Aplikasi Keamanan File Algoritma *Blowfish* pada Universitas Lancang Kuning

Nurliana Nasution[1], Ahmad Zamsuri[2], Khairani Djahara[3]
[1,2,3]Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Lancang Kuning
Jl. Yos Sudarso KM. 8 Rumbai, Pekanbaru, Riau, telp. 0811 753 2015
e-mail: [1]nurliana_2006@yahooc.com, [2]ahmadzamsuri@unilak.ac.id,
[3]khairani.djahara@unilak.ac.id

Abstrak

Salah satu algoritma kriptografi adalah algoritma Blowfish yang merupakan algoritma kriptografi modern kunci simetris berbentuk cipher block. Aplikasi yang dibangun ini dapat mengenkripsi file (plaintext) dalam bentuk teks, gambar, suara, video, juga archieve seperti .zip dan .rar. Enkripsi dilakukan dengan menggunakan kunci tertentu, sehingga menghasilkan chipertext (file yang sudah dienkrip atau disandikan) yang tidak dapat dibaca ataupun dimengerti. Ciphertext tersebut dapat dikembalikan seperti semula jika didekripsi menggunakan kunci yang sama sewaktu mengenkripsi file tersebut. Kunci yang digunakan maksimum 56 karakter.Metode yang digunakan untuk membangun aplikasi iniadalah metode waterfall. Perangkat lunak yang digunakan untuk User-System Interface-nya adalah Visual Basic 6.0. Sistem keamanan file merupakan sistem yang diperlukan bagi setiap lembaga atau organisasii, sehingga keberadaan sistem kemanan file menjadi penting untuk melindungi file penting agar data tersebut terjaga dari pihak-pihak yang tidak berkepentingan. Universitas Lancang Kuning belum memilki sistem keamanan file maka dianggap perlu untuk merancang sistem keamanan file algoritma blowfish. Adapun file-file penting Universitas Lancang Kuning yang akan penulis amankan yaitu file keuangan, surat-surat penting, data dosen dan data karyawan yang berekstensi Microsoft Office (.doc, .docx, .xlx, .xlsx)

Kata kunci: *Keamanan file, Algoritma Blowfish, Universitas Lancang Kuning*

Abstract

One of the cryptographic algorithm is Blowfish algorithm which is a modern cryptographic algorithms shaped symmetric key block cipher. This application is built to encrypt files (plaintext) in the form of text, images, sound, video, as well as .zip and .rar archives. Encryption is done using a specific key, so as to produce ciphertext (the files that have been encrypted or encoded) that can not be read or understood. The ciphertext can be restored if it is decrypted using the same key when encrypting the file. The key used maximum 56 karakter.Metode used to build applications iniadalah waterfall method. The software used for User-System Interface her is Visual Basic 6.0. The security system is a system file that is necessary for any institution or organisasii, so the existence of the file becomes an important security system to protect critical files so that the data is maintained on the parties who are not interested. Lancang Kuning University not have the file security system it is considered necessary to design a security system blowfish algorithm file. The important files Lancang Kuning University will secure that the author's financial files, important papers, lecturer of data and employee data with extension of Microsoft Office (.doc, .docx, .xlx, .xlsx)

Keywords: *File security, Blowfish algorithm, Lancang Kuning University*

1. Pendahuluan

Di era globalisasi ini, dimana segala sesuatunya itu berjalan dengan cepat, kemajuan teknologi semkain memudahkan manusia untuk berkomunikasi dan saling bertukar informasi. Tetapi dengan kemajuan teknnologi itu pula dapat mengakibatkan informasi yang ditukar bisa terganggu dan bia saja dapat di ubah oleh orang lain yang tidak berhak.

