Jurnal Widya
Volume 5, Nomor 1, bulan April 2024: halaman 468-481
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id/
editor.jurnalwidya@gmail.com

P-ISSN: 2746-5411
E-ISSN: 2807-5528

PERANCANGAN DAN IMPLEMENTASI ALGORITMA BLOWFISH UNTUK KEAMANAN DATA FILE CITRA DIGITAL

Design And Implementation Of Blowfish Algorithms For Security Of Digital Image File Data

Nandri Marsan Sitinjak[1], Rini Oktari Batubara[2], Frans Ikorasaki[3]
[1]Program Studi Manajemen Informatika, Akademi Manajemen Informatika Komputer Widyaloka, Medan, Sumatera Utara, Indonesia
[2,3]Program Studi Sistem Informasi, Universitas Potensi Utama, Medan, Sumatera Utara, Indonesia
Email : nandrimarsan@gmail.com[1], rini.admmedan@gmail.com[2], ikorasaki222@gmail.com[3]

ABSTRAK

Kerahasiaan data sangat diperlukan baik dalam suatu organisasi maupun pribadi, bahkan dalam jaringan internasional yang sering disebut internet. Untuk menjaga kerahasiaan data, maka diperlukan metode enkripsi agar data tidak dapat dibaca dan dimengerti. Algoritma blowfish sebagai penyandi data yang cepat dan menggunakan 64 bit untuk setiap 16 kali putaran secara berulang-ulang, desainnya mudah untuk dianalisa yang membuatnya tahan terhadap kesalahan dan akan berada pada *domain public* (bebas paten). File hasil enkripsi pada aplikasi menggunakan format **.enc*. Mengalami keterlambatan dalam memproses enkripsi file. Hasil pengujian keamanan pada file enkripsi menggunakan metode *algoritma blowfish*, menunjukan hasil bahwa file enkripsi sangat memiliki tingkat kesulitan dalam membobol kunci. Untuk mengatasi masalah tersebut banyak bermunculan teknologi-teknologi enkripsi dan peneliti yang dapat dipilih *user* komputer dalam pengamanan data-data pribadinya. Salah satu metode yang dianggap tangguh dalam melakukan pengamanan ini adalah metode algoritma *blowfish* yang merupakan penyandian dengan cara mengubah letak dari huruf-huruf pada pesan yang akan disandikan. Dan untuk membaca pesan aslinya kembali, cukup dengan mengembalikan letak dari huruf-huruf pada pesan tersebut berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati pihak pengirim dan penerima. Hasil dari ujicoba terhadap berbagai jenis file menunjukkan bahwa aplikasi dapat digunakan untuk tipe file jpg,bitmap,png tanpa ada kesalahan.

Kata Kunci : Algoritma Blowfish, Dekripsi, Enkripsi, File, Key, Kriptografi.

ABSTRACT

*Data confidentiality is needed both in an organization and in private, even in an international network which is often called the internet. To maintain data confidentiality, encryption methods are needed so that data cannot be read and understood. The blowfish algorithm is a fast data encoder and uses 64 bits for every 16 rounds repeatedly, the design is easy to analyze which makes it resistant to errors and will be in the public domain (patent free). Encrypted files on the application use the * .blw format. Experience additional time on different file sizes. The results of security testing on file encryption using the brute force attack method shows the results that from 50 attempts to break the password, the percentage of failure is 100%. The results of tests on various types of files indicate that the application can be used for all file types without errors.*

Keywords: *Blowfish Algorithm, Decryption, Encryption, File, Key, Cryptography.*

Jurnal Widya

Volume 5, Nomor 1, bulan April 2024: halaman 468-481
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id/
editor.jurnalwidya@gmail.com

P-ISSN: 2746-5411
E-ISSN: 2807-5528

1. Pendahuluan

Masalah keamanan komputer merupakan sesuatu yang sangat penting dalam era informasi terutama bagi suatu instansi. Kerahasiaan data merupakan salah satu masalah yang penting dalam keamanan data terutama pada data teks. Data menjadi salah satu yang sangat penting dalam instansi. Hal itu menjadi masalah penting bagi instansi, ketika pesan dikirim dari satu tempat ke tempat lain, kemungkinan terdapat beberapa ancaman yang dapat merusak sistem keamanan data tersebut seperti pencurian atau kerusakan pada data. Untuk melindungi data penting tersebut maka data dapat dienkripsi dan didekripsi atau diubah menjadi kode yang tidak dapat diketahui orang lain[1]

