dengan 32 bit berikutnya dari kunci, dan teruskan hingga seluruh panjang kunci telah ter-XOR-kan (kemungkinan sampai P14, 14x32 =448, panjang maksimal kunci).
3. Terdapat 64 bit dengan isi kosong. Bit-bit tersebut dimasukan ke langkah 2.
4. Gantikan P1 dan P2 dengan keluaran dari langkah 3.
5. Enkripsikan kembali keluaran langkah 3 dengan langkah 2, namun kali ini dengan upa-kunci yang berbeda (sebab langkah 2 menghasilkan upa-kunci baru).
6. Gantikan P3 dan P4 dengan keluaran dari langkah 5.
7. Lakukan seterusnya hingga seluruh P-box teracak sempurna.
8. Total keseluruhan terdapat 521 iterasi untuk menghasilkan seluruh upa-kunci yang dibutuhkan. Aplikasi hendaknya menyimpannya daripada harus membuat ulang seluruh upa-kunci tersebut.

Enkripsi data terjadi dengan memanfaatkan perulangan 16 kali terhadap jaringan feitsel, dan setiap perulangan terdiri dari permutasi dengan masukan kunci dan substitusi data. Semua oprasi dilakukan dengan memanfaatkan oprator XOR dan oprator penambahan. Penambahan dilakukan terhadap empat larik lookup yang dilakukan setiap putarannya. Adapun proses enkripsi data pada algoritma blowfish adalah sebagai berikut:

1. Masukan dari proses ini adalah data 64 bit yang diinisialkan “x”
2. Bagi x menjadi 2 bagian sama besar, x Left (x kiri) sepanjang 32 bit, dan x Rigjht (x kanan) sepanjang 32 bit.
3. Lakukan iterasi (perulangan) sebanyak i = 1 hingga i = 16:

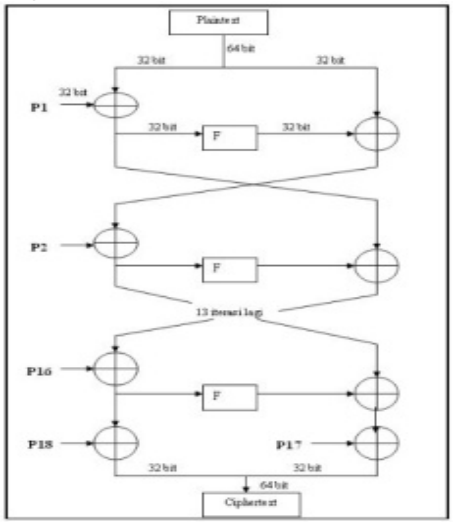
xL = xL XOR P[i];
xR = F(xL) XOR xR;
swap (tukar) (xL, xR);

4. Fungsi F adalah sebagai berikut: bagi xL menjadi 4 buah, 8 bit a, b, c dan d. F(xL) = ((S1[a] + S2[b] mod 232) XOR S3[c]) + S4[d] mod 232.
5. Langkah terakhir adalah :

Swap (tukar) (Xl, xr);
xR = xR XOR P[17];
xL = xL XOR P[18];

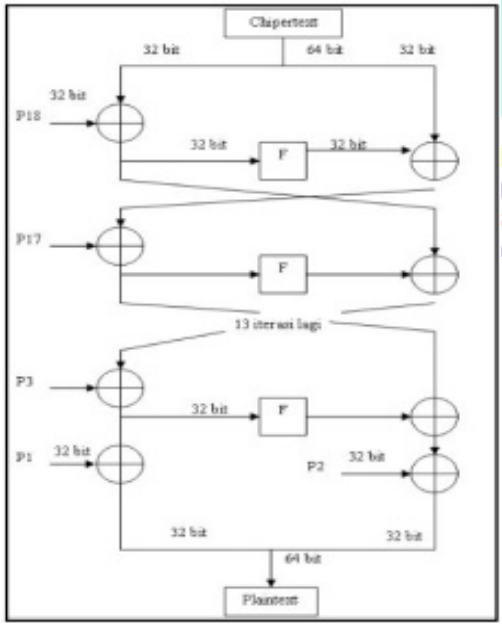
ISSN : 2548-6985

Gabungkan xL dan xR menjadi 64 bit return hasil gabungan. Adapun proses dekripsi dapat dilihat pada Gambar II.3



Gambar 2. Proses Enkripsi Blowfish
Sumber: buku pengantar ilmu kriptografi (2008)

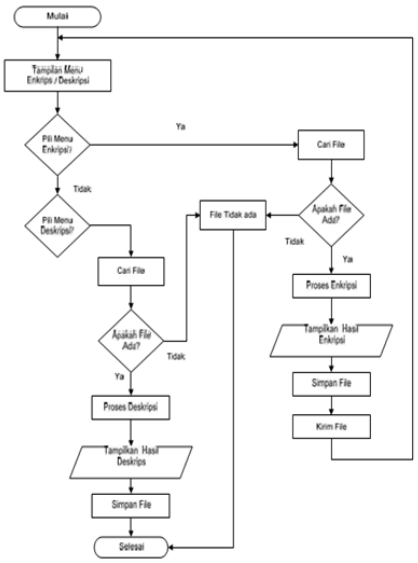
Proses deskripsi data pada algoritma blowfish hampir sama persis dengan proses enkripsi, hanya saja P-box digunakan dengan urutan terbalik. Sehingga P-box di mulai dari P18, P17....P1. Adapun proses dekripsi dapat dilihat pada Gambar 3.



