

PENGAMANAN FILE INVOICE PADA PT MITRA TEKNIK MENGUNAKAN METODE ALGORITMA RC4

Naufal Fakhri^{1*}, Hari Soetanto², Painem³, Windarto⁴

^{1,2,3,4} Teknik Informatika, Fakultas Teknologi Infirmasi, Universitas Budi Luhur, DKI Jakarta, Indonesia

Email: ^{1*}naufalfakhri11@gmail.com, ²hari.soetanto@budiluhur.ac.id, ³painem@budiluhur.ac.id,
⁴windarto@budiluhur.ac.id
(* : *corresponding author*)

Abstrak- Pada tahun 2008 berdirilah instansi yang bernama Mitra Teknik. Instansi ini bergerak di bidang Kitchen Set Restaurant dan per Hotelan. Dalam instansi ini mempunyai beberapa pelayanan, diantaranya melakukan *service (maintenance)*, membuat alat kitchen set sesuai permintaan customer. Mitra Teknik ini juga sudah banyak bekerja sama dengan Restoran maupun Hotel. Dan dari situlah banyak pesaing yang ingin menjatuhkan dengan cara apapun. Seperti mengambil data invoice perusahaan, dan mengubahnya dengan nama perusahaan lain. Tujuan penelitian ini adalah membuat aplikasi pengamanan file invoicedan file dokumen dengan format docx, pdf, xls, xlsx, txt, jpg pada PT. Mitra Teknik menggunakan algoritma RC4 dan model waterfall. Hasil dari penelitian diperoleh setelah proses enkripsi dengan algoritme RC4 rata-rata besar ukuran dokumen 13.634750 byte dan rata-rata waktu lama proses enkripsi 9.250 millisecond serta setelah proses dekripsi dengan algoritme RC4 rata-rata besar ukuran dokumen 13.634750 byte dan rata-rata waktu lama proses dekripsi 9.250 millisecond.

Kata Kunci: *File Invoice, Kitchen Set Restaurant, Algoritma RC4, PT Mitra Teknik*

SECURING INVOICE FILES AT PT MITRA TEKNIK USING THE RC4 ALGORITHM METHOD

Abstract- *In 2008 an agency called Mitra Teknik was established. This agency is engaged in Kitchen Set Restaurant and Hospitality. This agency has several services, including carrying out service (maintenance), making kitchen set tools according to customer requests. This Technical Partner has also worked closely with Restaurants and Hotels. And that's where a lot of competitors are looking to knock them out in any way. Like taking company invoice data, and changing it with another company name. The purpose of this study is to create an application for securing invoice files and document files in docx, pdf, xls, xlsx, txt, jpg formats at PT. Mitra Teknik uses the RC4 algorithm and the waterfall model. The results of the study were obtained after the encryption process with the RC4 algorithm the average document size was 13.634750 bytes and the average encryption process took 9250 milliseconds and after the decryption process with the RC4 algorithm the average document size was 13.634750 bytes and the average processing time 9250 millisecond decryption.*

Keywords: *File Invoice, Kitchen Set Restaurant, RC4 Algorithm, PT Mitra Teknik*

1. PENDAHULUAN

Pengembangan produk di dunia industri akan semakin diperlukan untuk menjadikan Indonesia sebagai negara maju. Produk adalah titik awal dan akhir kesuksesan di industri manufaktur. Oleh karena itu, keberhasilan persaingan industri ini akan ditentukan oleh keberhasilan pengembangan produk yang sesuai dengan kebutuhan dan harapan konsumen. Pada tahun 2008, sebuah agen bernama Mitra Teknik didirikan. Agensi ini berspesialisasi dalam permainan memasak untuk restoran dan hotel. Agensi ini memiliki serangkaian layanan, antara lain penyediaan layanan (pemeliharaan), produksi peralatan dapur atas permintaan klien. Mitra teknis ini juga telah bekerja sama dengan restoran dan hotel.

