Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.1, Februari 2023

Program Aplikasi Algoritma *Blowfish* Pada Sistem Keamanan Data File

Blowfish Algorithm Application Program For Data File Security Systems

Ngarap Imanuel Manik[1], Hendrikus JuanFernando[2]

[1,2] Mathematics Departement, SoCS,Bina Nusantara University
Jl.Kebon Jeruk Raya no.27 Jakarta Barat, Indonesia

Corresponding author e-mail: manik@binus.ac.id

Received: November 20, 2022**. Revised:** December 28, 2022**. Accepted:** January 12, 2023**. Issue Period:** Vol.7 No.1 (2023),Pp.**10-21**

Abstrak: Berbagai macam layanan komunikasi tersedia di internet, diantaranya adalah web, email, milis, newsgroups, dan sebagainya. Dengan semakin maraknya orang memanfaatkan layanan komunikasi tersebut, maka permasalahan pun bermunculan, apalagi ditambah dengan adanya hacker dan cracker. Banyak orang kemudian berusaha menyiasati bagaimana cara mengamankan informasi yang dikomunikasikannya, atau menyiasati bagaimana cara mendeteksi keaslian dari informasi yang diterimanya. Untuk mengamankan data atau message diperlukan metode enkripsi yang pada makalah ini digunakan Algoritma Blowfish. Makalah ini menyajikan analisis kinerja Algoritma Blowfish dan perancangan program aplikasi untuk mengamankan suatu file data. Untuk menekripsi dan mendekripsi suatu file data, user harus menjalankan program aplikasi tersebut dan juga memberikan key sebagai kunci yang digunakan. Hasil penelitian menunjukkan bahwa program dapat digunakan untuk semua tipe file data tanpa ada kesalahan.

Kata kunci: : Criptografi, enkripsi, dekripsi, Algoritma Blowfish

Abstract: *Various kinds of communication services are available on the internet, including the web, email, mailing lists, newsgroups, and so on. With more and more people taking advantage of these communication services, problems have arisen, especially with the addition of hackers and crackers. Many people then try to figure out how to secure the information they communicate, or how to detect the authenticity of the information they receive. To secure data or messages, an encryption method is needed, which in this paper uses the Blowfish Algorithm. This paper presents an analysis of the performance of the Blowfish Algorithm and the design of an application program to secure a data file. To encrypt and decrypt a data file, the user must run the application program and also provide the key as the key used. The research results show that the program can be used for all types of data files without any errors.*

Keywords: *Cryptography, encryption, decryption, Blowfish Algorithm*

DOI: 10.52362/jisamar.v7i1.984

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.1, Februari 2023

I. PENDAHULUAN

Berbagai macam layanan komunikasi tersedia di internet, diantaranya adalah *web*, *email*, *milis*, *newsgroups*, dan sebagainya. Dengan semakin maraknya orang memanfaatkan layanan komunikasi tersebut, maka permasalahan pun bermunculan, apalagi ditambah dengan adanya *hacker* dan *cracker*. Banyak orang kemudian berusaha menyiasati bagaimana cara mengamankan informasi yang dikomunikasikannya, atau menyiasati bagaimana cara mendeteksi keaslian dari informasi yang diterimanya. Untuk lebih jelasnya akan digambarkan dalam suatu kasus berikut. Seorang pengirim pesan yang hendak mengirimkan suatu surat pesan kepada rekannya, menginginkan agar pesannya tidak dibaca oleh orang yang tidak berhak membacanya, padahal bila administrator *server* sedang iseng, sangat mungkin orang tersebut dapat membaca pesan yang bersangkutan. Penerima pun ingin mendapat keyakinan bahwa pengirimnya merupakan orang yang dikenalnya, bukan orang yang berpura-pura sebagai temannya.

Pada kenyataannya, ternyata keadaan seperti inilah yang terjadi pada masa sekarang ini. Perasaan khawatir dari pengirim pesan apakah pesannya benar-benar sampai ke pihak yang tepat, apakah pesannya tidak dibaca oleh pihak lain yang tidak berhak, serta berbagai kekhawatiran lainnya sering dirasakan oleh sang pengirim pesan. Begitu pula dengan penerima pesan, perasaan khawatir juga terjadi dalam dirinya, apakah pesan yang diterimanya benar-benar berasal dari pihak yang tepat, apakah pesannya tidak mengalami perubahan dan benar seperti apa yang telah dibuat oleh pengirim pesan, serta berbagai kekhawatiran lainnya. Oleh karena itu, perlu ada suatu cara agar berbagai perasaan khawatir itu hilang. Keaslian pesan yang dibuat oleh pengirim pesan harus benar-benar terjaga dan benar-benar sampai ke penerima pesan dalam bentuk yang sama, serta pesan tersebut tidak terbaca dan terjamah oleh pihak lain yang tidak berhak, harus dijadikan prioritas utama. Salah satu caranya adalah dengan menggunakan teknik kriptografi. [1]

