JPTIS : JURNAL PENELITIAN TEKNOLOGI INFORMASI DAN SAINS
Vol.1, No.1 Maret 2023
e-ISSN: 2985-7635; p-ISSN: 2985-6280, Hal 09-21

Analisis Dan Implementasi Algoritma Rivest Code-5 Pada Keamanan Data

Sastya Hendri Wibowo
Universitas Muhammadiyah Bengkulu

Diana
Universitas Muhammadiyah Bengkulu
eshawewibowo@gmail.com

Korespondensi penulis: eshawewibowo@gmail.com

Abstract. *The RC-5 algorithm is an algorithm with the encryption method using the symmetric method and processing in the form of a cipher block, the same keywords are used for the encryption and decryption processes. The testing and analysis phase consists of a). Testing the execution time of the key generation process (set up key) b). Testing the success of the encryption and decryption process on the client-server integration method c). Testing the success of the encryption and decryption process using the file operation method d). Comparison of overhead/file size before and after passing through the system. The testing phase and execution time analysis are carried out when using the file operation method where the test will be divided into 3 parts, namely the execution time for the key setup process, the encryption process, and the decryption process. Testing the success of the encryption and decryption process on the client-server integration method is divided into 2 parts, namely testing the encryption process and the decryption process. In testing the encryption process, the characters that will be sent to the server will be encrypted first with a key to becoming a ciphertext in the form of integer data. The test results obtained are 1). The execution time for key generation (set up key) is very fast, around 9-10 ns. 2). In the encryption and decryption process, the execution time depends on the size of the plaintext file. The larger the plaintext file size, the longer the execution time. Where for a file with a size of 1 kb requires an execution time of 50.6 ms in the encryption process. 3). There is no difference between the size of the file before entering encryption and after decryption. Where for files with a size of 500 bytes before entering the encryption process, a file of 500 bytes will be generated from the decryption process.*

Keywords: *cryptography, encryption, decryption, rc-5 algorithm*.

Abstrak. Algoritma RC-5 merupakan algoritma dengan metode enkripsi menggunakan metode simetrik dan pengolahan dalam bentuk blok chiper, kata kunci yang sama digunakan untuk proses enkripsi dan dekripsi. Tahap pengujian dan analisa terdiri a). Pengujian waktu eksekusi proses pembangkitan kunci (*set up key*) b). Pengujian keberhasilan proses enkripsi dan dekripsi pada metode integrasi *client server* c). Pengujian keberhasilan proses enkripsi dan dekripsi menggunakan metode operasi file d). Perbandingan overhead / ukuran file sebelum dan sesudah melewati sistem. Tahap pengujian dan analisa waktu eksekusi dilakukan pada saat menggunakan metode operasi file dimana pengujiannya akan dibagi menjadi 3 bagian yaitu waktu eksekusi untuk proses

Received November 30, 2022; Revised Desember 02, 2022; Januari 01, 2023
* Sastya Hendri Wibowo, eshawewibowo@gmail.com

set up key, proses enkripsi, dan proses dekripsi. Pengujian keberhasilan proses enkripsi dan dekripsi pada metode integrasi *client server* dibagi menjadi 2 bagian yaitu pengujian pada proses enkripsi dan proses dekripsi. Pada pengujian proses enkripsi, karakter yang akan dikirimkan ke *server*, akan di enkripsi terlebih dahulu dengan sebuah kunci menjadi suatu ciphertext yang berupa data interger. Hasil pengujian didapat adalah 1). Waktu eksekusi untuk pembangkitan kunci (set up key) sangat cepat sekali yaitu sekitar 9-10 ns. 2). Pada proses enkripsi dan dekripsi, waktu eksekusi tergantung dari besar atau kecilnya ukuran file plaintext. Semakin besar ukuran file plaintext maka semakin lama waktu eksekusinya. Dimana untuk file dengan ukuran sebesar 1 kb membutuhkan waktu eksekusi sebesar 50,6 ms pada proses enkripsi. 3). Tidak terdapat perbedaan antara besar file sebelum masuk enkripsi dengan sesudah dekripsi. Dimana untuk file dengan ukuran sebesar 500 bytes sebelum masuk proses enkripsi, akan dihasilkan file sebesar 500 bytes dari proses dekripsi.