Dan di sinilah banyak pesaing ingin membagi diri dengan cara tertentu. Ambil informasi penagihan perusahaan dan ganti dengan nama perusahaan yang berbeda. Sayang sekali jika dokumen ini jatuh ke tangan yang salah dan disalahgunakan. Itu sebabnya saya membuat situs web ini untuk melindungi file dokumen Anda. Untuk menjaga keamanan data dan mencegah kehilangan data, hal ini dapat dilakukan dengan beberapa cara, salah satunya melalui enkripsi.

Menurut Menezes, kriptografi adalah ilmu yang mempelajari teknik matematika yang berkaitan dengan aspek keamanan informasi, seperti kerahasiaan, verifikasi entitas dan keaslian data, serta verifikasi integritas. Ada beberapa jenis algoritma dalam kriptografi, diantaranya RC4 [1]. Menurut operasinya, algoritma kriptografi RC4 adalah jenis enkripsi aliran. Keuntungannya adalah dengan metode ini, algoritma enkripsi RC4 dapat dilakukan pada data dengan panjang yang berbeda. Algoritma metode enkripsi aliran RC4 terdiri dari dua bagian, yaitu: definisi kunci dan pembangkitan aliran. Pada konfigurasi kunci, terdapat tiga langkah dalam prosesnya, yaitu memulai S-Box, menyimpan kunci dalam key byte array, dan menebus S-Box.

Stream generation menghasilkan nilai pseudo-random yang di XOR untuk menghasilkan *ciphertext* atau sebaliknya yaitu menghasilkan plaintext [2]. Kriptografi adalah studi tentang penulisan rahasia menggunakan teknik matematika. Dengan menjaga kerahasiaan data dengan kriptografi, maka data mentah (plaintext) yang dikirimkan diubah menjadi data terenkripsi, setelah itu data terenkripsi hanya dapat diubah kembali menjadi data sebenarnya dengan kunci [8]. Hal ini tentu saja dapat mengurangi penyalahgunaan data oleh pihak ketiga yang tidak berwenang. Kriptografi dibagi menjadi tiga, yaitu kriptografi simetris, kriptografi asimetris, dan kriptografi hybrid [9].

Di sisi lain, apa itu kriptografi asimetris menggunakan dua kunci berbeda yang digunakan, yaitu enkripsi dan dekripsi. Kunci bersifat publik dan kunci bersifat pribadi. Beberapa contoh algoritma yang menggunakan kriptografi asimetris adalah algoritma Rivest-Shamir-Adleman (RSA) dan DiffieHellman. Berikutnya adalah kriptografi hybrid, yaitu kriptografi yang menerapkan algoritma yang berbeda untuk memanfaatkan setiap algoritma.[10]. RC4 adalah algoritma enkripsi aliran yang dapat digunakan secara efisien dan efektif. Maka dari itu, RC4 sangat populer untuk aplikasi jaringan, termasuk RC4, yang digunakan dalam standar Wireless Equivalent Privacy (WEP) dan Transport Layer Security (TLS).

Algoritma kriptografi Rivest Code 4 dikembangkan oleh RSA Data Security Inc (RSADSI) dalam bentuk perlindungan torrent. Algoritma RC4 mengenkripsi bitwise dengan menggabungkan plaintext dengan Xor, yang panjang kuncinya berkisar antara 1 hingga 256 byte. Pintasan keyboard ini digunakan untuk menginisialisasi tabel 256-byte yang berfungsi sebagai generator angka pseudo-acak dan kemudian XOR dengan teks biasa dapat menghasilkan ciphertext [3].

Penelitian zahrul dan painem (2020) [3] dengan judul implementasi kriptografi algoritma RC4 dan 3DES dan steganografi dengan algoritma EOF untuk keamanan data berbasis desktop pada SMK as-su`udiyah. Penelitian wahyu et.al., (2020) [4] dengan judul aplikasi pengamanan file dengan metode kriptografi aes 192, rc4 dan metode kompresi huffman. Penelitian rohman et.al., (2018) [5] dengan judul implementasi kriptografi pada pengiriman pesan email dengan menggunakan metode RC4 dan Blowfish berbasis web pada PT.Dascom Jaya Sakti. Penelitian kirman (2018) [6] dengan judul implementasi algoritma RC4 untuk proteksi file mp3. Penelitian sumarno (2018) [7] dengan judul analisis kinerja kombinasi algoritma *message-digest* algoritim 5 (MD5), *Rivest Shamir Adleman* (RSA) dan *Rivest Cipher* 4 (RC4) pada keamanan e-Dokumen.