Dengan adanya teknik kriptografi, berbagai kekhawatiran dan semua yang diharapkan oleh pengirim pesan maupun penerima pesan dapat teratasi. Salah satu dari teknik kriptografi adalah dengan menggunakan algoritma *Blowfish*. Algoritma *Blowfish* merupakan algoritma kriptografi yang cukup baik dan aplikatif. Program aplikasi yang akan dirancang nantinya adalah dengan menggunakan algoritma *Blowfish*. Dengan adanya program aplikasi ini diharapkan dapat mengatasi masalah seperti yang telah disebutkan di atas.[2][3]

Makalah ini membahas bagaimana menerapkan algoritma enkripsi dan dekripsi *Blowfish* melalui pembuatan program aplikasi sehingga dapat digunakan untuk berbagai keperluan pengiriman dan penerimaan pesan.

Algoritma *Blowfish*

Enkripsi Algoritma *Blowfish*

Blowfish adalah *cipher* blok 64-bit yang memiliki sebuah kunci yang panjangnya variabel. Algoritma *Blowfish* terdiri dari dua bagian yaitu *key expansion* dan enkripsi data. Blok diagram enkripsi algoritma *Blowfish* dapat dilihat pada gambar 1.[4][5]

Key expansion mengkonversikan sebuah kunci sampai 448 bit ke dalam beberapa *array subkey* dengan total 4168 byte. Enkripsi data terdiri dari sebuah fungsi yang sederhana dengan iterasi 16 kali. Setiap *round* mempunyai sebuah permutasi *key-dependent* dan sebuah subsitusi *key* dan *data-dependent*. Semua operasi, penjumlahan dan XOR pada word 32-bit. Hanya operasi tambahan di indeks empat yaitu *lookup data array per round*.

Blowfish menggunakan sejumlah *subkey* yang besar. *Key* ini harus dihitung awal sebelum enkripsi atau dekripsi.

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

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

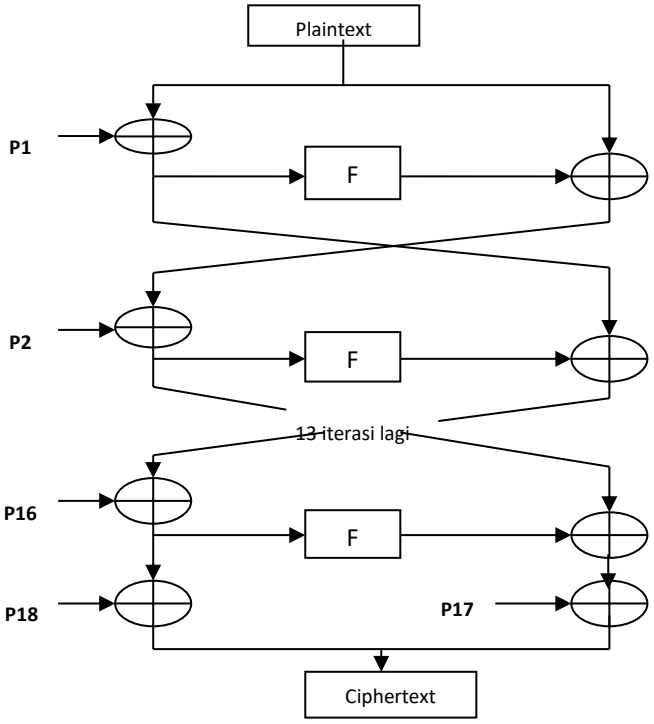
Empat *S-box* 32- bit mempunyai masing-masing 256 *entry* yaitu :

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

DOI: 10.52362/jisamar.v7i1.984

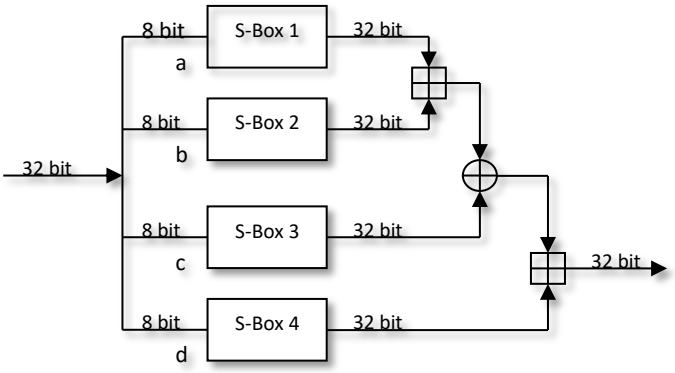
Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.1, Februari 2023