Oleh karena itu peneliti merekomendasikan sebuah sistem keamanan pesan menggunakan teknik kriptografi dan steganografi. Kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut dengan melakukan pembangkitan kunci, enkripsi dan dekripsi. Kriptografi bertujuan untuk memberi layanan keamanan (yang juga dinamakan sebagai aspek-aspek keamanan)[2]. *Blowfish* merupakan salah satu algoritma yang tidak dipatenkan dan cukup kuat karena memiliki ruang kunci yang besar dan panjangnya bisa beragam, sehingga tidak mudah diserang pada bagian kuncinya. Suatu sistem *kriptografi* yang baik terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan[3]. Namun untuk menggunakan teknik kriptografi dibutuhkan sebuah metode yang baik dalam kriptografi. Peneliti menggunakan metode *Algoritma Blowfish* untuk keamanan data file citra digital. Untuk itu dibangun sebuah aplikasi yang dapat digunakan untuk mengamankan data atau informasi berupa *file* dengan menggunakan metode *Blowfish* ini. Selain itu diharapkan pula aplikasi yang dibangun ini dapat melihat kinerja algoritma *Blowfish* dari segi waktu prosesnya[4]. Dengan menggunakan teknik kriptografi menggunakan metode *Algoritma Blowfish* akan dapat melakukan teknik kriptografi. Namun teknik kriptografi membutuhkan sebuah metode, oleh karena itu peneliti menggunakan metode *Algoritma Blowfish* untuk keamanan data file citra digital[5]. Untuk mengatasi masalah tersebut banyak bermunculan teknologi-teknologi enkripsi dan peneliti yang dapat dipilih user komputer dalam pengamanan data-data pribadinya. Salah satu metode yang dianggap tangguh dalam melakukan pengamanan ini adalah *Blowfish* diciptakan oleh seorang *Cryptanalyst* bernama *Bruce Schneier*, Presiden perusahaan *Counterpane Internet Security*, *Inc* (Perusahaan konsultan tentang kriptografi dan keamanan komputer) dan dipublikasikan tahun 1994[6]. Dibuat untuk digunakan pada komputer yang mempunyai *microposesor* besar (32-bit keatas dengan *cache* data yang besar). *Blowfish* merupakan algoritma yang tidak dipatenkan dan *licensefree*, dan tersedia secara gratis untuk berbagai macam kegunaan. Pada saat *Blowfish* dirancang, diharapkan mempunyai kriteria perancangan sebagai berikut. 1. Cepat, *Blowfish* melakukan *enkripsi* data pada *microprocessors* 32-bit dengan *rate* 26 *clock cycles* per *byte*. 2. *Compact* (ringan), *Blowfish* dapat dijalankan pada memori kurang dari 5K. 3[7]. Sederhana, *Blowfish* hanya menggunakan operasi-operasi sederhana: penambahan, *XOR*, dan *lookup* tabel pada operan 32-bit. 4[8]. Memiliki tingkat keamanan yang bervariasi, panjang kunci yang digunakan oleh *Blowfish* dapat bervariasi dan bisa sampai sepanjang 448 bit[9]. Dalam penerapannya sering kali algoritma ini menjadi tidak optimal. Karena strategi *implementasi* yang tidak tepat. Algoritma *Blowfish* akan lebih optimal jika digunakan untuk aplikasi yang tidak sering berganti kunci, seperti jaringan komunikasi atau enkripsi *file* otomatis.[10]. Selain itu, karena algoritma ini membutuhkan memori yang besar, maka algoritma ini tidak dapat diterapkan untuk aplikasi yang memiliki memori kecil seperti *smart card*. Panjang kunci yang digunakan, juga mempengaruhi keamanan penerapan algoritma ini[11].

2. Tinjauan Pustaka

Jurnal Widya
Volume 5, Nomor 1, bulan April 2024: halaman 468-481
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id/
editor.jurnalwidya@gmail.com
P-ISSN: 2746-5411
E-ISSN: 2807-5528

2.1 Kriptografi

Sejarah kriptografi sebagian besarmerupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (transposition cipher) dan algoritma substitusi (substitution cipher). Ciphertransposisi mengubah susunan huruf-huruf di dalam pesan, sedangkan ciphersubstitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain[12].

2.2 Keamanan File

keamanan file adalah pengelolaan akses dan otorisasi yang baik dan memiliki kebijakan yang jelas tentang siapa yang memiliki akses ke file-file penting dan sejauh mana tingkat akses mereka. Hal ini dapat dilakukan melalui penerapan hak akses yang tepat, pengaturan grup pengguna, dan autentikasi ganda jika diperlukan. Dengan demikian, risiko akses yang tidak sah dapat dikurangi dan kerahasiaan data tetap terjaga[13].