Kata kunci: kriptografi, enkripsi, dekripsi, algoritma rc-5.

LATAR BELAKANG

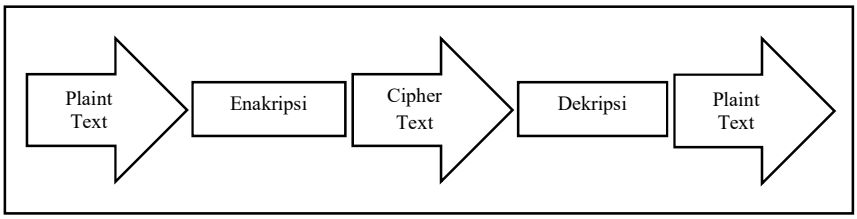
Di era konektivitas elektronik universal, gangguan berupa peretas, virus, penipuan elektronik, dan penyadapan elektronik sering terjadi. Itulah mengapa keamanan informasi sangat penting sehingga diperlukan sistem jaringan komputer yang memiliki tingkat keamanan yang dapat dijamin dan dapat mencegah serangan, meskipun pada akhirnya ada kompromi antara tingkat keamanan dan kemudahan menggunakan akses. Enkripsi dengan metode enkripsi diperlukan untuk melindungi data pesan secara online. Enkripsi adalah salah satu cara yang digunakan untuk melindungi sistem atau data terhadap hal-hal yang mengakibatkan tidak terpenuhinya aspek-aspek di atas, seperti menjaga keamanan dan keutuhan data atau informasi [1].

Kriptografi merupakan salah satu teknik yang dapat digunakan melindungi informasi rahasia atau pribadi. Proses konversi data dua arah yang terdiri dari *enkripsi* dan pemrosesan *dekripsi* adalah tingkat enkripsi [2]. Ada beberapa algoritma enkripsi yang sudah terbuka untuk dipelajari dan digunakan untuk proses keamanan data pada jaringan komputer, seperti Data Encryption Standard (DES), RC-4, TwoFish, RC-5, CAST, IDE, RSA dan lain-lain. Salah satu metode enkripsi data yang akan dibahas adalah kriptografi simetris RC-5 (*Rivest Code* 5) [3]. Algoritma RC-5 dikemukakan oleh Ronald L.Rivest dari MIT Laboratory for Computer Science, sehingga keamanan dan kerahasiaan data dapat terjaga saat melakukan komunikasi dan pertukaran informasi/data tidak dapat disadap pihak yang tidak berkepentingan. Metode RC5 adalah salah satu algoritma

enkripsi paling dasar tunduk pada peringkat RC5. Algoritma RC5 Menggunakan metode simetris dan pemrosesan dalam bentuk blok kriptografi. Jumlah Satu putaran algoritma RC5 dilambangkan dengan r yang nilainya antara 1, 2, 3, 4, ..., 225 jumlah kata dalam bit dilambangkan dengan w. Nomor yang didukung adalah 16-bit, 32-bit dan 64-bit, kata kunci (*keyword*) dilambangkan dengan b dalam rentang 1, 2, 3, 4, ..., 225. Ada 3 proses utama di RC5, yaitu perluasan kunci, enkripsi dan dekripsi. Perluasan kunci adalah proses generatif penguncian internal menggunakan pergeseran kiri reguler (<<<) dan operasi putaran shift reguler kanan (>>>), panjang kunci tergantung pada jumlah putaran [4].

KAJIAN TEORITIS

Kriptografi (cryptographi) berasal dari BahasaYunani: “cryptos” artinya “secret” (rahasia), sedangkan “graphein” artinya “writing” (tulisan). Sehingga kriptografi berarti “secret writing” (tulisan rahasia). Jadi kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kebentuk yang tidak dapat dimengerti lagi maknanya. Secara umum kriptografi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (plainteks) dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan informasi baru (chipertext) yang tidak dapat dibaca secara langsung. Chipertext tersebut dapat dikembalikan menjadi informasi awal (plainteks) melalui proses deskripsi. Urutan proses kriptografi secara umum dapat dilihat pada gambar dibawah ini :



