3rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
30 Agustus 2023 – Jakarta, Indonesia
Volume 2, Nomor 2, September 2023 - ISSN 2962-8628 (*online*)

PENERAPAN KRIPTOGRAFI RC4 UNTUK PENGAMANAN DOKUMEN PADA PT FAJAR MITRA KRIDA ABADI

Reza Nurmadjid[1*], Painem[2]

[1,2]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1*]1911500435@student.budiluhur.ac.id, [2]painem@budiluhur.ac.id
(* : corresponding author)

Abstrak-Perkembangan teknologi saat ini telah mengubah cara perusahaan mengelola dan melindungi data, khususnya data keuangan yang merupakan data sangat penting dan rahasia. PT. Fajar Mitra Krida Abadi, perusahaan kontruksi telekomunikasi & sipil. PT. Fajar Mitra Krida Abadi dalam melakukan pengamanan file atau melindungi data masih dilakukan dalam bentuk word maupun excel yang belum ada pengamanan file atau data. Berdasarkan latar belakang diatas, tujuan penelitan ini untuk melakukan pengamanan data keuangan pada PT. Fajar Mitra Krida Abadi. Salah satu metode yang akan digunakan untuk mengamankan data keuangan adalah dengan menggunakan metode *Rivest Code* 4 (RC4). Metode ini mengenkripsi data keuangan dengan algoritma yang kuat, sehingga hanya dapat diakses oleh pihak yang memiliki kunci yang tepat. Dengan penerapan kriptografi *Rivest Code* 4, PT. Fajar Mitra Krida Abadi dapat melindungi data keuangan mereka dari ancaman kebocoran dan penyalahgunaan. Kontribusi penelitian ini adalah modifikasi algoritme RC4 pada bagian *Key Scheduling Algorithm* (KSA) dengan menambahkan iterasi sebanyak 10 kali sehingga menghasilkan *ciphertext* yang berbeda jika menggunakan *file* yang sama dengan menggunakan metode RC4 sebelumnya. Hasil pengujian menunjukkan kecepatan waktu modifikasi RC4 pada proses dekripsi lebih cepat. Urgensi penelitian ini hilangnya reputasi untuk perusahaan. Kebocoran data dapat menyebabkan kerusakan reputasi perusahaan. Hilangnya kepercayaan pada perusahaan dan meragukan keamanan informasi data privasi mereka, menyebabkan berpindah untuk mencari tempat yang lebih terpercaya ke perusahaan lain. Hasil penelitian adalah dalam melakukan enkripsi dan dekripsi ukuran file semakin besar maka waktu yang dibutuhkan untuk proses enkripsi dan dekripsi semakin lama, waktu proses dekripsi file lebih cepat dibanding waktu proses enkripsi file.

Kata Kunci: Kriptografi, *Rivest Code 4* (RC4), *Key Scheduling Algorithm* (KSA)

APPLICATION OF RC4 CRYPTOGRAPHY FOR DOCUMENT SECURITY AT PT FAJAR MITRA KRIDA ABADI

Abstract-*Current technological developments have changed the way companies manage and protect data, especially financial data which is very important and confidential data. PT. Fajar Mitra Krida Abadi, a telecommunication & civil construction company. PT. Fajar Mitra Krida Abadi in securing files or protecting data is still done in the form of word or excel where there is no file or data security. Based on the background above, the purpose of this research is to secure financial data at PT. Fajar Mitra Krida Abadi. One method that will be used to secure financial data is to use the Rivest Code 4 (RC4) method. This method encrypts financial data with strong algorithms, making it accessible only to those with the right keys. With the application of Rivest Code 4 cryptography, PT. Fajar Mitra Krida Abadi can protect their financial data from the threat of leakage and misuse. The contribution of this research is the modification of the RC4 algorithm in the Key Scheduling Algorithm (KSA) section by adding 10 iterations so as to produce a different ciphertext if using the same file using the previous RC4 method. The test results show that the speed of the RC4 modification time in the decryption process is faster. The urgency of this research is the loss of reputation for the company. Data leaks can cause damage to a company's reputation. Loss of trust in companies and doubting the security of their information and privacy data, causing them to move to find a more trusted place to another company. The result of the research is that in encrypting and decrypting the larger the file size, the longer the time needed for the encryption and decryption process, the file decryption process time is faster than the file encryption process time.*

Keywords*: Cryptography, Rivest Code 4 (RC4), Key Scheduling Algorithm* (KSA)

1. PENDAHULUAN

Perkembangan teknologi saat ini sangat pesat, begitu juga dalam mengamankan data. Dalam dunia perusahaan, keamanan data sangatlah penting dan harus dijaga dengan baik. Data yang penting biasanya disimpan dan diolah menggunakan aplikasi *Microsoft Office*, data tersebut bisa berupa *Microsoft Word* atau *Microsoft Power*

Point untuk mengelola sebuah kata. *Microsoft Excel* untuk mengelola angka, dan *Microsoft Acces* digunakan untuk pengoperasian database [1][2].