$S_{4,0}$, $S_{4,1}$, $S_{4,2}$, $S_{4,3}$, ...$S_{4,255}$



Gambar 1. Blok diagram Algoritma Enkripsi *Blowfish*

Blowfish adalah sebuah jaringan *Feistel* yang mempunyai 16 *round*. Inputnya adalah (x) element data 64-bit. Untuk mengenkripsi (x) yaitu :
Bagi (x) dalam dua bagian 32-bit menghasilkan (x_L) dan (x_R). Untuk i = 1 sampai 16 maka :
$x_L = x_L \oplus P_i$ dan $x_R = F(x_L) \oplus x_R$
Swap (tukar) x_L dan x_R dan *Swap* (tukar) x_L dan x_R (mengulang *swap* yang lalu)
$x_R = x_R \oplus P_{17}$ dan $x_L = x_L \oplus P_{18}$ kemudian Gabungkan kembali x_L dan x_R



Gambar 2 Fungsi F (Bruce Schneier: 1996)

Fungsi F di atas adalah sebagai berikut :
Bagi x_L dalam empat kuarter 8-bit yaitu a, b, c dan d seperti gambar 2 maka :

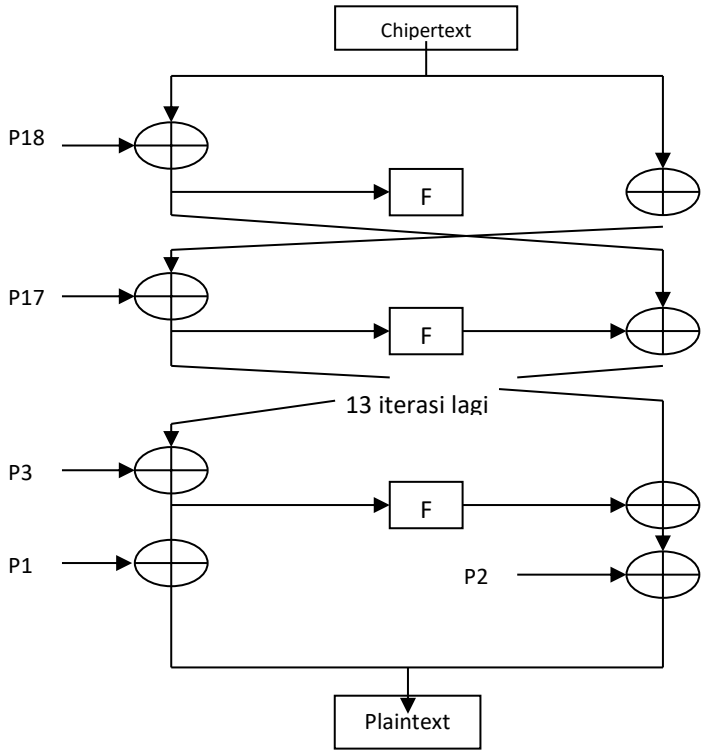
$$F(x_L) = ((S_{1,a} + S_{2,b} \bmod 2^{32}) \oplus S_{3,c}) + S_{4,d} \bmod 2^{32} \quad (1)$$

DOI: 10.52362/jisamar.v7i1.984

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.1, Februari 2023

Dekripsi Algoritma *Blowfish*

Dekripsi sama persis dengan enkripsi, kecuali bahwa P_1, P_2,…, P_{18} digunakan pada urutan yang berbalik (*reverse*). Blok diagram dekripsi seperti pada gambar 3.[8]



Gambar 3. Blok Diagram dekripsi *Blowfish*

Dengan membalikkan 18 *subkey* untuk medekripsi metode algoritma *Blowfish*. Pertama, masalah ini nampak tidak dapat dipercaya, karena ada dua XOR operasi yang mengikuti pemakaian f-fungsi yang sebelumnya, dan hanya satu yang sebelumnya pemakaian pertama f-fungsi. Meskipun jika kita memodifikasi algoritma tersebut sehingga pemakaian *subkey* 2 sampai 17 menempatkan sebelum *output* f-fungsi yang di-XOR-kan ke sebelah kanan blok dan dilakukan ke data yang sama sebelum XOR itu, walaupun itu berarti ia sekarang berada di sebelah kanan blok, karena XOR *subkey* tersebut telah dipindahkan sebelum *swap* (tukar) kedua belah blok tersebut (tukar separuh blok kiri dan separuh blok kanan). Kita tidak merubah suatu apapun karena informasi yang sama di-XOR-kan ke separuh blok kiri antara setiap waktu, informasi ini digunakan sebagai *input* f-fungsi. Kenyataannya, kita mempunyai kebalikan yang pasti dari barisan dekripsi.