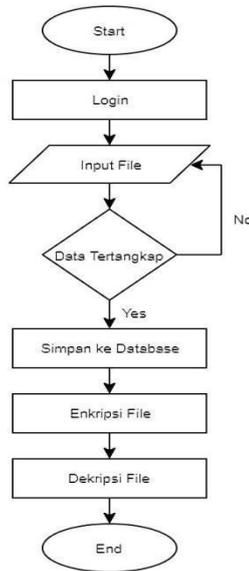
2. METODE PENELITIAN

2.1 Pengumpulan Data

Metode penelitian yang digunakan dalam penelitian ini adalah pengembangan dari metode Waterfall. Metode Waterfall (air terjun) adalah model pengembangan sistem informasi yang sistematis dan berurutan. Metode air terjun melibatkan langkah-langkah berikut:

- Komunikasi. Dalam membangun sistem Anda adalah menganalisis dan mengkomunikasikan persyaratan sistem berdasarkan hasil pengumpulan data. Pada tahap komunikasi disimpulkan bahwa diperlukan suatu sistem untuk melindungi dokumen penting di PT Mitra Teknik.
- Perencanaan. Perencanaan kesiapsiagaan menggambarkan pekerjaan yang akan dilakukan dari pengumpulan data hingga pengujian sistem, risiko yang timbul saat melakukan pekerjaan ini dan hasil yang dicapai, yaitu. pembuatan sistem pengamanan arsip dokumen penting yang mungkin ditemukan diperusahaan dengan menggunakan algoritma RC4 (Rivest Code 4).
- Permodelan. Tahap permodelan berfokus pada perancangan skema untuk sistem perlindungan file faktur dan kemudian database MySQL sebagai sistem penyimpanan data. Kemudian merancang sistem keamanan data. Diagram alir sistem ditunjukkan pada Gambar 1.
- Konstruksi. Kontruksi adalah langkah untuk menghasilkan kode untuk sistem yang dirancang sebelumnya yang akan d bangun. Bahasa pemrograman yang digunakan untuk membangun sistem adalah HTML, PHP dan menggunakan database MySQL sebagai penyimpan datanya.
- Distribusi. Tahap Distribusi merupakan tahap dimana sistem siap digunakan oleh pengguna. Agar sistem dapat terus berfungsi dengan baik, pekerjaan pemeliharaan rutin harus dilakukan sesuai kebutuhan [8].

Flowchart Sistem Pengamanan Data Digital



Gambar 1. Flowchart Sistem

2.2 Rancangan Penguji

Selama pembuatan situs web ini, pengujian dilakukan untuk menentukan apakah situs web berfungsi dengan benar dan tanpa kesalahan. Untuk melakukan pengujian, menggunakan metode pengujian *black box* yaitu metode pengujian perangkat lunak yang memverifikasi bahwa semua perangkat lunak berfungsi dengan benar sesuai dengan persyaratan fungsional yang ditentukan.

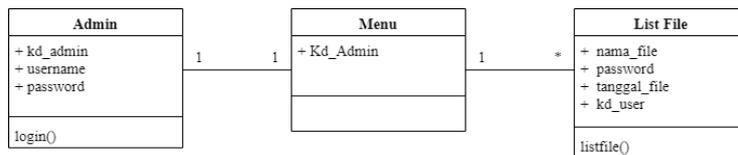
3. HASIL DAN PEMBAHASAN

Pada tahap ini berisikan hasil implementasi dari topik penelitian yang dibahas. Beserta penjelasan yang merupakan gambar, tabel, serta penjelasan.