Gambar 1. Proses Enkripsi dan Deskripsi

Terdapat dua jenis algoritma kriptografi berdasar jenis kuncinya [5] :

1. Algoritma Simetri (konvensional), Algoritma simetri disebut juga sebagai algoritma konvensional adalah algoritma yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Yang termasuk algoritma kunci simetri adalah OTP, DES, RC2,

RC4, RC5, RC6, IDEA, Twofish, Magenta, FEAL, SAFER, LOKI, CAST, Rijndael (AES), Blowfish, GOST, A5, Kasumi dan lain-lain

2. Algoritma Asimetri (kunci public), Algoritma asimetrik (juga disebut algoritma kunci public) didesain sedemikian sehingga kunci yang digunakan untuk enkripsi berbeda dari kunci yang digunakan untuk dekripsi.Enkripsi dengan kunci public Ke dinyatakan sebagai berikut :

   EKe (M) = C

   DKd (C) = M

Algoritma Rivest Code-5 merupakan metode enkripsi menggunakan metode simetrik dan pengolahan dalam bentuk blok chiper, jadi kata kunci yang sama digunakan untuk proses enkripsi dan dekripsi. Parameter-parameter yang digunakan dalam Rivest Code-5 adalah sebagai berikut [5] :

Kata kunci (key word) Variabel ini disimbolkan dengan b dengan range 0, 1, 2, ….255. Key word ini dikembangkan menjadi array S yang digunakan sebagai key pada proses untuk enkripsi dan dekripsi.

Untuk memahami cara kerja RC-5, dapat dimulai dengan melihat konsep dasar bagaimana RC-5 ini bekerja. Hal ini dilakukan untuk memahami cara kerja algoritma ini lebih lanjut. RC-5 Menggunakan operasi dasar untuk proses enkripsi sebagai berikut :

1. Data yang akan dienkripsi dikembangkan menjadi 2 bagian bagian kiri dan bagian kanan dan dilakukan penjumlahan dengan key word yang yang telah diekspansi sebelumnya. Penjumlahan ditunjukan dengan tanda ``+``, dan disimpan di dua register A dan register B.
2. Kemudian dilakukan operasi EX-OR, yang ditandai dengan tanda ``⊕``.
3. Melakukan rotasi kekiri (shift left) sepanjang y terhadap x word yang ditandai dengan x<<< y. y merupakan interpretasi modulo w atau jumlah kata w dibagi 2. Dengan lg[w] ditentukan jumlah putaran yang dilakukan.
4. Tahap akhir dilakukan penggabungan untuk mendapatkan data yang telah dienkripsi.

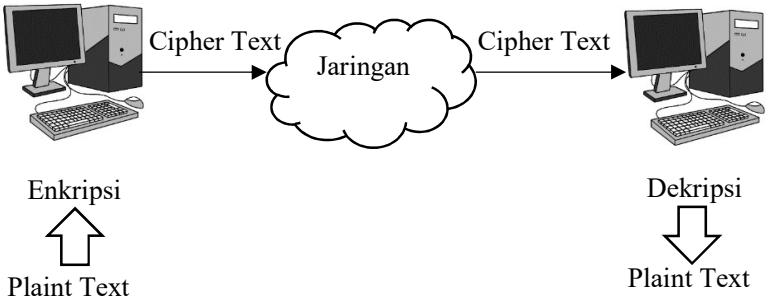
Proses dekripsi dilakukan dengan konsep dasar sebagai berikut :

e-ISSN: 2985-7635; p-ISSN: 2985-6280, Hal 09-21

1. Data yang telah dienkripsi dikembangkan kembali menjadi 2 bagian dan disimpan di dua register A dan register B.
2. Kemudian dilakukan rotasi ke kanan sejumlah r. satuan
3. Selanjutnya dilakukan operasi EX-OR yang ditandai dengan ``⊕``.
4. Tahap akhir dilakukan pengurangan terhadap masing-masing register dengan key word yang ditunjukan dengan tanda ``-``, untuk mendapatkan plaintext.