II. METODE DAN MATERI

Secara garis besar program aplikasi ini terbagi atas dua proses diatas yaitu yaitu proses enkripsi dan proses dekrips , sehingga rancangan program yang lainnya mengikuti dua proses tersebut.[6][7]

1. Rancangan Layar Program

Perancangan program ini terbagi menjadi beberapa halaman layar, yaitu halaman pembuka, halaman utama, dan halaman penutup. Berikut penjelasan rancangan dari masing-masing halaman layar tersebut :

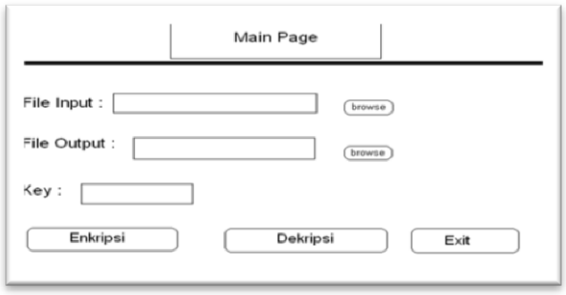
DOI: 10.52362/jisamar.v7i1.984

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.1, Februari 2023

- **Halaman Pembuka** ; Halaman ini berfungsi untuk memberikan informasi mengenai program apa yang akan dijalankan, garis besar *author* pembuat program, dan menghubungkannya dengan halaman utama.

Gambar 4. Rancangan Layar Halaman Pembuka

- **Halaman Utama ;** Halaman ini adalah halaman inti dari program aplikasi ini. Berikut bagian-bagian yang terdapat pada halaman ini :
  - Judul, menerangkan program aplikasi yang sedang digunakan.
  - *Static Text File Input*, memberikan informasi nama *file* yang akan dijadikan *file input*.
  - *Button Browse File Input*, memilih *file* yang akan dijadikan *file input*.
  - *Static Text File Output*, memberikan informasi nama *file* yang akan dijadikan *file output*.
  - *Button Browse File Output*, membuat dan memberi nama *file output*.
  - *Static Text Key*, memasukkan *key* yang akan dijadikan *key* untuk proses enkripsi atau dekripsi.
  - *Button* Enkripsi, menjalankan proses enkripsi.
  - *Button* Dekripsi, menjalankan proses dekripsi.
  - *Button* Exit, keluar dari program aplikasi.



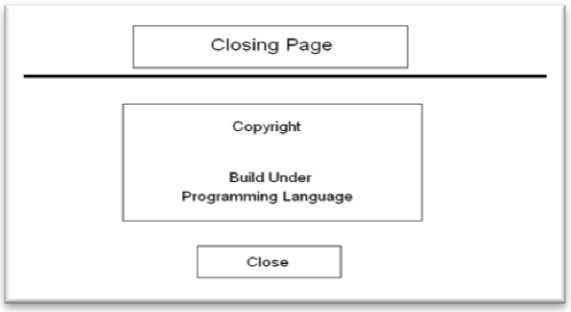
Gambar 4. Rancangan Layar Halaman Utama

- **Halaman Penutup**

Halaman ini berfungsi sebagai penutup program aplikasi dan info-info yang terdapat dalam pembuatan program.

DOI: 10.52362/jisamar.v7i1.984

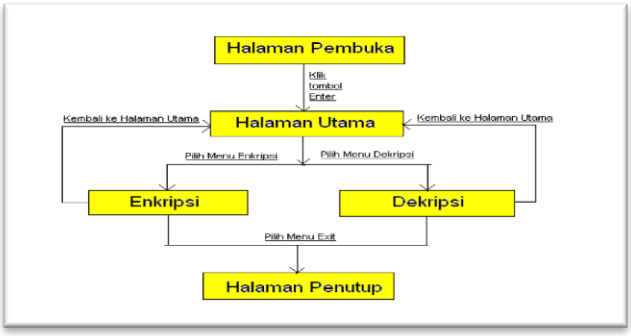
Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.1, Februari 2023



Gambar 5. Rancangan Layar Halaman Penutup

State Transition Diagram

State Transition diagram untuk proses di atas dapat dilihat seperti yang ditunjukkan pada gambar 6.