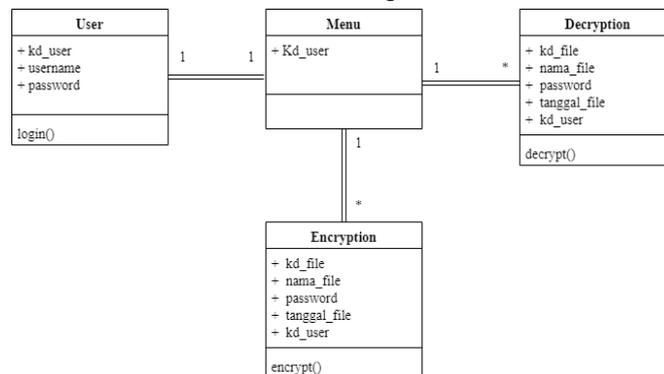
3.1 Rancangan Basis Data

a. Class Diagram

Pada gambar 3 merupakan gambar dari Class Diagram Admin. Pada gambar 3 Terdapat juga *class diagram user*.



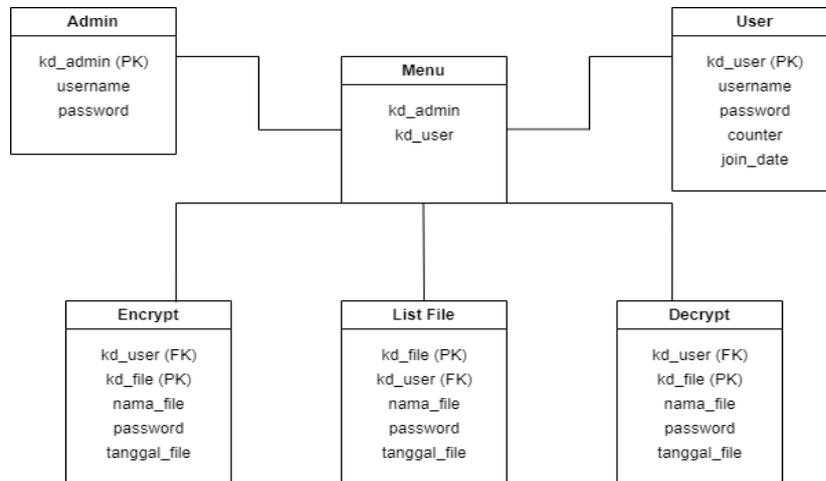
Gambar 2. Class Diagram Admin.



Gambar 3. Class Diagram User

b. *Logical Record Structur (LRS)*

Pada gambar 4 merupakan gambaran LRS program.



Gambar 4. LRS

Berdasarkan bab sebelumnya tentang penerapan skema RC4 (Rivest Code 4), berikut hasil implementasi Rivest Code 4 seperti pada Tabel berikut.

Tabel 1. Tabel Admin

Nama	Jenis Data	Keterangan
Kd_admin	Varchar (15)	Kode admin
Username	Varchar (50)	Username admin
Password	Varchar (50)	Password admin

Tabel 2. Tabel File

Nama	Jenis Data	Keterangan
Kd_file	Int (5)	Kode File
Nama_file	Text	Nama File
Password	Varchar (20)	Password File
Tanggal_file	Timestamp	Tanggal File
Kd_user	Int (5)	Kode User

Tabel 3. Tabel User

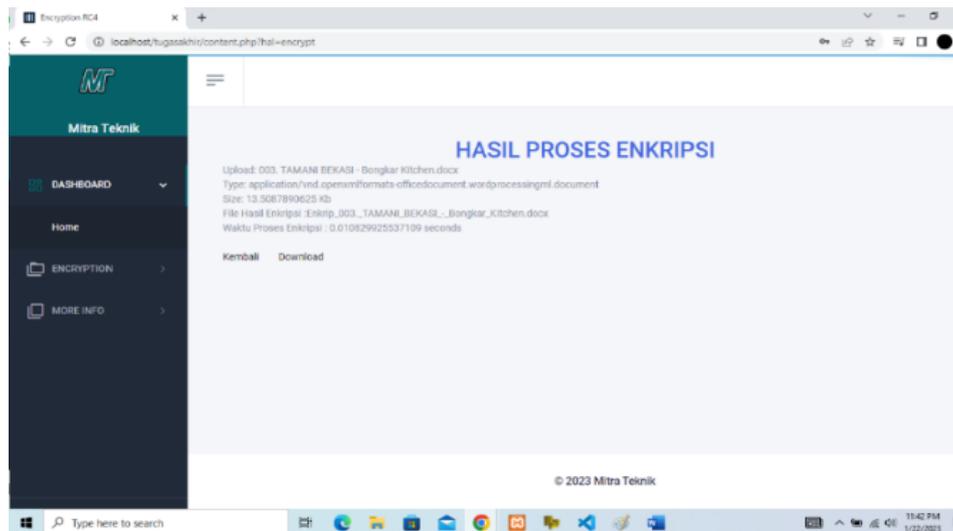
Nama	Jenis Data	Keterangan
Kd_user	Int (5)	Kode User
Username	Varchar (30)	Username
Password	Varchar (20)	Password
Counter	Char (5)	Penanda
Join_date	Timestamp	Tanggal Bergabung

