25. Penerapan Kriptografi Algoritma Blowfish pada Pengamanan Pesan Data Teks

by Much Aziz Muslim

Submission date: 23-Jul-2019 03:44PM (UTC+0700)
Submission ID: 1154296517
File name: iptografi_Algoritma_Blowfish_pada_Pengamanan_Pesan_Data_Teks.pdf (963.4K)
Word count: 2888
Character count: 18880

Techno.COM, Vol. 16, No. 4, November 2017 : 358-366

Penerapan Kriptografi Algoritma *Blowfish* pada Pengamanan Pesan Data Teks

Implementation Of Blowfish Algorithm Cryptography On Text Message Data Security

Budi Prasetiyo[1], Much Aziz Muslim[2], Hendi Susanto[3]
[1,2,3]Prodi teknik Informatika, FMIPA Universitas Negeri Semarang
e-mail: [1*]budipras@mail.unnes.ac.id, [2]a212muslim@yahoo.com, [3]hendi.susanto@outlook.com

Abstrak

Kriptografi dibutuhkan untuk pengamanan data dalam jaringan komunikasi. Artikel ini membahas implementasi algoritma Blowfish menggunakan Microsoft Visual Basic. Permasalahan pada tulisan ini bagaimana penerapan algoritma blowfish pada pengamanan dayta teks dan bagaiaman performa algoritma dalam mengkesekusi proses enkripsi maupun deksripsi. Metode yang digunakan yaitu menggunakan SDLC dengan membangun perangkat lunak menggunakan Visual Basic. Algoritma kriptografi yang digunakan yaitu Blowfish. Data uji menggunakan beberapa file dengan ukuran berbeda mulai dari 64Kb, 128Kb, 256Kb, 512Kb, dan 1024Kb. Berdasar hasil implementasi algoritma Blowfish menggunakan MS Visual data berhasil dienkripsi maupun didekripsi dan dapat kembali seperti semula, sehingga dapat digunakan untuk melakukan pengamanan data. Hasil pengujian waktu eksekusi menunjukkan proses enkripsi membutuhkan waktu yang lebih lama daripada proses dekripsi. Data yang diperoleh menunjukkan proses deksripsi 33% lebih cepat daripada proses enkripsi.

Kata kunci— kriptografi, enkripsi, deksripsi, *Blowfish*

Abstract

Cryptography is required for data security in communication networks. This article discusses the implementation of Blowfish algorithm using Microsoft Visual Basic. The problem in this paper is how to apply blowfish algorithm to safeguarding text harita and how to perform algorithm performance in encryption process encryption and description. The method used is using SDLC by building software using Visual Basic. The cryptographic algorithm used is Blowfish. The test data uses several files of different sizes ranging from 64Kb, 128Kb, 256Kb, 512Kb, and 1024Kb. Based on the results of Blowfish algorithm implementation using MS Visual data successfully encrypted and decrypted and can return as before, so it can be used to perform data security. The test results of the execution time depends on the process. Data generated 33% faster descriptor process.

Keywords— *cryptography, encryption, description, Blowfish*

1. PENDAHULUAN

Saat ini internet sudah tidak lagi menjamin penyediaan informasi yang aman [1]. Beberapa mesin pencarian yang terus berkembang menjadikan informasi bersifat publik, disamping itu munculnya isu-isu keamanan seperti virus, penyadap, *spam* maupun *hacker* dapat mengambil data-data yang bersifat rahasia [2]. Permasalahan keamanan maupun kerahasiaan data menjadi hal yang peting dari suatau data. Sehingga, proses pengiriman data maupun penyimpanan data membutuhkan suatu cara yang dapat menjamin keamanan data tersebut. Salah satu teknik untuk pengamanan data contohnya adalah kriptografi. Pada kriptografi data diubah menjadi bentuk bentuk lain, yaitu dengan proses enkripsi-dekripsi (penyandian). Enkripsi dilakukan ketika data akan dikirim. Proses ini akan mengubah suatu data asli menjadi data rahasia yang tidak dapat dibaca. Sementara itu, proses dekripsi dilakukan

oleh penerima data. Data rahasia yang diterima diubah kembali menjadi data asli menggunakan kunci.