2.3 Citra Digital

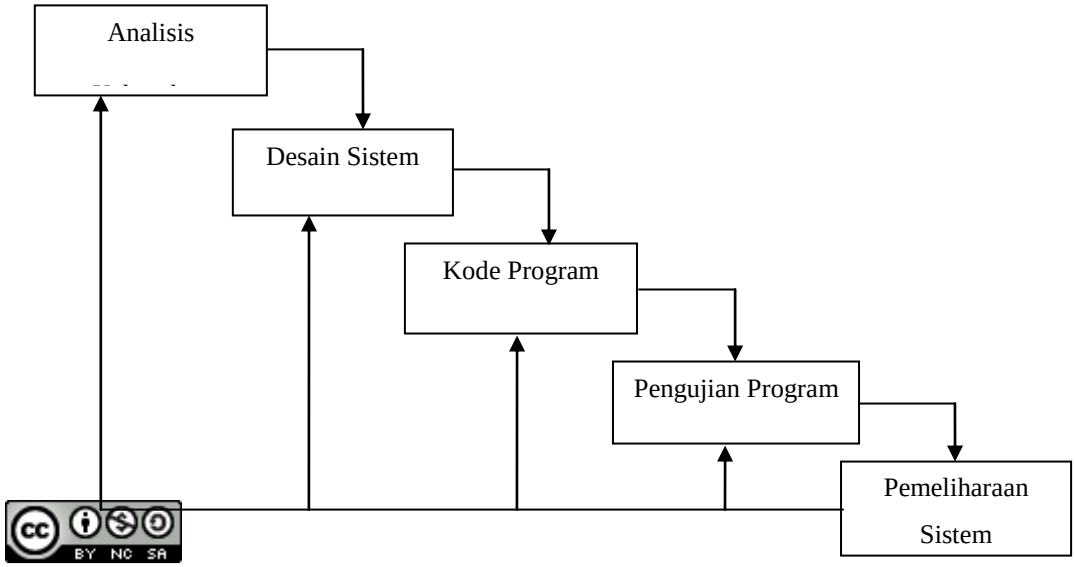
Citra digital adalah gambar dua dimensi yang dihasilkan dari analog dua dimensi yang kontinu menjadi gambar melalui proses sampling. Gambar analog dibagi menjadi N baris dan M kolom sehingga menjadi gambar diskrit. Citra digital merupakan citra yang dapat diolah komputer. Yang disimpan dalam komputer hanyalah angka-angka yang menunjukkan besar intensitas pada masing-masing piksel. Karena berbentuk data numerik, maka citra digital dapat diolah dengan komputer[14].

2.4 Blowfish

Blowfish adalah suatu algorima penyandian pesan yang diciptakan oleh seorang Cryptanalyst bernama Bruce Schneier Presiden perusahaan Counterpane Internet Security[15].

3. Metode Penelitian

Penelitian ini menggunakan beberapa tahapan. Tahapan dalam penelitian ini dapat dimodelkan pada diagram *Waterfall*. Adapun beberapa tahapan yang digunakan dalam penelitian ini dapat di lihat pada gambar 1.



Jurnal Widya
Volume 5, Nomor 1, bulan April 2024: halaman 468-481
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id/
editor.jurnalwidya@gmail.com

P-ISSN: 2746-5411
E-ISSN: 2807-5528

Gambar 1. Prosedur Perancangan Sistem

Dalam pengembangannya metode *waterfall* memiliki beberapa tahapan yaitu : *requirement* (analisis kebutuhan), design sistem (*system design*), *coding*, pengujian program, pemeliharaan sistem.

A. Analisis Kebutuhan

Berisi tentang hal-hal yang harus ada pada hasil perancangan agar mampu menyelesaikan masalah yang ada sesuai tujuan. Adapun yang menjadi kebutuhan dalam melakukan penelitian ini adalah sebagai berikut :

1. Perangkat Keras (*Hardware*)
   Perangkat keras yang digunakan antara lain :
   1. *Dual core; Processor* 2,40 *GHz*
   2. *Hard disk : 320GB*
   3. *RAM 4 GB*
   4. *Monitor LCD 14"*
   5. *Keyboard* dan *Mouse.*
2. Perangkat lunak (*Software*)
   Software yang digunakan untuk membuat penelitian ini antara lain :
   1. Sistem operasi *Windows 7*
   2. *Netbeans* 8.0

B. Desain Sistem

Secara umum Perancangan dan Implementasi Algoritma *Blowfish* Untuk Keamanan Data *File Citra Digital* menggunakan model perancangan *Unified Modelling Language*. Pada tahap ini akan dilakukan perancangan dari aplikasi yang akan dibuat meliputi :model sistem, perancangan *arsitektural* dan perancangan antarmuka.

C. Kode Program

Kode Program merupakan penerjemahan desain dalam bahasa yang bisa dikenali oleh komputer. Dilakukan oleh programmer yang akan meterjemahkan transaksi yang diminta oleh user. Tahapan inilah yang merupakan tahapan secara nyata dalam mengerjakan suatu sistem. Dalam artian penggunaan komputer akan dimaksimalkan dalam tahapan ini. Setelah pengkodean selesai maka akan dilakukan testing terhadap sistem yang telah dibuat tadi. Tujuan *testing* adalah menemukan kesalahan-kesalahan terhadap system tersebut dan kemudian bisa diperbaiki.