Keamanan dan kerahasiaan sebuah data atau informasi dalam komunikasi dan pertukaran informasi menjadi hal yang sangat penting. Itu dikarenakan seringkalinya data atau informasi yang penting kadang tidak sampai ke tangan si penerima atau juga bahkan bisa sampai ke tangan si penerima tapi data yang di terima tersebut di sadap terlebih dahulu tanpa pengetahun dari si pengirim maupun oleh si penerima itu sendiri. Dan bisa saja data asli tersebut oleh si penyadap dirubah datanya sehingga yang seharusnya dikirim ke si penerima berupa data yang asli menjadi data yang tidak sesuai, sehingga bisa menjatuhkan pihak si pengirim. Padahal isi data sebenarnya tidak seperti itu.

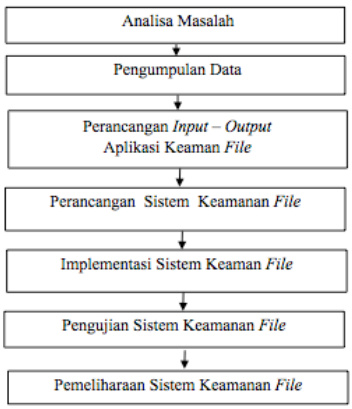
Hal inilah yang seringkali di takutkan oleh pihak – pihak yang saling ingin bertukar informasi. Mereka takut apakah data yang mereka kirim tersebut bisa sampai ke si penerima atau tidak, sehingga masalah keamanan dan rahasianya sebuah data merupakan hal yang sangat penting dalam pertukaran informasi. Maka dari itu saking pentingnya data yang di berikan tersebut agar bisa sampai ke penerima dalam bentuk yang autentik diperlukannya sebah metode untuk merahasiakan data yang dikirim tersebut.

Penelitian serupa pernah dilakukan oleh [1] yang juga menggunakan algoritma *blowfish* sebagai algoritma kriptografi. Penelitian [2] melakukan analisa kinerja algoritma *blowfish* pada simulasi data terbatas yaitu pada lalu lintas data di *website.* Pada peneliti [3] menggunakan metode *End Of File* (EOF) untuk enkripsi citra dengan cara menyisipkan/menyembunyikan kunci yang digunakan untuk proses enkripsi dan deskripsi pada citra hasil enkripsi setelah dikirimkan. Peneliti [4] menggabungkan dua metode yaitu steganografi DCS dan *blowfish* untuk strategi pengamanan ganda konten digital. Peneliti [5] menggunakan algoritma *blowfish* untuk pengamanan suara. Dari penelitian ini keamanan data suara tergantung dari panjang kunci, dimana panjang kunci yang fleksibel dengan menggunakan algoritma *blowdfish* yaitu pada satu sampai enam belas karakter.

Universitas Lancang Kuning belum memiliki sistem pengamanan file serta data-data yang terdapat pada Universitas Lancang Kuning belum dilindungan sehingga hal tersebut sangat mengkhawatirkan karena Universitas Lancang Kuning salah satu lembaga pendidikan yang besar di Riau.

2. Metode Penelitian

Metodologi penelitian dan kerangka kerja penelitian yang digunakan merupakan langkah-langkah yang akan dilakukan dalam rangka penyelesaian masalah yang akan dibahas. Adapun tahapan-tahapan kerangka kerja yang dibutuhkan dalam penyusunan penelitian ini dapat dilihat seperti gambar 1.



Gambar 1. Metode Penelitian

2.1. Analisa Masalah

Langkah analisis masalah adalah untuk dapat memahami masalah yang telah ditentukan ruang lingkup dan batasannya. Dengan menganalisa masalah yang telah dilakukan tersebut, maka diharapkan masalah dapat dipahami dengan baik. Teknik analisis yang digunakan dengan beberapa tahap berikut :

1. Tahap *identify* yaitu : mengidentifikasi permasalahan yang terjadi
2. Tahap *understand* yaitu : memahami lebih lanjut tentang masalah yang ada dengan cara melakukan pengumpulan data yang diperlukan.
3. Tahap *analyze* yaitu : mencari kelemahan-kelemahan sistem yang ada dan mengumpulkan informasi tentang kebutuhan-kebutuhan lebih lanjut yang diperlukan oleh pemakai.