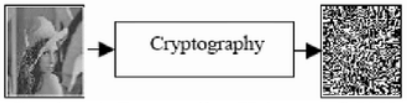
Berbagai cara terus dikembangkan untuk meningkatkan pengamanan data, diantaranya kriptografi. Kriptografi dilakukan dengan cara mengacak pesan sehinggatidak dapat terbaca [3]. Dengan cara penyandian ini, data asli tidak akan terbaca oleh pihak yang tidak berkepentingan [4]. Dalam kriptografi terdapat beberapa algoritma penyandian data. Algoritma kunci simetri termasuk algoritma yang masih sering digunakan dalam algoritma kriptografi. Algoritma kunci simetri [5] yang juga dikenal dengan *single -key* (kunci tunggal) atau *private key* (kunci privat) merupakan bagian dari algoritma kriptografi, dimana menggunakan kunci (privat) dan algoritma (publik) untuk melakukan enkripsi maupun dekripsi. Beberapa jenis algoritma kunci simetri yang populer diantaranya DES [6], TDES [7], Blowfish [8], CAST5 [9], IDEA [10], TEA [11], AES (alias Rijndael) [12,13], Twofish [14], RC6, dan Serpent. Implementasi algoritma kriptografi diantaranya Sitinjak yang menggunakan algoritma Blowfish [15], Muslim [16] melakukan implementasi algoritma *Twofish* menggunakan *library chilkat encryption activeX*, dan penelitian sebelumnya Alamsyah [17] melakukan kombinasi steganografi dengan kriptografi. Pada penelitian sebelumnya [23] menggunakan kriptografi kunci publik algoritma RSA-CRT untuk aplikasi instant messaging. Sedangkan pada [24] melakukan kombinasi antara steganografi dengan kriptografi DES untuk pengamanan data.

Pada artikel ini menggunakan algoritma *Blowfish* untuk pengamanan data teks. *Blowfish* merupakan algoritma kunci simetrik *cipher* blok yang dirancang pada tahun 1993 oleh Bruce Schneier. Pada saat itu banyak sekali rancangan algoritma yang ditawarkan, namun hampir semua terhalang oleh paten atau kerahasiaan pemerintah Amerika. Schneier menyatakan bahwa *Blowfish* bebas paten dan akan berada pada domain publik. Keamanan *Blowfish* terletak pada ukuran kunci variabel (128-448 bit) sehingga menyediakan tingkat keamanan yang tinggi. Berdasarkan uraian di atas, perlu dilakukan penelitian terhadap proses penyandian algoritma *Blowfish* serta implementasinya pada sebuah program komputer MS Visual Basic.

2. METODE PENELITIAN

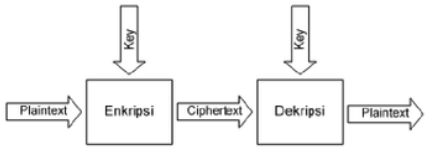
2.1 Kriptografi

Kriptografi berasal dari dua kata Yunani, yaitu "*cryptó*" yang berarti rahasia dan "*graphy*" yang berarti menulis. Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data [18]. Penyandian kriptografi seperti pada Gambar 1.



Gambar 1. Penyandian Kriptografi [19]

Cryptographic system atau *cryptosystem* adalah suatu fasilitas untuk mengkonversikan *plaintext* ke *ciphertext* dan sebaliknya. Kriptografi pada dasarnya terdiri dari dua proses, yaitu proses enkripsi dan proses dekripsi. Proses enkripsi adalah proses penyandian pesan terbuka menjadi pesan rahasia (*ciphertext*). *Ciphertext* inilah yang nantinya akan dikirimkan melalui saluran komunikasi terbuka. Pada saat *ciphertext* diterima oleh penerima pesan, maka pesan rahasia tersebut diubah lagi menjadi pesan terbuka melalui proses dekripsi sehingga pesan tadi dapat dibaca kembali oleh penerima pesan. Secara umum, proses enkripsi dan dekripsi dapat digambarkan sebagai berikut.