D. Pengujian Program

Pada tahap ini dilakukan pengujian aplikasi secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan sistem. Pengujian secara *black box (interface)* yaitu pengujian perangkat lunak yang tes *fungsionalitas* dari aplikasi yang bertentangan dengan *struktur internal* atau kerja.

E. Pemeliharaan Sistem

Perangkat lunak yang susah disampaikan kepada pelanggan pasti akan mengalami perubahan. Perubahan tersebut bisa karena mengalami kesalahan karena perangkat lunak harus menyesuaikan dengan lingkungan (*peripheral* atau *system* operasi baru) baru, atau karena pelanggan membutuhkan perkembangan fungsional.

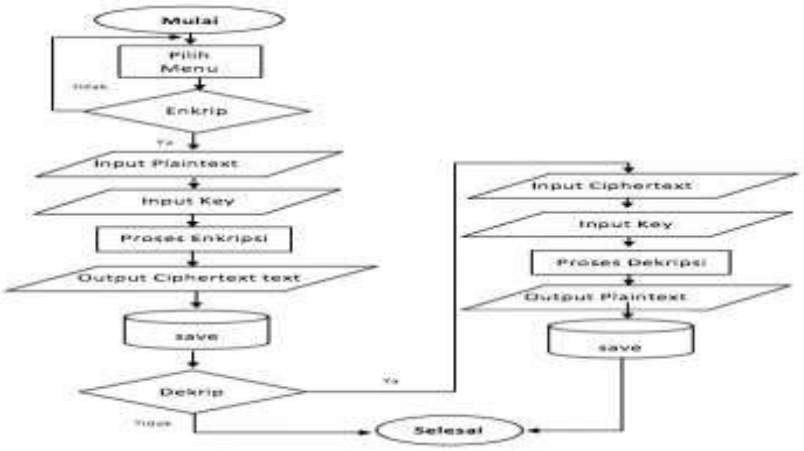
4. Hasil Dan Pembahasan

Jurnal Widya
Volume 5, Nomor 1, bulan April 2024: halaman 468-481
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id/
editor.jurnalwidya@gmail.com
P-ISSN: 2746-5411
E-ISSN: 2807-5528

4.1. Pembahasan

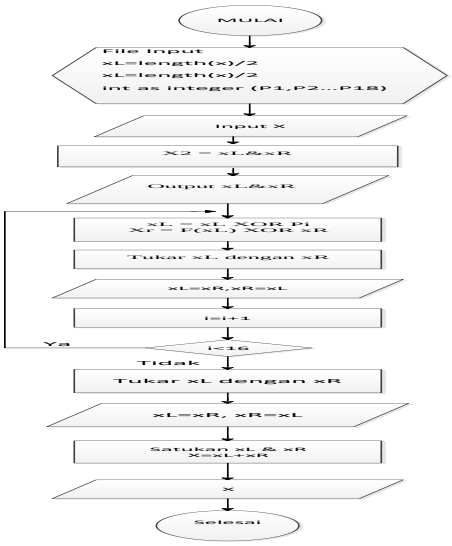
4.1.1 *Flowchart* Sistem Aplikasi Algoritma Blowfish.

Flowchart 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. sebagai berikut:



Gambar 2. *Flowchart* Sistem Aplikasi *Flowchart* Enkripsi *Blowfish*

4.1.2 *Flowchart* Enkripsi/Dekripsi Algoritma Blowfish



Gambar 3. *Flowchart* Enkripsi/Dekripsi *Blowfish*

Didalam proses ini terdapat *file biner* hasil konversI *file* asli kedalam biner dan kunci yang dibangkitkan terlebih dahulu sebelum dilakukan proses enkripsi atau dekripsi data. Kunci- kunci yang digunakan antara lain terdiri dari, 18 buah yang memiliki 32-bit *subkey* yang tergabung dalam P-array

Jurnal Widya
Volume 5, Nomor 1, bulan April 2024: halaman 468-481
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id/
editor.jurnalwidya@gmail.com

P-ISSN: 2746-5411
E-ISSN: 2807-5528

(P1, P2, ..., P18). Selain itu, ada empat 32-bit S-box yang masing-masingnya memiliki 256 entri : S1,0, S1,1, ...,S1,255. S2,0, S2,1, ..,S2,255. S3,0, S3,1, ...,S3,255. S4,0, S4,1, .., S4,255. Konsep dari algortima *blowfish* adalah bahwa setiap bit *file* akan ditambahkan dengan bit yang berasal dari kunci – kunci pada P-array dan S-*box*. Dalam penambahan bit harus mencukupi 64 bit, jika melebihi dari 64 bit maka akan dilakukan proses perulangan. Berikut ini gambaran dari proses tersebut.