3.2 Implementasi Rivest Code 4 (RC4)

Berdasarkan penerapan metode RC4, berikut ini adalah implementasi pada web yang dibuat.

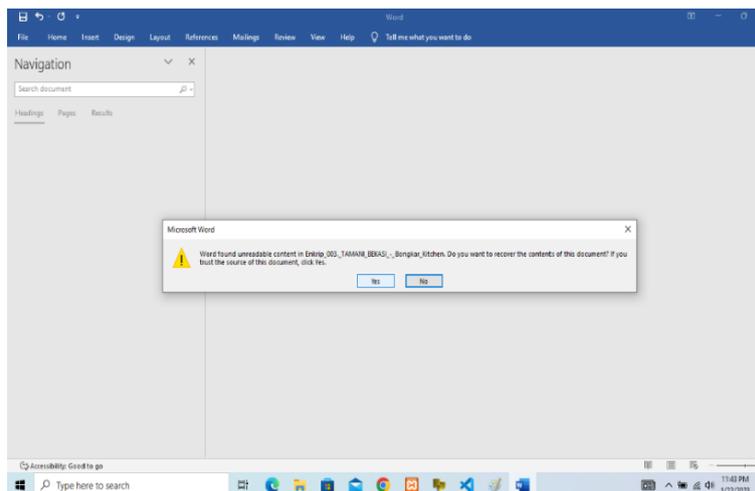
1. Implementasi Encrypt

Pada Gambar 5 adalah tampilan layar halaman *encrypt file.*, dan pada Gambar 5, terlihat bahwa aplikasi telah berhasil untuk mengamankan file yang berukuran 13.5087890625 KB atau setara dengan 135087890,625 MB, serta memiliki waktu untuk melakukan proses *encrypt file* tersebut adalah 0.010829925537109 Seconds.



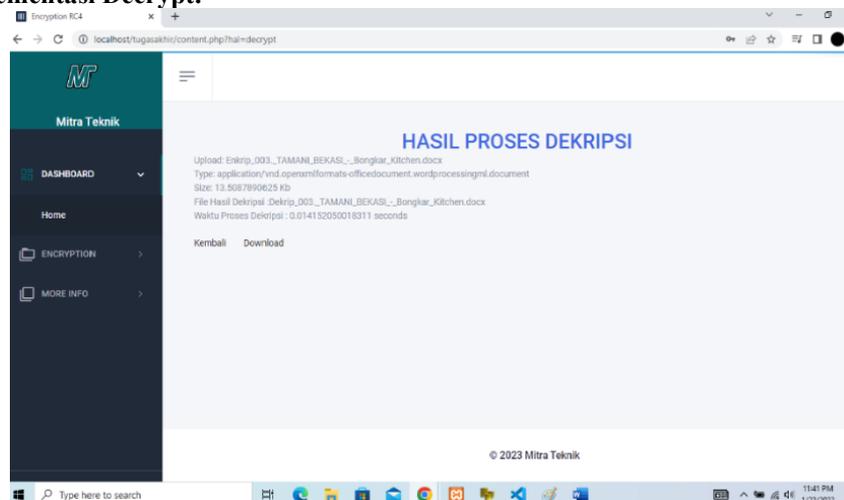
Gambar 5. Implementasi Encrypt

Pada gambar 6 merupakan hasil file yang telah di-encrypt, dimana saat file yang telah di-encrypt tersebut ingin dibuka, maka muncul notifikasi bahwa file tidak dapat dibuka.