Gambar 2. Proses enkripsi dan dekripsi

2.2 Algoritma *Blowfish*

Algoritma *Blowfish* diciptakan oleh Bruce Schneier, seorang *Cryptanalyst* dan Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang kriptografi dan keamanan komputer) dan dipublikasikan tahun 1994. Dibuat untuk digunakan pada komputer yang mempunyai microposesor besar (32-bit keatas dengan cache data yang besar). Blowfish merupakan algoritma yang tidak dipatenkan dan tersedia secara gratis untuk berbagai macam kegunaan.

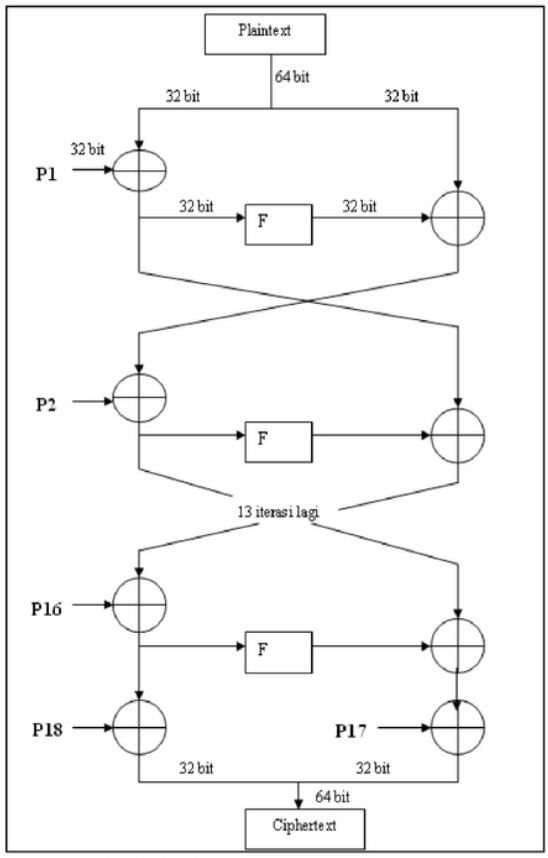
Algoritma *Blowfish* terdiri atas dua bagian, yaitu ekspansi kunci dan enkripsi data [20], yaitu Ekspansi kunci (*Key-expansion*) dan enkripsi data. *Blowfish* merupakan blok *cipher* 64-bit. Algoritma ini terdiri dari dua bagian:

1) *Key expansion* atau perluasan kunci
   Key *expansion* merubah kunci yang dapat mencapai 448 bit menjadi beberapa *array* sub kunci (*subkey*) dengan total 4168 *byte*.
2) Enkripsi data
   Enkripsi data terdiri dari iterasi fungsi sederhana sebanyak 16 kali. Masukannya adalah data X yang terdiri dari 64 bit. Setiap putaran terdiri dari permutasi kunci-*dependent* dan substitusi kunci- dan data-*dependent*. Semua operasi adalah penambahan dan XOR pada variabel 32-bit.

Proses enkripsi *Blowfish* sebagai berikut.

1. Bagi X menjadi dua bagian yang masing-masing terdiri dari 32-bit: XL, XR.
2. Lakukan langkah berikut
   For i = 1 to 16:
   XL = XL $\oplus$ Pi
   XR = F(XL) $\oplus$ XR
   Tukar XL dan XR
3. Setelah iterasi ke-16, tukar XL dan XR lagi untuk melakukan membatalkan pertukaran terakhir.
4. Lalu lakukan
   XR = XR $\oplus$ P17
   XL = XL $\oplus$ P18
5. Terakhir, gabungkan kembali XL dan XR untuk mendapatkan *ciphertext*.

Blok diagram algoritma enkripsi *Blowfish* ditunjukkan pada Gambar 1.



Gambar 1. Blok diagram algoritma enkripsi *Blowfish*.

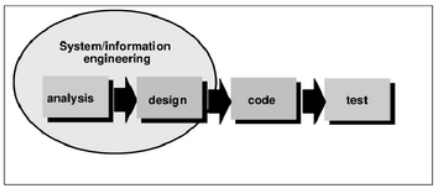
Pada Proses Dekripsi, langkah sama persis dengan proses enkripsi, hanya saja urutan Pbox digunakan dengan urutan terbalik.