File Awal (contoh simulasi *file biner* hasil konversi dari *file* asli)

11000011 11010011 11000011 10100110

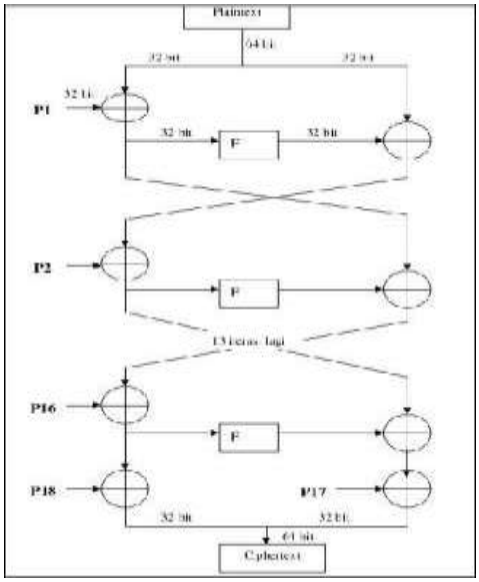
Untuk alur algoritma enkripsi dan dekripsi dengan metoda *Blowfish* dijelaskan sebagai berikut :

a. Enkripsi data terdiri dari iterasi fungsi sederhana (*Feistel Network*) sebanyak 16 kali putaran. Setiap putaran terdiri dari permutasi kunci-*dependent* dan substitusi kunci- dan data *dependent*. Semua operasi adalah penambahan (*addition*) dan XOR pada variabel 32-bit. Operasi tambahan lainnya hanyalah empat penelusuran tabel (*table lookup*) *array* berindeks untuk setiap putaran.

Untuk alur algoritma enkripsi dengan metoda *Blowfish* dijelaskan sebagai berikut :

1. Bentuk inisial *array* P sebanyak 18 buah (P1,P2, ……..P1 masing-msing bernilai 32-bit. *Array* P terdiri dari delapan belas kunci 32-bit subkunci : P1,P2,…….,P18
2. Bentuk S-box sebanyak 4 buah masing-masing bernilai 32-bit yang memiliki masukan 256.
3. *ChiperImage* yang akan dienkripsi diasumsikan sebagai masukan, *ChiperImage* 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.
5. Selanjutnya lakukan operasi XL = XL *xor* Pi dan XR = F(XL) *xor* XR
6. Hasil dari operrasi diatas ditukar XL menjadi XR dan XR menjadi XL.
7. Lakukan sebanyak 16 kali, perulangan yang ke-16 lakukan lagi proses penukaran XL dan XR.
8. Pada proses ke-17 lakukan operasi untuk XR = XR xor P17 dan XL = XL *xor* P18.
9. Proses terakhir satukan kembali XL dan XR sehingga menjadi 64-bit kembali.

Blowfish menggunakan jaringan *Feistel* yang terdiri dari 16 buah putaran. Skema jaringan *Feistel* dapat dilihat di gambar 4 sebagai berikut:



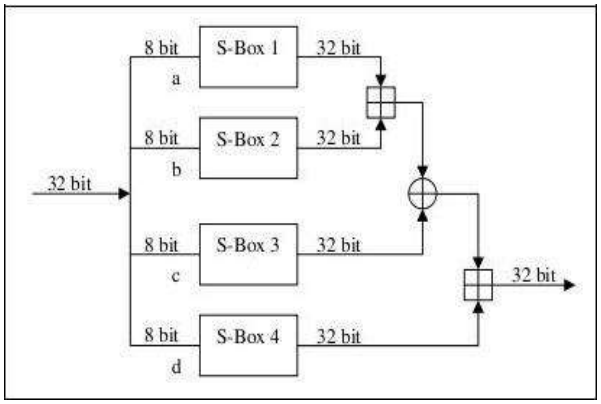
Gambar 4. Jaringan *Feistel* untuk Algoritma *Blowfish*

Jurnal Widya
Volume 5, Nomor 1, bulan April 2024: halaman 468-481
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id/
editor.jurnalwidya@gmail.com
P-ISSN: 2746-5411
E-ISSN: 2807-5528

Pada jaringan *feistel*, *Blowfish* memiliki 16 iterasi, masukannya adalah 64-bit elemen data X. Untuk melakukan proses enkripsi:

1. Bagi X menjadi dua bagian yang masing-masing terdiri dari 32-bit: XL, XR.
2. For i = 1 to 16:
   XL = XL XOR Pi
   XR = F(XL) XOR XR
   Tukar XL dan XR
3. Setelah iterasi ke-enam belas, tukar XL dan XR lagi untuk melakukan *undo* pertukaran terakhir.
4. Lalu lakukan
   XR = XR XOR P17
   XL = XL XOR P1
5. Terakhir, gabungkan kembali XL dan XR untuk mendapatkan *CipherImage.*

Algoritma *Blowfish* memiliki 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. Dalam algoritma *Blowfish* juga terdapat fungsi f. Berikut ini gambar mengenai fungsi f tersebut.