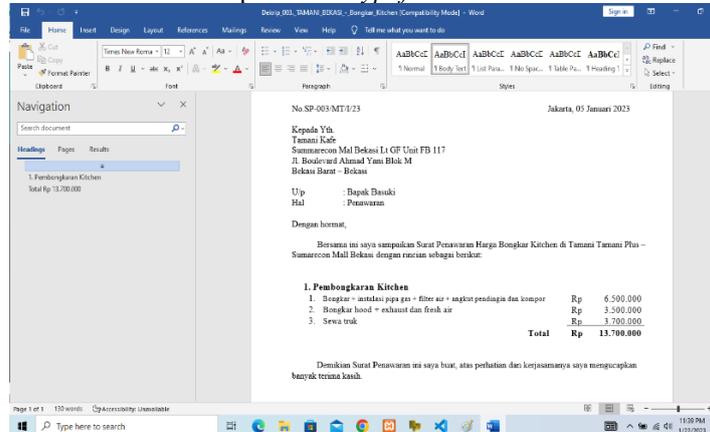
Gambar 6. Hasil Encrypt

2. Implementasi Decrypt.



Gambar 7. Implementasi Decrypt

Pada bagian *Decrypt file* ini, pada Gambar 7 adalah tampilan layar saat aplikasi telah berhasil untuk mengamankan *file* yang berukuran 13.5087890625 KB atau setara dengan 135087890,625 MB, serta memiliki waktu untuk melakukan proses *decrypt file* tersebut adalah 0.014152050018311 Seconds.



Gambar 8. Hasil Decrypt

Pada gambar 8 merupakan file yang telah di-*Decrypt*, file yang telah di *Decrypt* tersebut dapat dibuka.

3.3 Pengujian

Berikut adalah hasil dari implementasi *Rivest Code 4* yang berdasarkan bab sebelumnya tentang penerapan metode RC4 (*Rivest Code 4*) akan di tampilkan melalui tabel berikut.

Tabel 4. Hasil Pengujian Encrypt

Percobaan	Upload	Size (Byte)	Hasil <i>Encrypt</i>	Waktu Proses
1	003. TAMANI BEKASI - Bongkar Kicthen.docx	13.50000	Enkrip_003_TAMANI BEKASI_Bongkar Kitchen.docx	1,000
2	006. TELAGA SAMPIREUN ANCOL - Penggantian Pipa Gas.pdf	313.48000	Enkrip_006_TELAGA SAMPIREUN ANCOL_Penggantian Pipa Gas.pdf	21,000
3	009. TELAGA SAMPIREUN MENTENG – Gas Meter.pdf	140.24000	Enkrip_009_TELAGA SAMPIREUN MENTENG_Gas Meter.pdf	9,000
4	015. TAMANI DAPUR PUSAT – Cold Room Freezer.jpg	78.17000	Enkrip_015_TAMANI DAPUR PUSAT_Cold Room Freezer.jpg	6,000
	Rata-rata	13.634750		9.250

Tabel 5. Hasil Pengujian Decrypt

Percobaan	Upload	Size (Byte)	Hasil <i>Decrypt</i>	Waktu Proses
1	Enkrip_003_TAMANI BEKASI_Bongkar_Kicthen.docx	13.50000	Dekrip_003_TAMANI BEKASI_Bongkar Kitchen.docx	1,000
2	Enkrip_006_TELAGA SAMPIREUN ANCOL_Penggantian Pipa Gas.pdf	313.48000	Dekrip_006_TELAGA SAMPIREUN ANCOL_Penggantian Pipa Gas.pdf	22,000
3	Enkrip_009_TELAGA SAMPIREUN MENTENG_Gas Meter.pdf	140.24000	Dekrip_009_TELAGA SAMPIREUN MENTENG_Gas Meter.pdf	9,000
4	Enkrip_015_TAMANI DAPUR PUSAT_Cold Room Freezer.jpg	78.17000	Dekrip_015_TAMANI DAPUR PUSAT_Cold Room Freezer.jpg	5,000
	Rata-rata	13.634750		9.250

Hasil akhir dari penelitian ini diperoleh setelah proses enkripsi dengan algoritme RC4 rata-rata besar ukuran dokumen 13.634750 byte dan rata-rata waktu lama proses enkripsi 9.250 millisecond serta setelah proses dekripsi dengan algoritme RC4 rata-rata besar ukuran dokumen 13.634750 byte dan rata-rata waktu lama proses dekripsi 9.250 millisecond.