2.3 Visual Basic

Visual Basic adalah salah satu produk bahasa pemrograman yang dikeluarkan Microsoft, salah satu perusahaan *software* terkemuka di dunia. Visual Basic merupakan bahasa pemrograman yang mudah digunakan untuk pengembangan sistem, baik itu sistem kecil maupun sistem besar. Dengan banyaknya komponen kontrol yang disediakan oleh Visual Basic, membuat *programmer* dan para pengembang sistem lebih mudah dalam pembuatan sistem. Visual Basic banyak dipakai oleh *programmer* dan para pengembang sistem, karena kemudahan yang ditawarkan. Dalam pengembangan sistem, para *programmer* tidak terlalu dipusingkan dengan tampilan program, karena Visual Basic menyediakan banyak komponen kontrol untuk desain tampilan dari program, dengan Visual Basic dapat dikembangkan berbagai jenis sistem, seperti sistem *database*, jaringan internet, multimedia grafik, dan lainnya [21].

Langkah Penelitian

Pada penelitian ini dibangun suatu perangkat lunak kriptografi mengacu pada metode SDLC (*System Development Life Cycle)*. SDLC membagi penelitian menjadi 4 tahap yaitu: (1) *analysi*s, (2) *design*, (3) *code,* dan (4) *test*) [22] yang ditunjukkan pada Gambar 3.



Gambar 3. Langkah penelitian SDLC [21]

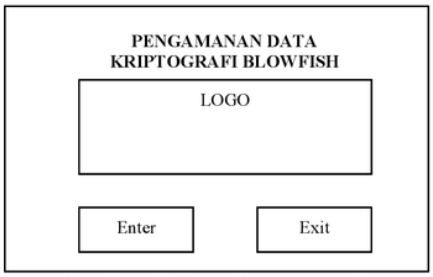
1) *Analysis* - Analisa Kebutuhan

Pada tahap analisa kebutuhan dilakukan studi literatur dan pengumpulan informasi mengenai proses yang akan digunakan untuk membangun model kriptografi yang meliputi:

a. Analisis kebutuhan perangkat lunak
b. Algoritma *Blowfish*
c. Pengamanan data

2) *Design* - Perancangan

Perancangan adalah proses penterjemahan sistem sesuai algoritma yang digunakan. Hal ini bertujuan agar program yang dibuat sesuai dengan hasil analisa kebutuhan. Hasil perancangan adalah bagan proses, *Data Flow Diagram* (DFD), dan perancangan antarmuka (*interface*). Perancangan halaman awal seperti Gambar 4.



Gambar 4. Tampilan antramuka

Halaman awal program terdiri dari logo dan 2 buah tombol menu, yaitu menu *Enter* yang digunakan untuk masuk ke program dan menu *Exit* untuk keluar dari program.

3) ***Code* - Pengkodean**

Tahap pengkodean merupakan tahap penterjemahan desain program yang telah dibuat ke dalam bentuk perintah-perintah yang dimengerti komputer. Pada penelitian ini dilakukan penulisan kode program sesuai pada langkah desain dengan menggunakan *software* Visual Basic. Pada pengkodean juga dibuat antarmuka sistem untuk mempermudah interaksi antara program dengan *user*.

4) *Test* - Pengujian

Pada penelitian ini pengujian program dilakukan dengan memberikan masukan (*input*) dengan beberapa macam kasus yang mungkin akan ditemukan. Masukan yang digunakan untuk pengujian pada penelitian ini berupa data teks sebagai pesan rahasia. Adapun metode pengujian yang digunakan pada perangkat lunak ini adalah metode pengujian *black box,* yang berfokus pada persyaratan fungsional perangkat lunak [22].

3. HASIL DAN PEMBAHASAN

Hasil implementasi ini adalah aplikasi sistem pengamanan data menggunakan algoritma *Blowfish* yang dibangun dengan program Microsoft Visual Basic 6.0. Pada halaman muka (*interface)* langsung menampilkan inputan enksripsi dan dekripsi. Penulis membagi sistem menjadi dua buah proses, yaitu proses enkripsi yang mana berfungsi mengubah *plaintext* menjadi *ciphertext* dan proses dekripsi yang mana berfungsi mengubah *ciphertext* menjadi *plaintext*. Selanjutnya dilakukan pengujian dengan masukan beberapa file untuk dilakukan proses endkripsi dan dekripsi.