Gambar 5. Fungsi f dalam algoritma *Blowfish*

F-function terdiri dari 4 buah *S-box* yang masing-masing menerima input 8 bit dan menghasilkan *output* 32 bit. Jadi 32 ketika bit hasil XOR P1 dan sub blok kiri memasuki F-*function*, akan dipecah menjadi 4 buah bagian yang masing-masing 8 bit. Masing-masing akan mengalami *substitusi* dan hasil dari sebuah S-*box* ialah 32 bit. Hasil dari *S-box* 1 akan dijumlahkan *modular* dengan hasil dari *S-box* 2, kemudian di XOR dengan hasil dari S-box 3, dan terakhir dijumlahkan *modular* dengan hasil dari *S-box* 4.

Secara matematis F-function dapat ditulis sebagai berikut:

F(xL) = ((S1,a + S2,b mod 232) XOR S3,c) + S4,d mod 232

Hasil dari F-function ini akan di XOR dengan subblok kanan (R) dari blok pertama. Hasilnya akan menjadi sub blok kiri untuk kemudian di XOR lagi dengan P2, dan seterusnya.

Dalam hal kasus ini, penulis memberikan contoh singkat cara kerja fungsi f yang hanya melakukan satu iterasi.

Fungsi *F* didapat dari :

XL dibagi menjadi 4 (*a*, *b*, *c*, *d*) masing-masing 8 bit =

a = 01000011
b = 01010110
c = 00010011
d = 10011111

Jurnal Widya
Volume 5, Nomor 1, bulan April 2024: halaman 468-481
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id/
editor.jurnalwidya@gmail.com

P-ISSN: 2746-5411
E-ISSN: 2807-5528

Fungsi F : $F(XL)$ = (((*S0.a* + *S1.b* mod 232) XOR *S2*, *c*) + *S3,d* mod 232)
S0.a + *S1.b* mod 232
= (11010001 00110001 00001011 10100110 . 01000011) + (01001011 01111010 01110000 11101001. 01010110) mod 232
=(11011010111111110101100000110001110010+11001010110110010000111 10111001000110) mod 232

Berikut ini adalah kebutuhan perangkat keras dan perangkat lunak untuk membuat Aplikasi Perancangan Dan Implementasi Algoritma *Blowfish* Untuk Keamanan Data *File Citra Digital* :Perangkat lunak laptop atau PC dengan spesifikasi sebagai berikut :

1. Satu unit laptop atau PC dengan spesifikasi sebagai berikut :
   a. *Processor Core i3* / *Core i2* / *Core 2 duo*
   b. *RAM* minimal 2 Gb
   c. *Hardisk* minimal 320 Gb
2. Perangkat Lunak dengan spesifikasi sebagai berikut :
   a. Sistem Operasi *Windows 7* / *Windows Xp*
   b. *Netbeans 8.0*

Setelah melakukan uji coba terhadap sistem, maka dapat hasil yang didapatkan yaitu :

1. Perhitungan metode ke dalam sistem telah sesuai.
2. Sistem yang diterapkan sesuai dengan yang dirancang.
3. Hasil enkripsi *file citra digital* berjalan dengan baik.
4. Hasil dekripsi *file citra digital* berjalan dengan baik.
5. Gambar yang sudah di enkripsi akan berubah dari gambar aslinya.
6. *Interface* bersifat *userfriendly* sehingga siapa saja dapat memahami penggunaan aplikasi.

Setiap sistem memiliki kelebihan dan kekurangan, berikut ini adalah kelebihan dan kekurangan sistem yang telah dibuat.

Adapun kelebihan sistem yang telah dibuat diantaranya yaitu :

1. Dapat meng-enkripsi file citra digital.
2. Dapat menggunakan teknik kriptografi.
3. Memberikan hasil keamanan yang baik..
4. Dapat mengamankan data dengan algoritma..

Adapun kekurangan sistem yang telah dibuat diantaranya yaitu :

1. Sistem yang telah dirancang menggunakan lebih dari satu metode.
2. *Interface* antar muka belum menarik.
3. Sistem ini belum diterapkan pada perangkat *mobile*.