2.2. Pengumpulan Data

Untuk mendukung penelitian ini, salah satu penunjangnya adalah data, Dalam tahap pengumpulan data berupa *file* penting yang dimiliki oleh Universitas Lancang Kuning.

2.3. Perancangan Input – Output Aplikasi Keamanan *File*

Pada tahapan ini merancang *input – output* dengan menggunakan bahasa pemograman VB 6.0 dengan menggunakan tool pada program tersebut.

2.4. Perancangan Sistem Keamanan *File*

Pada tahapan ini merancang sistem keamanan file dengan menggunakan metode algoritma bloefis pada Universitas Lancang Kuning dengan menggunakan bahasa pemograman VB 6.0.

2.5. Implementasi Sistem Keaman File

Pada tahap ini penulis mengimplementasikan sistem keamanan file dengan menjalankan aplikasi untuk inkripsi pada file penting Universitas Lancang Kuning.

2.6. Pengujian Sistem Keamanan File

Pada tahapan ini penulis melakukan pengujian dengan menggunakan data penting Universitas Lancang Kuning.

2.7. Pemeliharaan Sistem Keamanan File

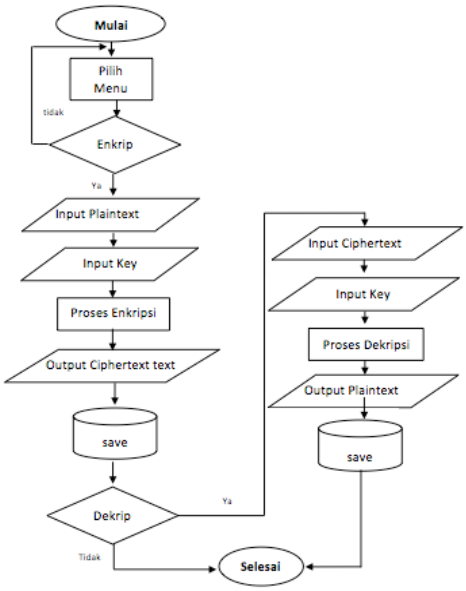
Pada tahap ini penulis melakukan pemeliharaan sistem keamanan file terkait penggunaan sistem dan kesalahan-kesalahan yang terjadi selama penggunaan sistem.

3. Hasil dan Pembahasan

Hasil dan pembahasan dibagi menjadi beberapa tahapan berikut.

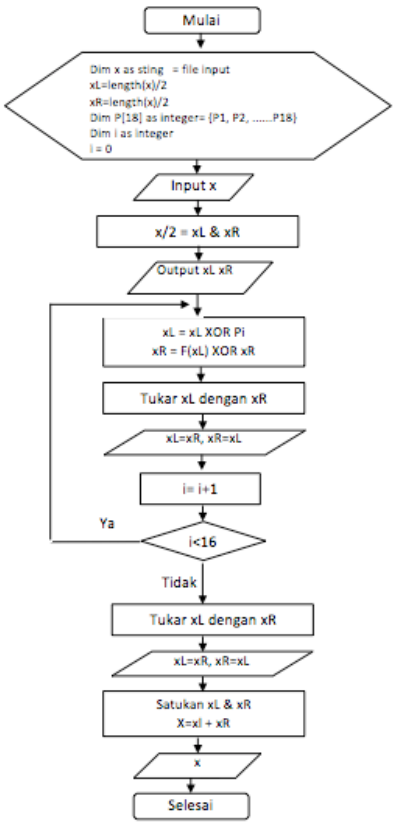
3.1. Bagan Alir Sistem Aplikasi

Bagan alir sistem aplikasi ini menjelaskan proses yang terjadi pada aplikasi yang dibuat secara keseluruhan. Pada bagan alir sistem aplikasi ini akan digambarkan bahwa data yang diinputkan pada aplikasi berasal dari satu sumber, yaitu dari harddisk ataupun media penyimpanan lainnya. Sebelum proses input file, user harus memilih instruksi (menu) yang akan digunakan untuk memproses file (enkripsi/dekripsi). Bagan alir sistem dapat dilihat pada gambar 2.