METODE PENELITIAN

Dalam sistem ini dibuat interaksi antara 2 buah PC (*Personal Computer*). Untuk PC pertama (*client*) akan menyiapkan data atau *plaintext* yang akan diberikan ke PC kedua (*server*) dan data tersebut dienkripsi terlebih dahulu menggunakan metode RC-5 menjadi sebuah data *chipertext* sebelum dikirim ke jaringan internet. Setelah itu data *ciphertext* akan didekripsi disisi s*erver* (PC2) sehingga data yang diterima oleh *server* akan kembali lagi seperti data awal atau kembali ke *plaintext* lagi.



Gambar 2. Sistem Algoritma Rivest Code-5

HASIL DAN PEMBAHASAN

1.1 Pengujian dan Analisa

Pada tahap pengujian ini, penulis akan menguji sistem *enkripsi* dan *dekripsi* menggunakan algortitma Rivest Code-5 dengan membagi menjadi 4 tahap pengujian yaitu :

a. Pengujian dan analisa waktu eksekusi

   Proses pembangkitan kunci (*set up key*)

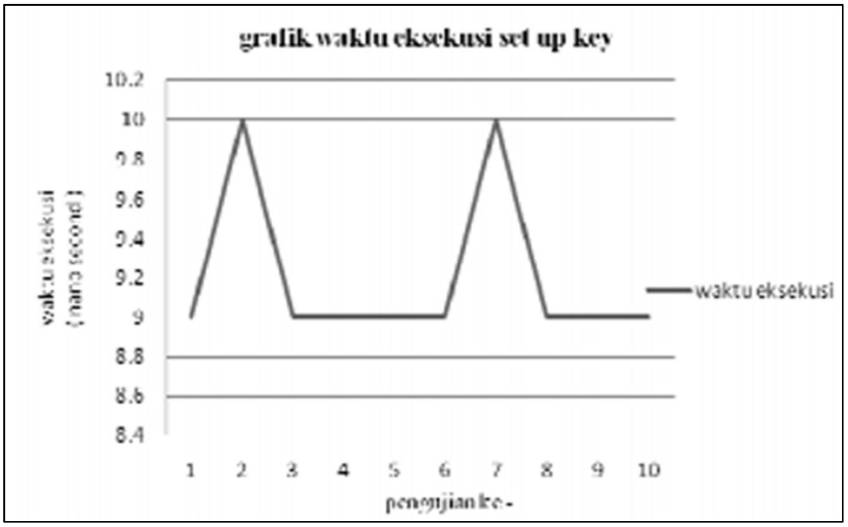
   Proses enkripsi

   Proses dekripsi

b. Pengujian keberhasilan proses enkripsi dan dekripsi pada metode integrasi *client server*
c. Pengujian keberhasilan proses enkripsi dan dekripsi menggunakan metode operasi file
d. Perbandingan overhead atau ukuran file sebelum dan sesudah melewati sistem

1.2 Pengujian Dan Analisa Waktu Eksekusi

Pengujian tahap ini dilakukan pada saat menggunakan metode operasi file dimana pengujiannya akan dibagi menjadi 3 bagian yaitu waktu eksekusi untuk proses set up key, proses enkripsi, dan proses dekripsi.



Gambar 3. Grafik Hasil Waktu Eksekusi Set Up Key

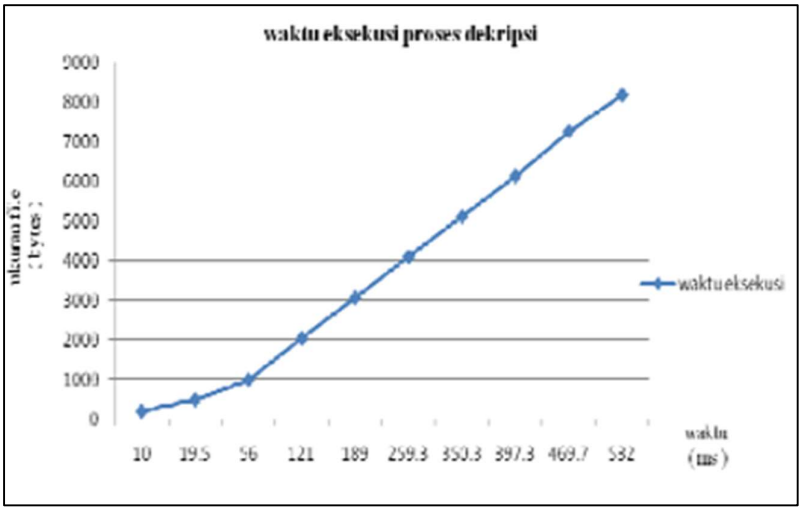
Pada gambar grafik diatas , dapat dikatakan untuk pembangkitan kunci (*set up key*) embutuhkan waktu antara 9 – 10 nano second, sedangkan waktu eksekusi pada proses