1) Proses enkripsi

Proses enkripsi yaitu proses perubahan pesan terbuka yang dapat dibaca (*plaintext*) menjadi informasi yang tidak dapat kita pahami isinya (*ciphertext*). Pada sistem ini penulis menggunakan algoritma kriptografi *Blowfish* untuk melakukan proses enkripsi. *Plaintext* akan dienkripsi menjadi informasi/pesan yang tidak dapat dimengerti. Hasil program yang sudah dibuat kemudian diujicoba untuk melakukan proses enkripsi sebagai berikut.

a. Input *plaintext*:

   Algoritma Blowfish diciptakan oleh Bruce Schneier, seorang Cryptanalyst dan Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang kriptografi dan keamanan komputer) dan dipublikasikan tahun 1994

b. Input kunci: *secretkey8980YhsklMls*

c. Hasil enkripsi sebagai berikut

—————————————,Ò±´õÂNí©Ïl~o£ä,Ãc8d+X[%•-
ýÈà"6[žu5#±¼æ[œÇå• c§xx¡´ês®™›F¦3B ÿ$Ùc–·Ì«ª¿ìÑ7´jðÂÎ• «ù‡3¹wÐwÜ2+¡(,0DLÊw6Rj,?ÄÜ…zŒ—
[YûÔAÖíNëŒÿv/Ft ä
ê‰,¯ #è§Ðw±• xÜÙJ(¼€uM+ÏÛ°• =Nkž¼}0Áázcè¦â 9ÉýwŠ•VF‰Hÿ™'ºsMâ0; s‹A ú)<üU3æ• ë·Oà9ç´Æ¨ÂÐ#
Œn

Dalam format format base64, hasil enkripsi sebagai berikut.

A4LSsbT1wk7tqRwOz0l+b6PkLMNjOGQrHAlYWyWVH/3l4Cl2W551NSOxvOZbnMflgWMbpwV4eKG0
6nOumZtGpjNCCv8k2WOWt8yrqr/s0Te0GWrwws6Qq/mHM7l30HcR3DlrOwEoBYlwREzKdzYPUmosPxTE3l
V6jJcBW1n7BtRB1u1O64z/di9GdAzkDeqJLK8j6KfQd7GBeNwg2QxKKLyAdRpNDCvP27Cd
PU5rnrx9MMHlemPoz6bioDnl/XeKlVZGiUj/mZGTEHMRTeUwO6AMF3OLF0Gg+ik8/FUzEAzmfxbr
t0/gOee0xqjC0COMbgAkEiLgcCEmODM/1jC04VQlZStWPfXV4xrN7QbjsQiD5JafcfM40pR2EV8F
GGARXM68xhGo8KUcBmrU7onG/s4slVmSNgssz6/XhuqzI6+cfx2fXyjoPEznabhMC244oJwwYNx2
fWN7CkmecjOL1tKpvm976cMWtdOY29L4/g3FA0FSZJvve65m+vmFzz0grscLbeaFJuCs+KLT0kip
Dmtg5YZ3/CbCAVvtJJCIGGTMbSWaTRnMPZ1f7fN/qvwXWYwlylqYW1nR/LFcD49jd+2JT00QZMqd
tMtLKnfXPhd00lbOxBk9UPZceq+jmveHTNZhjkOv

2) Proses Dekripsi

Dekripsi merupakan proses pengembalian berkas *ciphertext* menjadi berkas *plaintext*. Jadi secara umum proses dekripsi merupakan kebalikan dari proses enkripsi. *Ciphertext* akan di dekripsi menggunakan algoritma *Blowfish*.

Hasil program yang sudah dibuat kemudian diujicoba untuk melakukan proses enkripsi sebagai berikut.

a. Input *ciphertext*:

A4LSsbT1wk7tqRwOz0l+b6PkLMNjOGQrHAlYWyWVH/3l4Cl2W551NSOxvOZbnMflgWMbpwV4eKG0
6nOumZtGpjNCCv8k2WOWt8yrqr/s0Te0GWrwws6Qq/mHM7l30HcR3DlrOwEoBYlwREzKdzYPUmosPxTE3l
V6jJcBW1n7BtRB1u1O64z/di9GdAzkDeqJLK8j6KfQd7GBeNwg2QxKKLyAdRpNDCvP27Cd
PU5rnrx9MMHlemPoz6bioDnl/XeKlVZGiUj/mZGTEHMRTeUwO6AMF3OLF0Gg+ik8/FUzEAzmfxbr
t0/gOee0xqjC0COMbgAkEiLgcCEmODM/1jC04VQlZStWPfXV4xrN7QbjsQiD5JafcfM40pR2EV8F
GGARXM68xhGo8KUcBmrU7onG/s4slVmSNgssz6/XhuqzI6+cfx2fXyjoPEznabhMC244oJwwYNx2
fWN7CkmecjOL1tKpvm976cMWtdOY29L4/g3FA0FSZJvve65m+vmFzz0grscLbeaFJuCs+KLT0kip
Dmtg5YZ3/CbCAVvtJJCIGGTMbSWaTRnMPZ1f7fN/qvwXWYwlylqYW1nR/LFcD49jd+2JT00QZMqd
tMtLKnfXPhd00lbOxBk9UPZceq+jmveHTNZhjkOv

b. Input kunci: *secretkey8980YhsklMls*

c. Melakukan proses dekripsi. Hasil dekripsi sebagai berikut.

Algoritma Blowfish diciptakan oleh Bruce Schneier, seorang Cryptanalyst dan Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang kriptografi dan keamanan komputer) dan dipublikasikan tahun 1994

Dari pengujian yang telah dilakukan penulis, dapat menunjukkan bahwa data berhasil dienkripsi dan menghasilkan *ciphertext* yang bersifat rahasia, begitu pula saat proses dekripsi. *Ciphertext* berhasil didekripsi dan pesan dapat kembali seperti semula.

3) Hasil pengujian proses enkripsi dan deksripsi

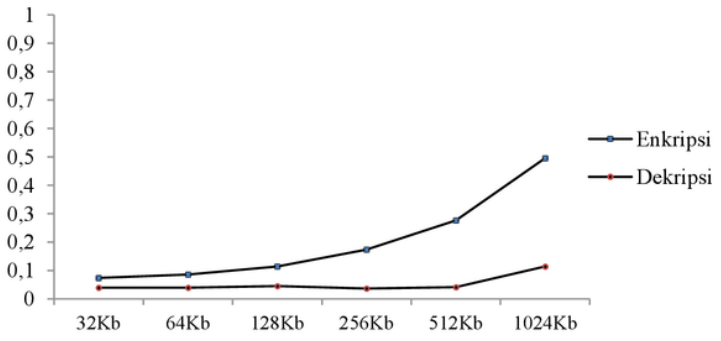
Pengujian selanjutnya yaitu untuk menganalisa kecepatan proses enkripsi dan deksripsi. Pengujian dilakukan dengan menggunakan beberapa buah file dengan ukuran yang berbeda-beda menggunakan komputer dengan spesifikasi Corei3 2,4 Ghz. Hasil pengujian proses enkripsi ditunjukkan pada Tabel 1, sedangkan waktu proses deksripsi ditunjukkan pada Tabel 2. Adapun grafik dari kedua proses tersebut dapat dilihat pada Gambar 5.

Tabel 1. Waktu ekseskusi proses enkripsi

Ukuran file	Waktu enkripsi (s)				Rata-rata
	Pengujian 1	Pengujian 2	Pengujian 3	Pengujian 4	
32Kb	0,168	0,044	0,048	0,036	0,07400
64Kb	0,161	0,065	0,061	0,058	0,08625
128Kb	0,19	0,085	0,089	0,091	0,11375
256Kb	0,256	0,150	0,146	0,141	0,17325
512Kb	0,360	0,253	0,247	0,245	0,27625
1024Kb	0,598	0,464	0,462	0,458	0,49550

Tabel 2. Waktu ekseskusi proses dekripsi

Ukuran file	Waktu dekripsi (s)				Rata-rata
	Pengujian 1	Pengujian 2	Pengujian 3	Pengujian 4	
32Kb	0,068	0,032	0,027	0,031	0,03950
64Kb	0,067	0,026	0,033	0,032	0,03950
128Kb	0,074	0,049	0,027	0,031	0,04525
256Kb	0,057	0,033	0,027	0,029	0,03650
512Kb	0,070	0,032	0,034	0,029	0,04125
1024Kb	0,064	0,029	0,034	0,330	0,11425