4.2. Hasil

4.2.1. Tampilan Hasil

1. Tampilan *Form Login*

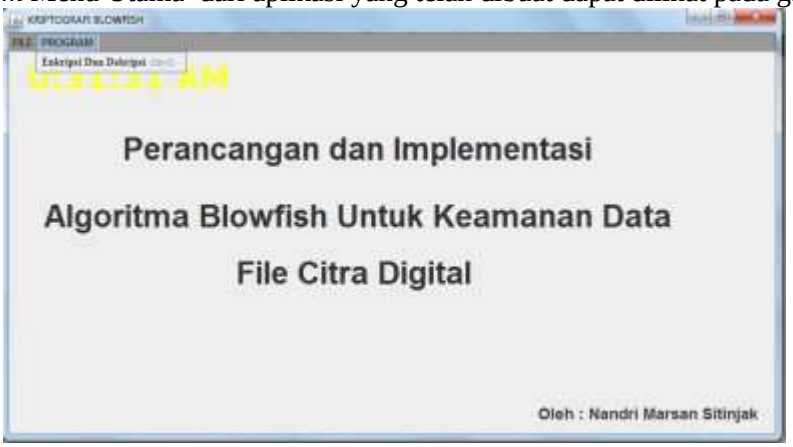
Tampilan *form Login* dari aplikasi yang telah dibuat dapat dilihat pada gambar 6.

Jurnal Widya
Volume 5, Nomor 1, bulan April 2024: halaman 468-481
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id/
editor.jurnalwidya@gmail.com
P-ISSN: 2746-5411
E-ISSN: 2807-5528

Gambar 6. Tampilan *Form Login*

2. Tampilan *Form* Menu Utama

Tampilan *form* Menu Utama dari aplikasi yang telah dibuat dapat dilihat pada gambar 7.



Gambar 7. Tampilan *Form* Menu Utama

3. Tampilan *Form* Menu Utama Algoritma *Blowfish*

Tampilan *form* Menu Utama Algoritma *Blowfish* dari aplikasi yang telah dibuat dapat dilihat pada gambar 8.

Jurnal Widya
Volume 5, Nomor 1, bulan April 2024: halaman 468-481
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id/
editor.jurnalwidya@gmail.com

P-ISSN: 2746-5411
E-ISSN: 2807-5528

Gambar 8. Tampilan *Form* Menu Utama Algoritma Blowfish

3. Tampilan *Form* Enkripsi

Tampilan *form* Enkripsi dari aplikasi yang telah dibuat dapat dilihat pada gambar 9.

Gambar 9. Tampilan *Form* Enkripsi

4. Tampilan *Form* Dekripsi

Tampilan *form* Dekripsi dari aplikasi yang telah dibuat dapat dilihat pada gambar 10.

Jurnal Widya
Volume 5, Nomor 1, bulan April 2024: halaman 468-481
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id/
editor.jurnalwidya@gmail.com
P-ISSN: 2746-5411
E-ISSN: 2807-5528

Gambar 10. Tampilan *Form* Dekripsi

5. Kesimpulan

Kesimpulan yang dapat diambil dari hasil perancangan dan implementasi keamanan data *file citra digital* dengan menggunakan kriptografi algoritma *Blowfish* adalah sebagai berikut :

1. Sistem yang dibangun sudah mampu mengimplementasikan sistem penyandian pada keamanan data *file citra digital*dengan menggunakan kriptografi *Blowfish*, baik dalam proses enkripsi maupun proses dekripsi.
2. Kecepatan sistem yang dibangun dalam melakukan enkripsi dan dekripsi akan sangat bergantung pada banyaknyajumlah *file* data *citra digital* yang akan di enkripsi maupun di dekripsi.
3. Berdasarkan hasil uji coba sistem dalam melakukan enkripsi terhadap data *file citra digital*, bahwa sistem yang dibangun sudah dapat menerima atau mengenkripsi jenis *file* gif, jpg.
4. Aplikasi yang dibangun dengan menggunakan bahasa pemrograman *Java* dapat digunakan untuk melakukan enkripsi dan dekripsi terhadap data *file citra digital*.

Adapun beberapa saran dari hasil skripsi ini adalah:

1. Agar kerahasiaan data *file citra digital* yang di enkripsi maupun di dekripsi tetap terjaga maka sebaiknya kerahasiaan kunci harus tetap dijaga kerahasiaanya. Kata kunci hanya boleh diketahui oleh orang yang bersangkutan.
2. Agar sistem ini berjalan lebih baik lagi dan sesuai dengan harapan oleh *user*, maka sebaiknya di dukung oleh perangkat yang sesuai dengan kebutuhan dari sistem tersebut.
3. Agar dokumen data *file citra digital* tersebut lebih terjaga kearahasiaan dan sistem penyandian lebih kuat pada algoritma *Blowfish*sebaiknya *user*memilih kunci yang tidak *familiar*sehingga enkripsi lebih aman.
4. Disarankan perbaikan sistem menjadi lebih baik lagi dalam pengamanan data *file citra digital*.