enkripsi dilakukan 10 kali pengujian dengan mneggunakan file.txt yang memiliki ukuran file yang berbeda beda. Sehingga hasil percobaannya dapat dilihat pada tabel dibawah ini :

Tabel 1. Waktu Eksekusi Pada Proses Enkripsi

No	Nama file (.txt)	ukuran file (bytes)	Waktu Eksekusi Proses Enkripsi dalam milisecond										
		plaintext	1	2	3	4	5	6	7	8	9	10	average
1	data1	200	10	15	15	10	10	15	10	10	10	10	11.5
2	data2	500	20	15	20	20	20	20	15	20	20	20	19
3	data3	1000	46	50	50	50	60	50	50	50	50	50	50.6
4	data4	2049	140	110	120	110	120	130	110	130	110	130	121
5	data5	3076	171	180	190	190	180	198	175	187	180	171	182.2
6	data6	4104	234	250	250	240	270	230	250	270	256	245	249.5
7	data7	5121	296	343	343	335	302	330	331	320	312	320	323.2
8	data8	6144	353	358	375	365	379	382	383	370	378	388	373.1
9	data9	7275	420	440	456	455	482	477	457	423	455	470	453.5
10	data10	8189	479	510	483	540	468	508	512	475	458	480	491.3

Pada pengujian waktu eksekusi pada proses dekripsi, cara pengujiannya juga hampir sama dengan proses enkripsi, sehingga dari data tabel bisa digambarkan grafiknya sebagai berikut ini :



Gambar 4. Grafik Waktu Eksekusi Proses Dekripsi

1.3 Pengujian Keberhasilan Proses Enkripsi dan Dekripsi Pada Metode Integrasi *Client Server*

Pada pengujian keberhasilan proses enkripsi dan dekripsi pada integrasi *client server*, pengujian akan bagi menjadi 2 bagian yaitu pengujian pada proses enkripsi dan proses dekripsi. Pada pengujian proses enkripsi, karakter yang akan dikirimkan ke *server*, akan di enkripsi terlebih dahulu dengan sebuah kunci menjadi suatu ciphertext yang berupa data interger. Ketika akan dikirin ke *server* melalui jaringan internet menggunakan socket, data integer akan diubah terlebih dahulu menjadi data bertipe string. Contoh hasil pengujian proses enkripsi dan dekripsi pada *client server* adalah sebagai berikut :

```
Proses di PC Client
plaintextnya adalah   ^ *

proses enkripsi dengan algoritma RC5
ciphertext (int) adalah  -1094006915 dan 1055364136

data diubah dari int menjadi string
ciphertext (string) adalah : }'  , (
```

Gambar 5. Proses Enkripsi Disisi *Client*

```
Proses di PC Server
ciphertext (string) yang diterima dari client melalui socket
ciphertext (string) diubah ke (int) -1094006915 , 1055364136

Proses Dekripsi dengan algoritma RC5
plaintextnya  adalah  ^ *
```