Gambar 2. *Flowchart* Sistem Aplikasi

Proses kerja untuk enkripsi dan dekripsi pada sistem ini menggunakan kunci dan proses yang sama. Hanya berbeda pada P-array (P1,P2,…….,P18) digunakan dengan urutan terbalik atau di inverskan. Oleh karena itu, flowchart program untuk proses enkripsi dan dekripsi digambarkan dalam satu bagan alir saja pada gambar 3.



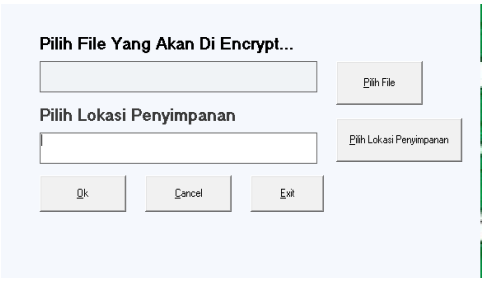
Gambar 3. *Flowchart* Proses Enkripsi dan Deskripsi

3.2. Desain Interface

Program berinteraksi dengan pengguna melalui layar tampilan dalam bentuk jendela (window). Layar tampilan menampilkan informasi yang berbeda-beda tergantung pada perintah yang diberikan oleh pengguna. Program ini diberi nama **Kriptofile**. Program **Kriptofile** ini memiliki beberapa tampilan, beberapa rancangan layar tampilan tersebut adalah pada gambar 4.

Gambar 4. Form Menu Utama

Tampilan utama aplikasi yang dibuat terlihat seperti pada gambar 4 di atas. Pada tampilan utama ini terdapat beberapa menu dan dari beberapa menu ini juga terdapat beberapa sub menu seperti menu file terdapat sub menu exit yang di gunakan untuk keluar dari aplikasi dan menutup semua jendela aplikasi ini, menu kriptografi terdapat dua sub menu yaitu sub menu enkrip yang merupakan perintah untuk menampilkan form Enkrip dan sub menu dekrip untuk menampilkan form dekrip, menu help terdiri dua sub menu yaitu sub menu tentang saya untuk menampilkan form tentang saya dan sub menu petunjuk pemakaian untuk menampilkan form petunjuk pemakaian.



Gambar 5. *Form Enkrip File*

Gambar 5 di atas merupakan tampilan form enkrip file. Hasil enkrpsi adalah "nama_file.unilak".

3.3. Cara Kerja Aplikasi Algoritma *Blowfish*

Algoritma enkripsi Blowfish dijelaskan sebagai berikut :

1. Bentuk inisial P-array sebanyak 18 buah (P1,P2,….....P18) masing-masing bernilai 32-bit.
   Berikut *source code* nya:

```
Private Const ROUNDS = 16
Private m_pBox(0 To ROUNDS + 1) As Long
```

2. Bentuk S-box sebanyak 4 buah masing-masing bernilai 32-bit yang memiliki masukan 256.

Berikut *source code* nya:

```
Private m_sBox(0 To 3, 0 To 255) As Long
```

3. Plaintext yang akan dienkripsi adalah file, kemudian plaintext tersebut diambil sebanyak 64-bit, dan apabila kurang dari 64-bit maka kita tambahkan bitnya, supaya dalam operasi nanti sesuai dengan datanya.
4. Hasil pengambilan tadi dibagi 2, 32-bit pertama disebut XL, 32-bit yang kedua disebut XR.

   Source code-nya:

```
Private Static Sub Encrypt(Xl As Long, Xr As Long)
Dim i As Long, j As Long, Temp As Long
```

5. Selanjutnya lakukan operasi xL = xL xor P1 dan xR = xL XOR f(xL)

   Source code-nya:

```
xL = xR Xor m_pBox(ROUNDS + 1)
Xr = Xr Xor f(xL)
```

6. Hasil dari operasi diatas, tukar XL menjadi XR dan XR menjadi XL.
7. Lakukan sebanyak 16 kali, perulangan yang ke-16 lakukan lagi proses penukaran XL dan XR.