Gambar 5. Waktu proses eksekusi enkripsi dan deksripsi

Pada Gambar 5 menunjukkan hasil pengujian waktu proses eksekusi dan deksripsi. Pada gambar dapat dilihat bahwa proses enkripsi membutuhkan waktu yang lebih lama daripada proses dekripsi.Mengacu pada Tabel 1 dan Tabel 2 diperoleh rata-rata rasio antara proses dekripsi dengan enkrispsi yaitu 33%, dimana waktu eksekusi proses deksripsi 33% lebih cepat daripada proses enkripsi.

4. KESIMPULAN

Berdasar hasil implementasi algoritma Blowfish menggunakan MS Visual data berhasil dienkripsi maupun didekripsi dan dapat kembali seperti semula. Hasil pengujian waktu eksekusi menggunakan beberapa file dengan ukuran berbeda mulai dari 64Kb, 128Kb, 256Kb, 512Kb, dan 1024Kb, secara umum menunjukkan proses enkripsi membutuhkan waktu yang lebih lama daripada proses dekripsi. Data yang diperoleh menunjukkan proses deksripsi 33% lebih cepat daripada proses enkripsi. Implementasi algoritma *Blowfish* menggunakan MS Visual Basic dapat digunakan untuk melakukan pengamanan data.

DAFTAR PUSTAKA

[1] Adeyinka, O., 2008, Internet Attack Methods and Internet Security Technology, Second Asia International Conference on Modelling and Simulation, pp.77-82, 13-15 May 2008.

[2] Kautzar, M.G., 2007, Studi Kriptografi Mengenai Triple DES dan AES, ITB, Bandung.

[3] Schneier, B., 1996, Applied Cryptography 2nd Edition, Wiley & Sons. Inc., New York.

[4] Savitri, Dian Intania. 2006. *Analisis Keamanan Algoritma Kriptografi DES, Double DES, dan Triple DES*. Bandung: ITB.

[5] J. Massey. An introduction to contemporary cryptology. *IEEE proceedings*, 76(5), 533--549, 1988.

[6] Data Encryption Standard, Federal Information Processing Standard (FIPS) Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington, DC (January 1977).

[7] Text Book: Cryptography and network security, Principles and practices by William Stalling, Retrieved on 8 December 2006.

[8] Bruce Schneier, "The Blowfish encryption algorithm9", Dr. Dobb's Journal of Software Tools, 19(4), p. 38, 40, 98, 99, April 1994.

[9] Heys, H.M.; Tavares, E. On the Security of the CAST Encryption Algorithm, Electrical & Computer Engg.

[10] X. Lai and J. Massey. A proposal for a new block encryption standard. In Proceedings of the EUROCRYPT 90 Conference, pp. 3 89-404, 1990.

[11] Wheeler, D.J., & Needham, R.J. (1994). TEA, a tiny encryption algorithm. In Fast Software Encryption – Proceedings of the 2nd International Workshop,1008.

[12] J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES algorithm submission, September 3, 1999.

[13] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, and Edward Roback, Report on the Development of the Advanced Encryption Standard (AES), Volume 106 Number 3 May– June 2001.

[14] Schneier, Bruce, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson;. 1998 "Twofish : A 128-bit block chiper".

[15] Suriski Sitinjak, Yuli Fauziah, and Juwairiah, "Aplikasi Kriptografi File Menggunakan Algoritma Blowfish," in Seminar Nasional Informatika 2010 (semnasIF 2010), Yogyakarta, 2010, pp. C-85.

[16] Muslim, M. A., & Prasetiyo, B. (2016). Implementation Twofish Algorithm fo Data Security in a Communication Network using Library Chilkat Encryption Activex. Journal of Theoretical and Applied Information Technology, 84(3), 370.

[17] Alamsyah, Muslim, M. A., & Prasetiyo, B. (2015). Data Hiding Security using Bit Matching-Based Steganography and Cryptography Without Change The Stego Image Quality. Journal of Theoretical and Applied Information Technology, 82(1), 106.

[18] Menezes A.J., Oorschot, P.C., dan Vanstone, S.A., 1996, Handbook of Applied Cryptography, CRC Press, Boca Raton, New York.