Gambar 6. Proses dekripsi disisi *server*

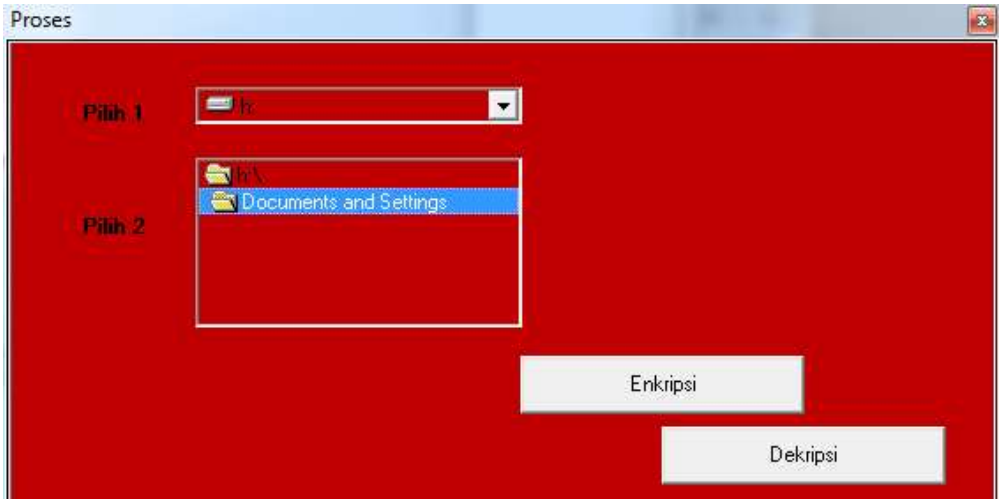
1.4 Pengujian Keberhasilan Proses Enkripsi Dan Dekripsi Pada Metode Operasi File

Pada pengujian keberhasilan proses enkripsi dan dekripsi Rivest Code-5 dengan metode operasi file, pengujiannya dilakukan dengan cara melakukan enkripsi file.txt yang berisi dari beberapa karakter dan akan menghasilkan file ciphertext.txt yang berisi beberapa karakter yang susah untuk dibaca. Sedangkan di poses dekripsi, file ciphertext.txt tadi didekripsi sehingga dapat menghasilkan file.txt kembali. Berikut contoh gambar proses enkripsi dengan metode operasi file dapat dilihat pada gambar dibawah :

A. Proses Enkripsi

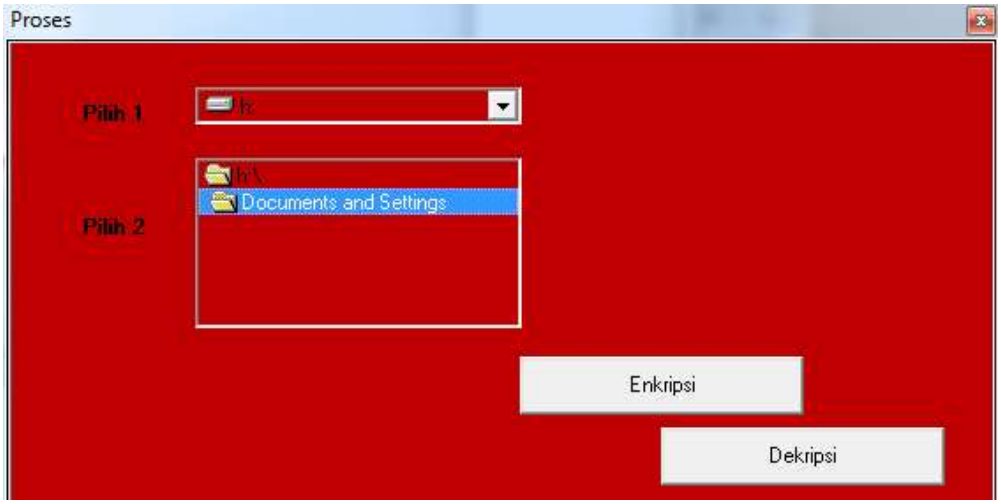
Pada Form Enkripsi dan Dekripsi, terdapat tampilan Pilih Folder Data, Pilih Data Teks, Hasil dan Pilih Proses.

e-ISSN: 2985-7635; p-ISSN: 2985-6280, Hal 09-21



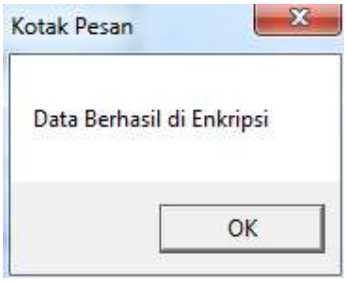
Gambar 7. Form Enkripsi

Untuk menjelaskan bagaimana langkah dari proses ini, penulis akan memberikan contoh untuk enkripsi Data.