4. Kesimpulan

Setelah melakukan proses perancangan dan pembuatan website serta berdasarkan permasalahan yang telah disebutkan pada bab sebelumnya maka dapat disimpulkan bahwa RC4 (*Rivest Code 4*) dapat digunakan untuk mengamankan dokumen dan dapat mengembalikan dokumen seperti semula. Dengan adanya RC4 (*Rivest Code 4*) yang berbasis website dapat mengamankan file invoice dan file penting lainnya. Dengan Website yang dibuat pada penelitian ini dapat dijadikan salah satu contoh untuk mengamankan sebuah *file*.

DAFTAR PUSTAKA

- [1] N. Ratama and M. Munawaroh, “Implementasi Metode Kriptografi dengan Menggunakan Algoritma RC4 dan Steganografi Least Significant Bit Dalam Mengamankan Data Berbasis Android,” *J. Media Inform. Budidarma*, vol. 6, no. 2, p. 1272, 2022, doi: 10.30865/mib.v6i2.3902.
- [2] A. S. Sitio, “Implementasi Keamanan Data Keuangan di SMK Swasta Musda Perbaungan Menggunakan Metode RC4,” *J. Ilmu Komput. dan Sist. Inf. ...*, vol. 3, no. 3, pp. 60–66, 2020, [Online]. Available: <http://ejournal.sisfokomtek.org/index.php/jikom/article/view/90%0Ahttp://ejournal.sisfokomtek.org/index.php/jikom/article/download/90/76>
- [3] Z. Basim and Painem, “Implementasi Kriptografi Algoritma Rc4 Dan 3des Dan Steganografi Dengan Algoritma Eof Untuk Keamanan Data Berbasis Desktop Pada Smk As-Su’udiyah,” vol. 3, no. 4, pp. 54–60, 2020.
- [4] W. Pramusinto, N. Wizaksono, and A. Saputro, “Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman,” *J. Bit*, vol. 17, no. 2, pp. 46–52, 2020.
- [5] F. D. Z. Rohman and M. Mufti, “Implementasi Kriptografi Pada Pengiriman Pesan Email Dengan Menggunakan Metode Rc4 Dan Blowfish Berbasis Web Pada PT.Dascom Jaya Sakti,” *Skanika*, vol. 1, no. 2, pp. 788–793, 2018, [Online]. Available: <http://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/291>
- [6] K. Kirman, “Implementasi Algoritma Rc4 Untuk Proteksi File Mp3,” *Pseudocode*, vol. 5, no. 1, pp. 80–86, 2018, doi: 10.33369/pseudocode.5.1.80-86.
- [7] Sumarno, “Analisis Kinerja Kombinasi Algoritma Message-Digest Algoritim 5 (MD5), Rivest Shamir Adleman (RSA) dan Rivest Cipher 4 (RC4) Pada Keamanan E-Dokumen,” *Tesis*, vol. 2, no. 1, pp. 1–71, 2018, [Online]. Available: <http://jurnal.unprimdn.ac.id/index.php/JUSIKOM/article/view/140>
- [8] R. S. Siregar, M. S. Asih, and N. Wulan, “Penerapan Algoritma RC4 dan Rail Fence Untuk Enkripsi Database Mahasiswa Pada Kampus POLTEKKES KEMENKES Medan,” *Jitekh*, vol. 7, no. 2, pp. 51–56, 2019.
- [9] D. Irwansyah, “Pengamanan Data Teks Dengan Algoritma Modifikasi Rc4,” *J. Pelita Inform.*, vol. 6, no. 3, pp. 309–312, 2018.
- [10] A. Setiawan *et al.*, “Keamanan Database Aplikasi Penggajian Karyawan,” vol. 4, no. 1, pp. 66–71, 2021.