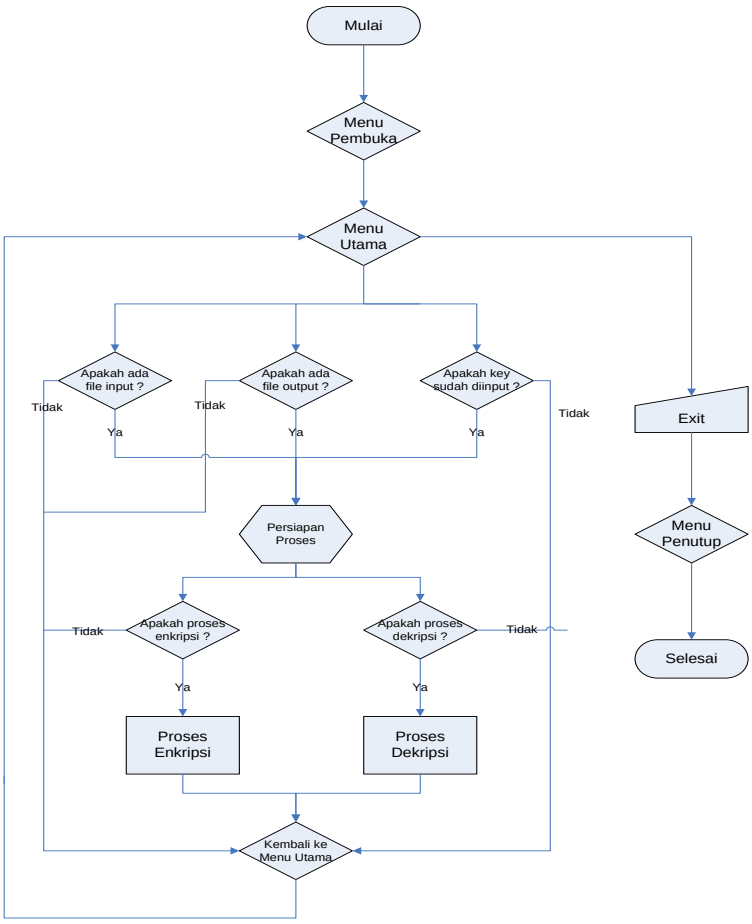


Gambar 6. *State Transition Diagram*

Secara keseluruhan program menegrjakan Langkah-langkah demi Langkah seperti yang ditampilkan dalam flowchart program pada gambar 7.

DOI: 10.52362/jisamar.v7i1.984

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.1, Februari 2023



Gambar 7. Flowchart Program secara Keseluruhan

III. PEMBAHASAN DAN HASIL

Untuk dapat menjalankan program aplikasi ini, dibutuhkan perangkat keras dan lunak yang memiliki spesifikasi sebagai berikut :

- CPU Intel Pentium 4 Core2Duo T7250 2.0GHz cache 2mb.
- Memory RAM 1GB DDR2.
- Hard Disk 120GB SATA.
- Monitor dengan resolusi 1280 x 800 pixels.
- VGA card nVIDIA GeForce 8600M.

Spesifikasi Perangkat Lunak yang Dibutuhkan

Spesifikasi dari perangkat lunak yang digunakan dalam pengembangan dan pengujian program aplikasi ini adalah sebagai berikut :

- Operating System : Microsoft Windows XP.
- Compiler Software : Microsoft Visual C++ 6.0.

Persiapan Data

Sebelum menjalankan program aplikasi ini, maka perlu disiapkan terlebih dahulu *file input* yang hendak dijadikan *plaintext* yang nantinya akan dienkripsi menjadi *file output* atau *chipertext*. Hampir semua *file* dapat dienkripsi dengan program aplikasi ini, hanya saja semakin besar ukuran *file* maka semakin lama pula waktu yang dibutuhkan untuk proses enkripsi.