Gambar 3 Proses Dekripsi Blowfish
Sumber: buku pengantar ilmu kriptografi (2008)

METODE PENELITIAN

Perancangan proses digambarkan dalam bentuk Flowchart yang bertujuan untuk menunjukan alur kerja proses dari system aplikasi yang akan dibuat. Perancangan dapat dilihat pada gambar dibawah ini.



Gambar 4. Flowchart Perancangan Proses Aplikasi

HASIL DAN PEMBAHASAN

Dan adapun analisa yang dari proses penelitian tersebut adalah sebagai berikut :
Pada proses enkripsi sebuah masukan dimisalkan adalah (x) elemen data 64 bit. Untuk melakukan proses enkripsi:

(x) dibagi menjadi dua bagian sehingga masing-masing 32-bit (xL dan xR).
Untuk i = 1 sampai 16 maka:
XL =XL xor Pi
XR = F(XL) XOR XR

Swap(tukar) xl dan xr (mengulang swap yang lalu)
XR = XR xor P17
XL = XL xor P18

Pada analisa proses ekspansi kunci dapat dicontohkan pengirim membuat kunci dengan karakter BLOWFISH sehingga kunci tersebut di XOR kan dengan P1 sampai P14 yaitu 32 bit awal kunci hingga seluruh kunci telah tersorkan sampai P14. Dimana karakter BLOWFIS kita ubah kedalam heksa dan desimal untuk mendapatkan bilangan biner dapat kita lihat pada tabel ASCII yang ada pada lampiran

Tabel 1. Kunci BLOWFISH

Karakter	Bilangan Heksa	Bilangan Desimal	Bilangan Biner
B	42	66	1000010
L	4C	76	1001100
O	4F	79	1001111

W	57	87	1010111
F	46	70	1000110
I	49	73	1001001
S	53	83	1010011
H	48	72	1001000

Agar lebih mudah menghitung dengan cara manual, proses perhitungan dilakukan dengan bilangan decimal.

Tabel 2. Proses Analisa

XL			**XR**
KAPUTAMA			
Bilangan desimal : **75658085**			Bilangan desimal : **84657765**
1,001E+26			1,01E+26
XL Xorkan dengan P1 yg sudah termodifikasi dengan kunci			
75658085 xor 667264763			
591910302			
1,00011E+29			
Kemudian XL yang sudah termodifikasi dibagi menjadi 4 buah masing-masing 8 bit a, b, c dan d dengan perhitungan menggunakan rumus F(XL)=((S1[a]+S2[b] mod 232 xor S3[c])+S4[d] mod 232))			
A	b	c	
100011	1000111	11010101	
A= (S1 + a)			
TRUE			
B=(S2 +b)			
TRUE			
C=(S3 +c)			
TRUE			
D=(S4 +d)			
TRUE			
F(XL)=((A+B mod 232 xor C)+D mod			
232))			
= (164 xor 805139376) + 5			
805139225			
805139225			
			XR = XR xor F(XL)
			= **84657765** xor 805139225
			720811388
			Hasil XR Pindahkan ke XL
XL= 720811388			**591910302**

Selain itu dari hasil uji coba yang telah dilakukan akan dianalisa kembali apakah rancangan ini dapat memenuhi tujuan yang akan dicapai seperti yang telah dipaparkan pada bab 1.

Proses Enkripsi

Berikut ini adalah pembentukan chiperteks yang dilakukan pada proses enkripsi di dalam form enkripsi blowfish, yaitu:

1. Jalankan aplikasi kriptografi Blowfish sehingga akan muncul form utama seperti yang terlihat dibawah ini:

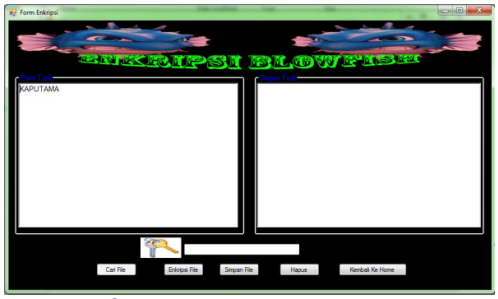
Gambar 5. Form Utama

2. Selanjutnya pilih button yang bergambar  untuk masuk ke form enkripsi.
3. Maka akan muncul form Enkripsi Blowfish sperti yang terlihat pada gambar dibawah ini.