[19] Munir, R., 2006, Pengantar Kriptografi, ITB, Bandung.

[20] Bruce Schneier, "Applied Cryptography", John Wiley & Sons, Inc. 1996.

[21] Firdaus, Microsof Visual Basic 6.0 Untuk orang awam, Maxikom Palembang, April 2006.

[22] Pressman, R.S., 2001, Software Engineering: A Practitioner's Approach, 6th Edition, The McGraw-Hill Companies, Inc, Singapore.

[23] Arief, A., & Saputra, R. (2016). Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging. *Scientific Journal of Informatics*, *3*(1), 46-54.

[24] Prasetiyo, B., Gernowo, R., & Noranita, B. (2015). Kombinasi Steganografi Berbasis Bit Matching dan Kriptografi DES untuk Pengamanan Data. *Scientific Journal of Informatics*, *1*(1), 79-93.

25. Penerapan Kriptografi Algoritma Blowfish pada Pengamanan Pesan Data Teks

ORIGINALITY REPORT

11%	%	11%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Leili Nosrati, Amir Massoud Bidgoli. "A review of mobile banking security", 2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), 2016 Publication	4%
2	Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer Abdulsattar Lafta, Mohammed Mahdi Hashim, Hassanain Mahdi Alzuabidi. "Combination of Steganography and Cryptography: A short Survey", IOP Conference Series: Materials Science and Engineering, 2019 Publication	1%
3	Swati Maurya, Anita Singhrova. "Chapter 4 ‘Changing Trend in Network Security Measures: A Review’", Springer Nature, 2018 Publication	1%
4	Wei Zhong. "Performance Study of Cryptographic Storage Area Network", 2007 IFIP International Conference on Network and	1%

Parallel Computing Workshops (NPC 2007), 09/2007
Publication

5	Yi Shang, , Wenjun Zeng, Dominic K. Ho, Dan Wang, Qia Wang, Yue Wang, Tiancheng Zhuang, Aleksandre Lobzhanidze, and Liyang Rui. "Nest: Networked smartphones for target localization", 2012 IEEE Consumer Communications and Networking Conference (CCNC), 2012. Publication	1%
6	P. Israsena. "Hardware Implementation of a TEA-Based Lightweight Encryption for RFID Security", RFID Security, 2009 Publication	1%
7	A. Delis. "An Inline Detection and Prevention Framework for Distributed Denial of Service Attacks", The Computer Journal, 10/16/2006 Publication	1%
8	Ana Grbovic, Ivana Ognjanovic, Ivan Vuckovic. "Security of AMR system in HPP Perucica", 2018 23rd International Scientific-Professional Conference on Information Technology (IT), 2018 Publication	1%
9	Reni Haerani, Zaenal Muttaqin. "Rancangan Implementasi Protokol S/Mime Pada Layanan	1%

E-mail Sebagai Upaya Peningkatan Jaminan Keamanan Dalam Transaksi Informasi Secara Online (Studi Kasus : PT. XYZ)", JSiI (Jurnal Sistem Informasi), 2018
Publication

---

10 G. S. Sureshchandar, Rainer Leisten. "Software metrics for enhanced business excellence: An investigation of research issues from a macro perspective", Total Quality Management & Business Excellence, 2006 <1%
Publication

---

11 V K Nisha, Liyamol Aliyar, Asha Ali. "An overview of cryptographic solutions to web security", 2010 IEEE International Conference on Computational Intelligence and Computing Research, 2010 <1%
Publication

---

12 A B Nasution, S Efendi, S Suwilo. "Image Steganography In Securing Sound File Using Arithmetic Coding Algorithm, Triple Data Encryption Standard (3DES) and Modified Least Significant Bit (MLSB)", Journal of Physics: Conference Series, 2018 <1%
Publication

---

13 "Encyclopedia of Cryptography and Security", Springer Nature, 2005 <1%
Publication

---

14 Pahrul Irfan. "Aplikasi Enkripsi Citra Menggunakan Algoritma Kriptografi Arnold Cat Map Dan Logistic Map", Jurnal Matrik, 2017

Publication

<1%

Exclude quotes	On	Exclude matches	< 10 words
Exclude bibliography	Off		