DOI: 10.52362/jisamar.v7i1.984

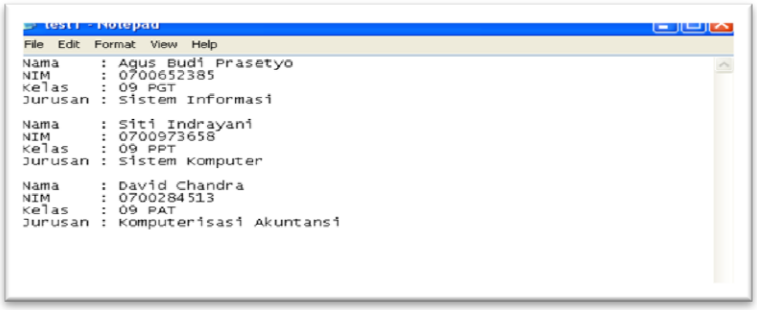
Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.1, Februari 2023

Pengujian Program Aplikasi

Program aplikasi ini dapat dioperasikan dengan menjalankan *file* Blowfish.exe. Setelah menjalankan *file* tersebut, maka akan tampil halaman pembuka, dan selanjutnya halaman utama. Berikut akan diberikan beberapa contoh penggunaan program aplikasi ini dengan menggunakan beberapa tipe *file input* :

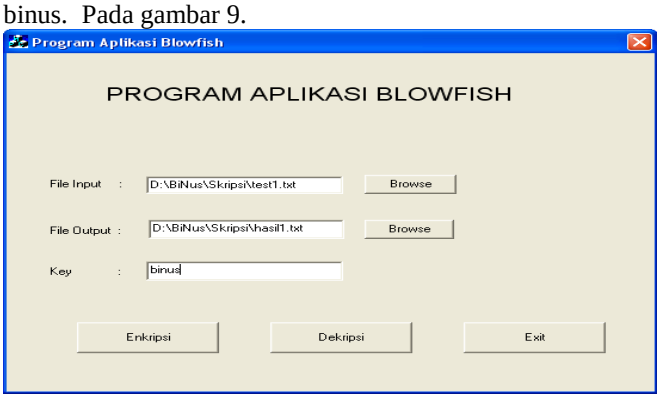
Menggunakan File Teks

Contoh berikut ini menggunakan *file input* berupa *file* bertipe teks dengan nama test1.txt. pada gambar 8.



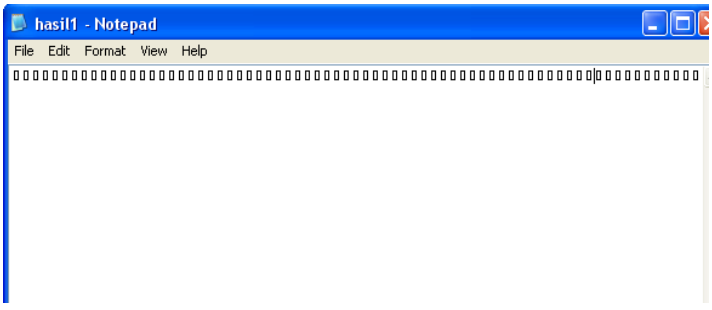
Gambar 8. *Preview file* test1.txt sebelum enkripsi

Kemudian program dijalankan dan diatur sehingga *file output* yang dihasilkan bernama hasil1.txt. *Key* yang digunakan contohnya adalah binus. Pada gambar 9.



Gambar 9. *Preview* program enkripsi test1.txt menjadi hasil1.txt

Setelah memilih enkripsi, maka akan tercipta sebuah *file* baru sebagai *file output* yang bernama hasil1.txt dengan isi yang sudah tidak terbaca seperti gambar 10.

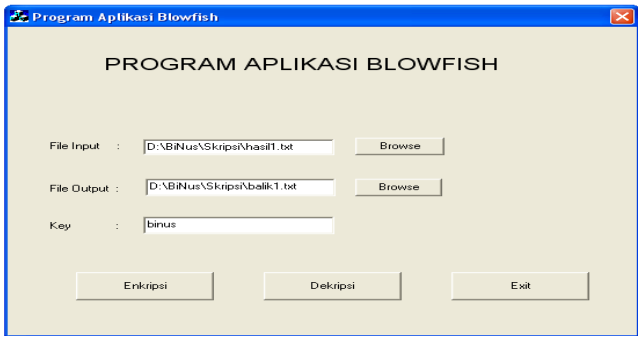


Gambar 10. *Preview* hasil1.txt hasil enkripsi dari test1.txt

DOI: 10.52362/jisamar.v7i1.984

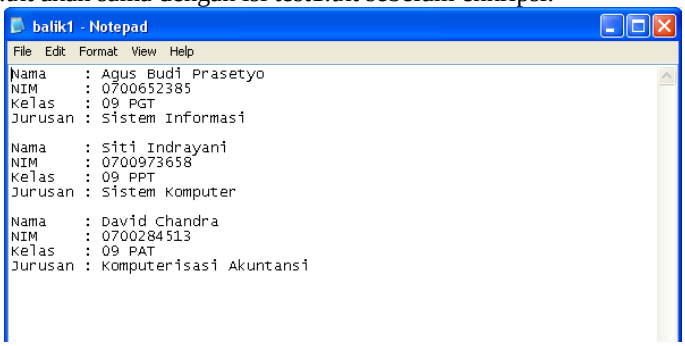
Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.1, Februari 2023

Untuk mengembalikannya seperti semula sehingga dapat dibaca kembali, maka program aplikasi dapat dijalankan kembali dengan menggunakan *key* yang sama. Hasil dekripsi dinamakan dengan balik1.txt. pada gambar 11.