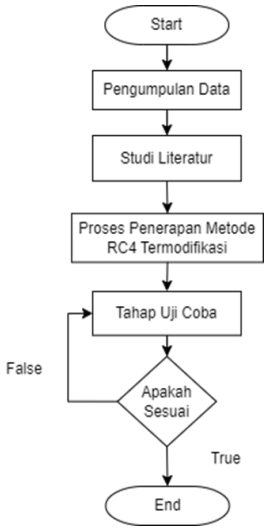
Tujuan penelitan ini untuk melakukan pengamanan data keuangan pada PT. Fajar Mitra Krida Abadi. Urgensi penelitian ini hilangnya reputasi untuk perusahaan. Kebocoran data dapat menyebabkan kerusakan reputasi perusahaan. Hilangnya kepercayaan pada perusahaan dan meragukan keamanan informasi data privasi mereka, menyebabkan berpindah untuk mencari tempat yang lebih terpercaya ke perusahaan lain. Untuk mengatasi masalah tersebut, data harus dilindungi dari pencurian data yang akan berdampak buruk bagi perusahaan tersebut, agar tidak ada penyalahgunaan data Keuangan tersebut, sehingga dibutuhkan upaya pencegahan di PT. Fajar Mitra Krida Abadi. Dengan menerapkan kriptografi RC4 berbasis *web*, PT. Fajar Mitra Krida Abadi dapat memastikan bahwa data keuangan mereka terlindungi dan aman. Manfaat dari penelitian ini untuk perusahaan, agar sistem kripotgrafi ini bukan hanya diterapkan pada file keuangan tetapi pada bidang lainnya, sehingga penggunaan algoritme RC4 dapat digunakan dalam berbagai bidang dengan baik dan bijak. Ini membantu perusahaan untuk memenuhi standar keamanan data yang ditetapkan oleh peraturan yang berlaku [3].

Penelitian terkait dengan kriptografi dilakukan oleh [4] menyatakan bahwa kelebihan dari metode RC4 ini adalah ketika ada suatu kerusakan pada satu bit, tidak mempengaruhi keseluruhan ini pesan. Penelitian berikutnya membahas enkripsi kriptografi dengan metode Rivest Code 4 (RC4) berbasis web dari [5] dengan berjudulkan "Implementasi Algoritma Kriptografi RC4 Untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web Pada PT. Trans Intra Asia" pada penelitian di atas bertujuan untuk mengamankan database aplikasi penggajian karyawan berbasis web dengan metode Rivest Code 4 (RC4). Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5 [6]. Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Algoritma Kriptografi [3]. Berbeda dengan penelitian sebelumnya, penelitian ini berupaya menerapkan modifikasi algoritma RC4 untuk mengamankan data pada perusahaan PT. Fajar Mitra Krida Abadi agar *file* enkripsi tersebut tidak dapat di dekripsi dengan algoritma RC4 yang biasa.

Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping [7]. Terdapat penelitian terdahulu mengenai kasus yang ada, beberapa penelitian tersebut dijadikan acuan dan referensi untuk melakukan penelitian ini, beberapa jurnal tersebut seperti yang di atas. Perbedaan dari penelitian saat ini menggunakan metode yang berbeda, metode yang digunakan pada penelitian ini yaitu RC4, keunggulan RC4 sendiri yaitu kemudahan dalam implementasi dan penggunaannya, serta kecepatan operasional dan penyebarannya. Alasan memilih metode RC4 menurut [4], kelebihan dari metode RC4 ini hasil pesannya tidak mempengaruhi keseluruhan isi pesan ketika ada suatu kerusakan pada satu bit. Algoritma ini memungkinkan pemrosesan data yang berkelanjutan dengan cepat dan efisien. Dan pada format yang dienkripsi akan diimplementasikan sistem pengamananan data berbasis web menggunakan metode algoritma RC4 untuk mengenkripsi data keuangan berupa file yang ada di PT. Fajar Mitra Krida Abadi. Kontribusi penelitian ini adalah modifikasi algoritme RC4 pada bagian *Key Scheduling Algorithm* (KSA) dengan menambahkan iterasi sebanyak 10 kali sehingga menghasilkan *ciphertext* yang berbeda jika menggunakan *file* yang sama dengan menggunakan metode RC4 sebelumnya.

2. METODE PENELITIAN

Dalam rangka menjalankan penelitian, metode penelitian digunakan sebagai pedoman utama untuk memastikan pencapaian tujuan yang telah ditetapkan sebelumnya tetap terpenuhi. Tahapan penelitian ini dapat dilihat dalam Gambar 1. Berikut ini adalah penjelasan dari setiap tahapan metode yang dilakukan. Pada Gambar 1 menunjukkan alur penerapan metode yang dilakukan, meliputi : pengumpulan data, studi literatur, proses penerapan metode RC4 termodifikasi, dan tahap uji coba.