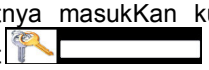
Gambar 6. Form Enkripsi

Setelah muncul form Enkripsi Blowfish, tekan tombol  untuk memilih file teks yang akan dienkripsikan dengan menggunakan algoritma blowfish, kemudian akan muncul file teks pada plain teks seperti gambar dibawah ini.

ISSN : 2548-6985



Gambar 7. Form Enkripsi

Selanjutnya masukKan kunci pada gambar tersebut  dan tekan tombol enkripsi sehingga akan menghasilkan chiperteks seperti yang terlihat pada gambar dibawah ini.

Gambar 8 Form Enkripsi

Kemudian tekan tombol 

dan cari tempat penyimpanan untuk menyimpan hasil enkripsi tersebut.

Proses Dekripsi

Setelah proses enkripsi dilakukan dan terbentuk ciper teks, kemudian kita akan mengembalikan plainteks ke bentuk semula. Berikut adalah cara mengembalikan ciper teks menjadi plain teks.

1. Jalankan aplikasi kriptografi Blowfish seperti proses enkripsi sehingga akan muncul form utama seperti yang terlihat dibawah ini:

Gambar 9. Form Utama

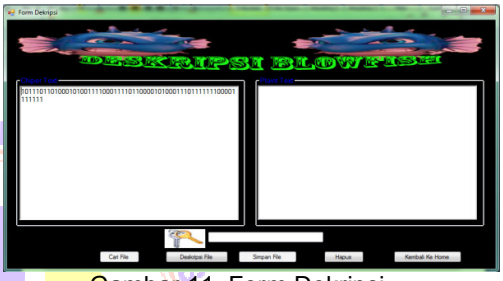
2. Selanjutnya pilih button yang bergambar 

untuk masuk ke form dekripsi.
3. Maka akan muncul form Dekripsi Blowfish sperti yang terlihat pada gambar dibawah ini.

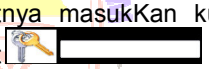
Gambar 10.Form Dekripsi

Setelah muncul form Dekripsi Blowfish, tekan tombol 

untuk memilih file teks yang akan didekripsikan dengan menggunakan algoritma blowfish, kemudian akan muncul file teks pada chiper teks seperti gambar dibawah ini.



Gambar 11. Form Dekripsi

Selanjutnya masukKan kunci pada gambar tersebut  dan tekan tombol enkripsi sehingga akan menghasilkan chiperteks seperti yang terlihat pada gambar dibawah ini.

Gambar 12. Form Dekripsi

KESIMPULAN

Dari hasil perancangan dan pembuatan program aplikasi kriptografi menggunakan algoritma blowfish ini, dapat diambil kesimpulan sebagai berikut :

1. Spesifikasi program aplikasi ini dapat dijalankan sesuai dengan spesifikasi teknis yang dirancang.
2. Program aplikasi kriptografi ini akan membatasi orang yang tidak berhak atas informasi atau data yang dimiliki oleh si-pengirim dalam proses pengiriman menggunakan email untuk dibaca karena pesan sudah dienkripsi

3. Kunci yang digunakan untuk mengekripsi plainteks harus sama dengan kunci yang digunakan untuk mendekripsi chiperteks. Jika kunci yang digunakan untuk mendekripsi file tidak sama dengan kunci yang digunakan untuk mengenkripsi file, maka hasil dekripsi file tidak akan sama dengan plainteks semula sebelum di enkripsi.
4. Hasil dekripsi dari chiperteks akan menghasilkan plainteks yang sama sebelum proses enkripsi.

DAFTAR PUSTAKA

1. Ariyus, Dony. 2008. Pengantar Ilmu Kriptografi,(Teori, Analisis, Dan Implementasi) penerbit Andi Yogyakarta.
2. Sadikin, Rifki. 2005. Kriptografi untuk Keamanan Jaringan, penerbit Andi Yogyakarta.
3. Budi Sutedjo S.Kom.,MM dan Udaya, Y. 2004. Algoritma dan teknik Pemograman, penerbit Andi Yogyakarta.
4. Moh. Sjukani 2009. Algoritma (Algoritma dan Struktur data 1) dengan C, C++ dan java, edisi 5 teknik-teknik dasar pemograman komputer. Penerbit Mitra Wacana Media.
5. Candraleka Happy 2008. Cara Mudah mengelola email untuk pemula, penerbit Mediakita.
6. Bruce Schneier. Applied Cryptograpy, http:// www.schneier.ac.id/395/1/pdf diakses 20 mei 2016.
7. Suriski sitinjak, Yuli Fauziah, Juwariah. Aplikasi Kriptografi File Menggunakan Algoritma Blowfish