Jurnal Widya
Volume 5, Nomor 1, bulan April 2024: halaman 468-481
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id/
editor.jurnalwidya@gmail.com

P-ISSN: 2746-5411
E-ISSN: 2807-5528

5. Untuk kedepannya supaya algoritma *Blowfish* lebih baik dalam mengamankan data *file citra digital*, sebaiknya dilakukan perpaduan metode yang membuat algoritma tersebut menjadi terjaga kerahasiaannya sehingga tidak mudah diketahui.

Referensi

[1] F. Syafar *et al.*, "Blowfish Advanced CS Untuk Solusi Keamanan Sistem Komputer Sekolah," vol. 01, pp. 353–361, 2023.

[2] B. Dengan *et al.*, "APLIKASI ANDROID UNTUK PENGAMAN TEKS MENGGUNAKAN KRIPTOGRAFI BERLAPIS DENGAN ALGORITMA CAESAR , BLOWFISH DAN AES (ADVANCED ENCRYPTION STANDAR)," no. August, 2019.

[3] H. G. Simanullang and A. P. Silalahi, "ALGORITMA BLOWFISH UNTUK MENINGKATKAN KEAMANAN DATABASE MYSQL," vol. 4, no. 1, pp. 10–14, 2018.

[4] K. Pengantar, "No Title".

[5] D. F. Abdul, M. I. Budiman, and T. Kurniawan, "Analisis Sistem Keamanan Sistem Operasi (Windows , Linux , MacOS)," no. March, 2019.

[6] N. Z. Munantri, H. Sofyan, and M. Y. Florestiyanto, "Aplikasi Pengolahan Citra Digital Untuk Identifikasi Umur Pohon," *Telematika*, vol. 16, no. 2, p. 97, 2020, doi: 10.31315/telematika.v16i2.3183.

[7] S.- Muryanah, "Menyisipkan Pesan Rahasia Kedalam Gambar Dengan Metode Blowfish Dan Least Significant Bit (Lsb)," *JIKA (Jurnal Inform.*, vol. 4, no. 3, p. 87, 2020, doi: 10.31000/jika.v4i3.2869.

[8] E. Susanto, D. Adika Prasetya, I. Arbatona, J. Christian Marpaung, and S. Hikmatyar Rahadian, "Pengamanan Objek Vital, Keamanan File, Dan Keamanan Cyber Pada Pt Pos Indonesia," *J. Mutiara Ilmu Akunt.*, vol. 1, no. 3, pp. 163–174, 2023.

[9] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[10] F. D. Silalahi, "Keamanan Cyber (Cyber Security)," *Penerbit Yayasan Prima Agus Tek.*, pp. 1–285, 2022, [Online]. Available: http://penerbit.stekom.ac.id/index.php/yayasanpat/article/view/367

[11] F. Riza, N. Sridewi, A. M. Husein, and M. K. Harahap, "Analisa Frekuensi Hasil Enkripsi Pada Algoritma Kriptografi Blowfish Terhadap Keamanan Informasi," *J. Teknol. dan Ilmu Komput. Prima*, vol. 1, no. 1, pp. 11–15, 2018, doi: 10.34012/jutikomp.v1i1.233.

[12] D. A. Meko, "Jurnal Teknologi Terpadu Perbandingan Algoritma DES , AES , IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data Donzilio Antonio Meko Program Studi Teknik Informatika , STIMIK Kupang Jurnal Teknologi Terpadu," *J. Teknol. Terpadu*, vol. 4, no. 1, pp. 8–15, 2018.

[13] N. Permatasari and Y. Mardiana, "Aplikasi Penyandian Pesan Teks Berbasis Web Menggunakan Algoritma Blowfish," *Semin. Nas. Ilmu Komput.*, vol. 3, no. 1, pp. 61–68, 2023.

[14] R. P. Saputra, J. Wahyudi, and J. Jumadi, "Comparative Analysis of the Blowfish Algorithm and the Des Algorithm in the Document File Encryption and Decryption

Jurnal Widya
Volume 5, Nomor 1, bulan April 2024: halaman 468-481
https://jurnal.amikwidyaloka.ac.id/index.php/awl
jurnal@amikwidyaloka.ac.id/
editor.jurnalwidya@gmail.com

P-ISSN: 2746-5411
E-ISSN: 2807-5528

Process," *J. Komputer, Inf. dan Teknol.*, vol. 2, no. 2, pp. 605–612, 2022, doi: 10.53697/jkomitek.v2i2.1041.

[15] T. S. Alasi and J. Sembiring, "Algoritma Blowfish Untuk Pengaman Pesan Teks," *J. Armada Inform.*, vol. 3, no. 1, pp. 215–223, 2019.