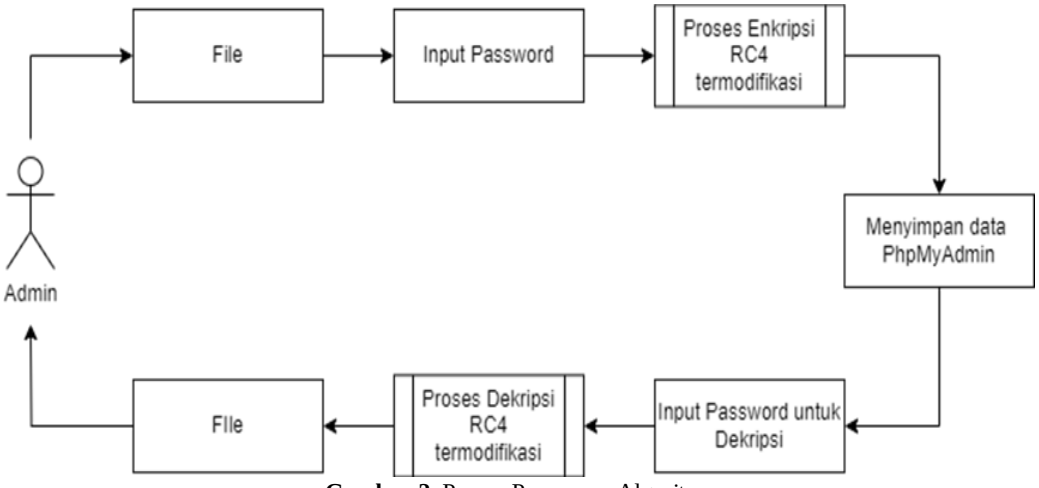
Gambar 1. Skema Penerapan Metode

2.1 Pengumpulan Data

Pada tahap ini, dilakukan proses pengumpulan data yang digunakan dalam penelitian ini [8][9]. Proses wawancara dilakukan dengan berdialog langsung dengan *owner* dari PT. Fajar Mitra Krida Abadi untuk memperoleh informasi terkait keamanan yang diterapkan di perusahaan tersebut. Observasi dilakukan untuk pengumpulan data dengan mengamati sistem yang telah digunakan sebelumnya di perusahaan. Tujuan dari observasi ini adalah untuk memahami sistem yang sudah ada dan mendapatkan wawasan mengenai kebutuhan dan kelemahan yang ada.

2.2 Penerapan Metode RC4

RC4 (*Rivest Cipher* 4) adalah sebuah algoritma *stream cipher* yang menggunakan kunci simetris [10] untuk mengenkripsi teks biasa digit demi digit atau *byte* demi *byte* atau *byte* demi *byte* dengan menggabungkannya melalui operasi biner dengan bilangan semi-acak. Langkah inisialisasi RC4 terdiri dari memilih *byte* keluaran dengan mencari nilai S[i] dan S[j], menambahkannya modulo 256, dan menggunakan hasilnya sebagai indeks dalam array S. *Byte* diperoleh dari operasi Ini operasi, S(S[i] + S[j]), digunakan sebagai *byte* dalam aliran kunci, K. [11]. Permasalahan di PT. Fajar Mitra Krida Abadi adalah belum adanya program enkripsi untuk keamanan *file* data penting. Sehingga diperlukannya program enkripsi untuk menjamin keamanan *file-file* tersebut. Gambar 2 menunjukkan proses penerapan metode pada program yang dihasilkan menggunakan metode *Rivest Code* 4 (RC4). Pada Gambar 1 adalah alur metode dari RC4 [12].



Gambar 2. Proses Penerapan Algoritma

2.3 Rancangan Pengujian

Pengujian yang dilakukan terdiri dari dua macam yaitu pengujian sistem aplikasi dengan menggunakan metode *Blackbox* [13] dan pengujian *file* [10]. Pengujian *Blackbox* diperlukan untuk mengetahui program bekerja sesuai dengan kebutuhan oleh perusahaan dan tidak terdapat *error* saat dioperasikan. Pengujian *file* diperlukan untuk melihat efisiensi dan efektifitas dari *file* sebelum di enkripsi atau deskripsi dan sesudah di enkripsi atau deskripsi dari segi ukuran dan proses waktu.

3. HASIL DAN PEMBAHASAN

Hasil penelitian ini berisi data penelitian, hasil implementasi metode dan pengujian sistem aplikasi serta pengujian file.