Gambar 8. Proses Enkripsi Data

Setelah Data ditemukan, maka tombol Enkipsi ditekan akan memberikan pemberitahuan nama kunci dari data tersebut seperti pada Gambar 9.



Gambar 9. Pesan Proses Enkripsi

Dari gambar di atas yang sudah di enkripsi yaitu gambar 8 dan gambar 9 hasil kodenya adalah:

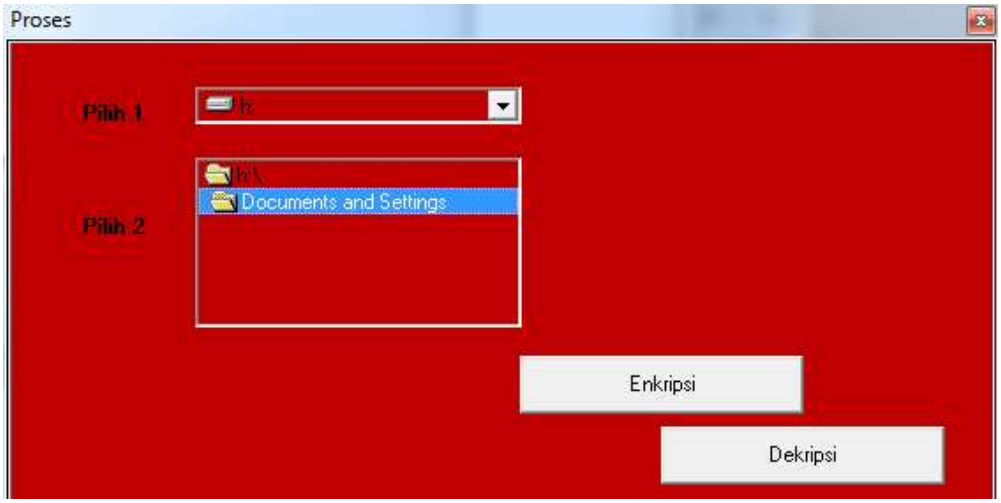
```
Private Sub Command1_Click()
On Error GoTo Err
   Dim Path As String
   Dim Data As String
   Dim File As String
   Dim md5 As String
   Dim FileName As String
   md5 = ".{645FF040-5081-101B-9F08-00AA002F954E}"
   Path = dirDir.Path
   Data = Mid$(Path, InStrRev(Path, "\") + 1, Len(Path))
   File = Left$(Path, Len(Path) - Len(Data))
   If Not UCase$(Path) = UCase$(WindowsDirectory) _
   And Not UCase$(Data) = UCase("desktop") Then

      FileName = File & Data & md5
      Name dirDir.Path As FileName
      dirDir.Path = File
      MsgBox "Folder Sudah di Enkripsi", vbApplicationModal +
vbInformation, "Enkripsi"
   Else
      MsgBox "Folder Cannot be Locked.", vbApplicationModal +
vbCritical, "Pesan"
   End If
Err:
   Exit Sub
End Sub
```

B. Proses Dekripsi

e-ISSN: 2985-7635; p-ISSN: 2985-6280, Hal 09-21

Pada proses Dekripsi hampir Tampilan menu Dekripsi sama dengan proses Enkripsi, pertama menentukan dimana letak file yang yang telah di Enkripsi dan selanjutnya menekan tombol Dekripsi. Ditunjukkan pada Gambar 10.



Gambar 10. Proses Dekripsi Data

Selanjutnya akan tampil pesan bahwa Data Sudah di Dekripsi.