Gambar 11. *Preview* program dekripsi hasil1.txt menjadi balik1.txt

Isi dari balik1.txt akan sama dengan isi test1.txt sebelum enkripsi.



Gambar 12. *Preview file* balik1.txt hasil dekripsi dari hasil1.txt

Menggunakan File *Image*

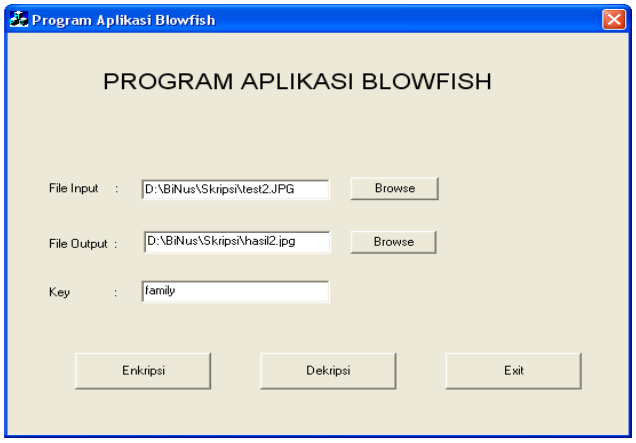
Contoh berikut ini menggunakan *file input* berupa *file* bertipe *image* dengan nama test2.jpg seperti gambar 13.

Gambar 13 *Preview file* test2.jpg sebelum enkripsi

Kemudian program dijalankan dan diatur sehingga *file output* yang dihasilkan bernama hasil2.jpg. *Key* yang digunakan contohnya adalah *family*.

DOI: 10.52362/jisamar.v7i1.984

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.1, Februari 2023

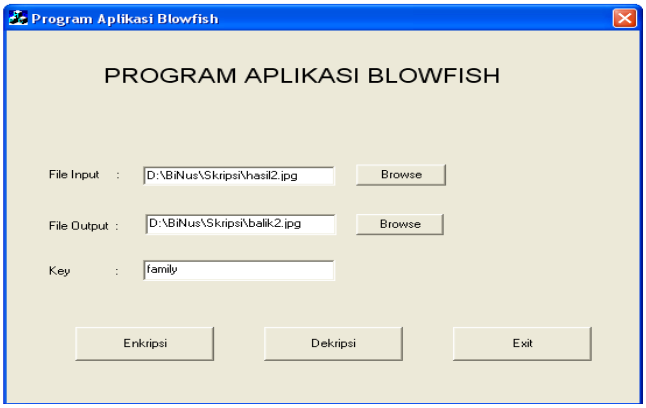


Gambar 14. *Preview* program enkripsi test2.jpg menjadi hasil2.jpg

Setelah memilih enkripsi, maka akan tercipta sebuah *file* baru sebagai *file output* yang bernama hasil2.jpg dengan isi yang sudah tidak terbaca.

Gambar 15. *Preview* hasil2.jpg hasil enkripsi dari test2.jpg

Untuk mengembalikannya seperti semula sehingga dapat dibaca kembali, maka program aplikasi dapat dijalankan kembali dengan menggunakan *key* yang sama. Hasil dekripsi dinamakan dengan balik2.jpg. (gambar 16)



Gambar 16. *Preview* program dekripsi hasil2.jpg menjadi balik2.jpg

Isi dari balik2.jpg akan sama dengan isi test2.jpg sebelum enkripsi, pada gambar 17

DOI: 10.52362/jisamar.v7i1.984

Journal of Information System, Applied, Management, Accounting and Research.
http://journal.stmikjayakarta.ac.id/index.php/jisamar ,
jisamar@stmikjayakarta.ac.id , jisamar2017@gmail.com
e-ISSN: 2598-8719 (Online), p-ISSN: 2598-8700 (Printed) , Vol. 7 No.1, Februari 2023

Gambar 17. *Preview file* balik2.jpg hasil dekripsi dari hasil2.jpg

Selain melakukan percobaan dengan dua tipe data diatas (*text file* dan *image file*), program aplikasi juga dicoba untuk menekripsi dan mendekripsi tipe data yang lain. Berikut hasil percobaan program dengan beberapa *file* lain.