   Berikut *source code*-nya:

```
Xr = Xr Xor m_pBox(j + 1)
Xl = Xl Xor f(Xr)
j = j + 2
```

8. Pada proses ke-17 lakukan operasi:
   XR = XR xor P17
   XL = XL xor P18

   Berikut *source code*-nya:

```
Temp = Xr
Xr = Xl Xor m_pBox(ROUNDS)
```

9. Proses terakhir satukan kembali XL dan XR sehingga menjadi 64-bit kembali.

   Berikut *source code*-nya:

```
Xl = Temp Xor m_pBox(ROUNDS + 1)
```

Gambar 6. *Form Dekripsi File*

Gambar 6 di atas merupakan tampilan dekripsi file. Pada algoritma blowfish terdapat keunikan dalam hal proses dekripsi, yaitu proses dekripsi dilakukan dengan urutan yang sama persis dengan proses enkripsi, hanya saja pada proses dekripsi P1, P2, …, P18 digunakan dalam urutan yang terbalik dan sebagai inputannya adalah *ciphertext*.

4. Kesimpulan

Setelah melakukan penelitian dan perancangan aplikasi sistem keamanan file algoritma Blowfish Pada Universitas Lancang Kuning , maka dapat diambil beberapa kesimpulan sebagai berikut :

1. Aplikasi keamanan file ini masih mengamankan data yang berekstensi Microsoft Office (.doc, .docx, .xlx, .xlsx).
2. Aplikasi keamanan file ini menggunakan perancangan SDLC dan implementasi dengan pemograman visual basic.

Berdasarkan hasil penelitian yang dilakukan untuk pengamanan file pada Universitas Lancang Kuning, saran untuk penerapan dan kelanjutan sistem ini adalah :

1. Bagi para peneliti yang ingin mengembangkan sistem keamanan file dengan algoritma *blowfish* ini dapat dikembangkan lagi menjadi lebih baik dengan melengkapi dan menambah jenis file yang akan diamankan.
2. Bagi para peneliti yang ingin mengembangkan sistem keamanan file lebih baik lagi dengan algoritma yang lebih baik dalam hal penerapan keamanan serta handal dari perusak dokumen melalui jaringan online.

Daftar Pustaka

[1] Sitinjak Suriski, Yuli Fauziah, Juwairiah. *Aplikasi Kriptografi File Menggunakan Algoritma Blowfish.* Seminar Nasional Informatika 2010 (semnasIF 2010). 2010: halaman 78 – 86.

[2] Utami Ema, Shanty Erikawaty, Aryani Tambunan. Penerapan Algoritma *Blowfish* untuk Membuat Sebuah Model Kriptosistem Algoritma dan Menganalisa Kinerja Algoritma *Blowfish* dengan Simulasi Data Terbatas. *Jurnal DASI*. 2010; vol. 11 (no. 2): halaman 33 – 44.

[3] Iswahyudi Catur, Emy Setyaningsih, Naniek Widyastuti. *Pengamanan Kunci Enkripsi Citra pada Algoritma Super Enkripsi Menggunakan Metode End Of File.* Prosiding Seminar Nasional Aplikasi Sains dan Teknologi (SNAST) Periode III. Yogyakarta. 2012: halaman 278-285.

[4] Wijaya Satriya Ermadi, Yudi Prayudi. *Integrasi Metode Steganografi DCS pada Image dengan Kriptografi Blowfish sebagai Model Anti Forensik untuk Keamanan Ganda Konten Digital.* Seminar Nasional Aplikasi Teknologi Informasi (SNATI). Yogyakarta. 2015: halaman 11 – 17.

[5] Sutardi. Implementasi Algoritma *Blowfish* untuk Keamanan Data Suara. *DINAMIKA Jurnal Ilmiah Teknik Mesin*. 2015; vol.6 (no.2): halaman 51 – 58.