Gambar 11. Pesan Proses Dekripsi

Dari gambar yang sudah di deskripsi yaitu pada gambar 10 dan gambar 11 adapun hasil dari codingnya yaitu:

```
Private Sub Command2_Click()
On Error GoTo Err
   Dim Path As String
   Dim Temp As String
   Dim Data As String
   Dim File As String
   Dim md5 As String
```

```
    Dim FileNameAs String
    Path = dirDir.Path
    Temp = Mid$(Path, InStrRev(Path, "\") + 1, Len(Path))
    Data = Left$(Temp, InStr(Temp, ".{") - 1)
    File = Left$(Path, Len(Path) - Len(Temp))
FileName = File & Data
    Name dirDir.Path As FileName
dirDir.Path = File
MsgBox "Kunci Folder Tealah di Deskripsi.", vbApplicationModal + vbInformation, "Pesan"
Err:
    Exit Sub
End Sub


Private Sub Command3_Click()
Me.Hide
End Sub
```

KESIMPULAN DAN SARAN

1. Waktu eksekusi untuk pembangkitan kunci (set up key) sangat cepat sekali yaitu sekitar 9-10 ns.
2. Pada proses enkripsi dan dekripsi, waktu eksekusi tergantung dari besar atau kecilnya ukuran file plaintext. Semakin besar ukuran file plaintext maka semakin lama waktu eksekusinya. Dimana untuk file dengan ukuran sebesar 1 kb membutuhkan waktu eksekusi sebesar 50,6 ms pada proses enkripsi.
3. Tidak terdapat perbedaan antara besar file sebelum masuk enkripsi dengan sesudah dekripsi. Dimana untuk file dengan ukuran sebesar 500 bytes sebelum masuk proses enkripsi, akan dihasilkan file sebesar 500 bytes dari proses dekripsi.
4. Algoritma Rivest Code-5 merupakan algoritma lama, untuk pengembangan perlu mencoba algoritma yang terbaru yang sesuai dengan perkembangan perangkat lunak saat ini

DAFTAR REFERENSI

Andrizal, "Algoritma Enkripsi Rivest Code 5 (Rc-5), "Dept. Teknik Elektro Option Teknik Komputer Itb, 2008.

Aprizaldi. "Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma AES 128 Untuk Enkripsi dan Dekripsi Data". Jurnal Teknik Informatika. 2022.

Bruce Schneier, Applied Cryptography : Protocols, Algorithms, and Source Code in C, 2nd Edition.

Budi Rahardjo," Keamanan Sistem informasi Berbasis Internet", PT Insan Komunikasi Indonesia, Bandung, 2002.

E. [5]Setyaningsih, Kriptografi & Implementasinya Menggunakan Matlab, Yogyakarta:Andi, 2015.

Hamdani, Suryawan, S.H., dan Septiarini, A. 2013. "Pengujian Algoritma Rivest Code 5 Untuk Enkripsi Struktur File Dokumen". Prosiding STI 2013 Seminar Nasional Teknik Informatika, Prospek dan Tantangan Mobile Application. Juni 2013,Universitas Ahmad Dahlan.

Harni Kusniyati. "Penerapan Algoritma Rivert Code 4 Pada Aplikasi Kriptografi Dokumen". Jurnal Petir. 2018

Kaliski, B.S Jr and Yin, Y.L. 1998. On the Security of the RC5 Encryption Algorithm RSA Laboratories Technical Report TR-602. RSA Laboratories, a division of RSA Data Security, Inc.

Rehman, S.U. 2012. "Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)". International Journal of Computer Science Issues. Vol 9. No. 2. Issue 1 January 2012. page 96 - 101.

S.H. Suryawan, Hamdani, "Pengamanan Data File Dengan Menggunakan Algoritma Enkripsi Rivest Code 5 ," Jurnal Informatika Mulawarman , vol.8, no. 2, pp. 44-49, 2013.

T. Zebua and E. Ndruru, "PENGAMANAN CITRA DIGITAL BERDASARKAN MODIFIKASI ALGORITMA RC4," J. Teknol. Infomasi dan Ilmu Komput., vol. 4, no. 4, pp. 275–282, 2017.

Widodo Arif Prabowo. "Penyandian File Word Berdasarkan Algoritma Rivest Code 5". Jurnal Sains Komputer & Informatika. 2018.

H. Pandiangan, S. Sijabat "PERANCANGAN MEDIA PENGIRIMAN PESAN TEKS DENGAN PENYANDIAN PESAN MENGGUNAKAN ALGORITMA RC4 BERBASIS WEB ," Jurnal Matik Penusa , vol. Volume XIX, No. 1 , no. ISSN 2088-3943 , pp. 63-71, Juni 2016

ski