Tipe *File*	Ukuran *File*	Waktu	Status
Text Document	1 kb	Seketika	Berhasil
Microsoft Word Document	146 kb	0.3 detik	Berhasil
JPEG Image	256 kb	0.5 detik	Berhasil
Adobe Acrobat Document	389 kb	0.7 detik	Berhasil
MP3 Format Sound	4.49 mb	7 detik	Berhasil
FLV File	6.96 mb	11 detik	Berhasil
WMV File	16.9 mb	26 detik	Berhasil
DIVX File	50.9 mb	1 menit 26 detik	Berhasil

Dari hasil percobaan di atas, terlihat bahwa program dapat digunakan untuk berbagai macam tipe *file* data, hanya saja semakin besar ukuran *file* tersebut maka semakin lama waktu yang dibutuhkan dalam proses programnya

Kelebihan dan Kekurangan Program Aplikasi

Program aplikasi ini memiliki beberapa kelebihan dan juga kekurangan. Kelebihan-kelebihan dari program aplikasi ini diantaranya :

- Menggunakan algoritma enkripsi *Blowfish* yang kuat dalam hal pengamanan data.
- Waktu yang digunakan relatif cepat untuk *file-file* bertipe dan berukuran standar.
- Tampilannya sederhana sehingga sangat mudah untuk dimengerti.
- Ukuran hasil *file output* relatif sama dengan *file input.*

Selain kelebihan, tentunya program aplikasi ini juga masih memiliki beberapa kekurangan, diantaranya :

- Untuk *file* yang berukuran besar, waktu yang dibutuhkan relatif lama.
- Kurang baik untuk jenis-jenis *file* tertentu.
- Untuk *file-file* lain yang belum dicoba, hasil *file output* belum dapat diketahui.

IV. KESIMPULAN

Setelah melakukan perancangan program aplikasi dan implementasi program tersebut, maka dapat disimpulkan bahwa program aplikasi ini dapat digunakan untuk berbagai macam tipe *file* data, diantaranya *file* bertipe teks, *sound*, *video*, dan sebagainya. Kemudian hasil yang diinginkan relatif dapat tercapai dengan baik. Aplikasi algoritma *Blowfish* pada

DOI: 10.52362/jisamar.v7i1.984

perancangan program aplikasi dapat berjalan dengan baik, artinya sebuah data dapat disamarkan dan dikembalikan seperti semula dan semakin besar ukuran suatu file data maka semakin lama pula waktu yang diperlukan untuk proses enkripsi maupun dekripsi yang dijalankan.

REFERENSI

[1] Ahmad Ibnu Riza ,Athoillah Islamy (2020), "Spatial Analysis Of Sustainable Land Use Development Coastal Areas In Batanng Regency", Bappenas Working Papers Volume III No. 1 – Maret 2020, p 42-53

[2] Angga Danimartiawan, dkk, (2002), *IPsec:"*Aplikasi Teknik Kriptografi untuk Keamanan Jaringan Komputer", makalah tidak diterbitkan

[3] Kurniawan, Yusuf, (2004), *Kriptografi : keamanan internet dan jaringan komunikasi*, Informatika, Bandung.

[4] Neha Khatri and Valmik. (2015), "Blowfish Algorithm" , International Journal of Engineering Sciences & Management Research (IJESMR), 2 (10), p: 45-50,

[5] Pia Singh, (2015), "Image -Encryption and Decryption using Blowfish-Algorithm in Matlab", https://www.ijser.org/research

[6] Pahrul Irfan, at al, (2022), "Application of the Blowfish Algorithm in Securing Patient Data in the Database", Matrix: Jurnal Manajemen Teknologi dan Informatika Volume 12 Issue 2 Year 2022 p 102-108.

[7] Yongki Iswo, Poltak Sihombing, (2016), "Combination of AES Algorithm with Blowfish Algorithm for File Attachment at E-Mail Sending", Jurnal Methodika, Vol. 2 No. 1 Maret 2016 ISSN : 2442-7861, p:96-101 https://ejurnal.methodist.ac.id

[8] Veena Parihar , Aishwary Kulshrestha, (2016), "Blowfish Algorithm : A Detailed Study", International Journal For Technological Research In Engineering Volume 3, Issue 9, May-2016. p 2253-2255

DOI: 10.52362/jisamar.v7i1.984