3.1 Data Penelitian

Data yang digunakan dalam penelitian ini adalah data keuangan pada PT. Fajar Mitra Krida Abadi dengan menerapkan Algoritma RC4 dapat mencegah dan melindungi data keuangan tersebut agar tidak ada penyalahgunaan oleh pihak yang tidak bertanggung jawab. *File* tersebut berisi Surat Pernyataan Direksi, Laporan Auditor Independen, Keuangan, Laba Rugi, Perubahan Ekuitas, Arus Kas, Rincian Piutang Usaha dan Utang Usaha. Data penelitian yang didapatkan dari tempat riset disajikan pada Tabel 1.

Tabel 1. Data Penelitian

No	Nama File	Ukuran File	Ekstensi
1	Laporan Keuangan 31 Desember 2020 Dan Laporan Auditor Inderpenden-1	5.44 MB	pdf
2	Laporan Laba Rugi Untuk Tahun Yang Berakhir 31 Desember 2020 (Dalam Rupiah)	97.7 KB	xlsx
3	Laporan Auditor Independen	1.72 MB	pptx
4	Laporan Keuangan 31 Desember 2020	2.48 MB	docx
...	...	...	...
10	Laporan Keuangan 20 Oktober 2019	2.35 MB	pdf

3.2 Implementasi Metode

Pada tahap implementasi metode RC4 pada aplikasi berbasis web, terdapat beberapa langkah yang dilakukan, antara lain sebagai berikut :

3.2.1 Proses Enkripsi

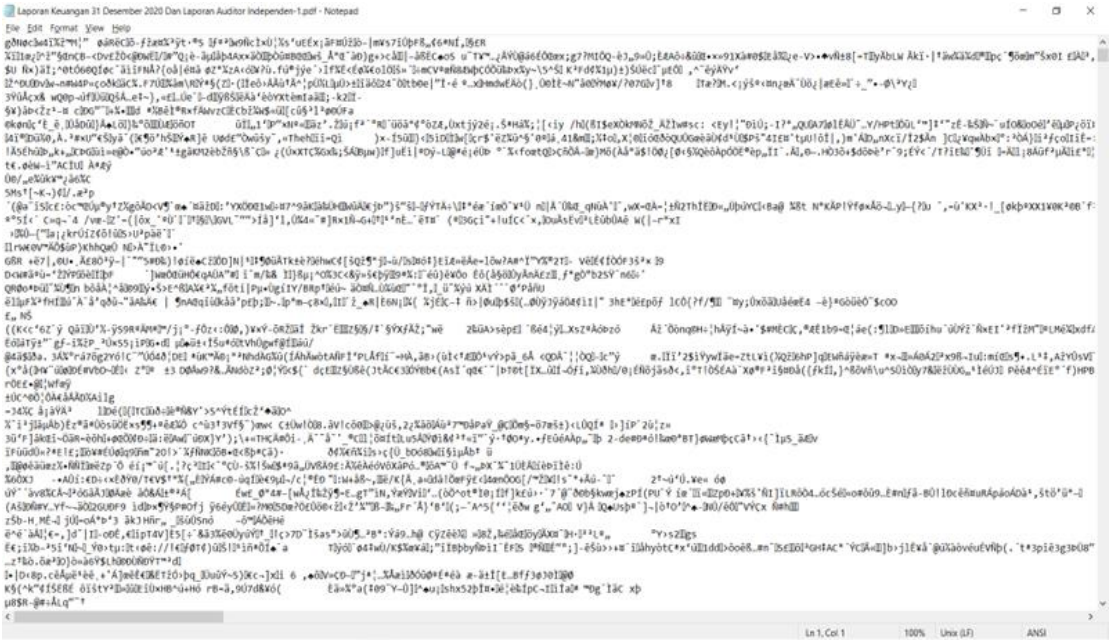
Pada Algoritme 1, dijelaskan bagaimana proses enkripsi dilakukan. Terdapat modifikasi yang di tambahkan pada bagian KSA yang dibagian kotak merah. Modifikasi yang dilakukan terdapat pertambahan iterasi menjadi 10 kali dan menghasilkan output yang berbeda dari RC4 sebelumnya. Pada Gambar 3 merupakan hasil dari enkripsi *file* menjadi *ciphertext*.

Algoritme 1. Enkripsi RC4 Termodifikasi

```
1.  Start
2.  Input key enkripsi
3.   i=0
4.    If i<256 then
5.        S[i]=i
6.        Key[i]=key[i]
7.        Modkey length j
8.        i=i+1
9.  i=0
10. j=0
11. if i<256 then
12.      j=(s[i]+key[i] mod key length) mod 256
13.      swap s[i] & s[j]
14. else
15. k=0
16. if (k<10) then
```

Modifikasi RC4 Pada Proses Enkripsi

```
17.       i=(i+1)mod 256
18.       j=(j+ s[i] mod 256 swap s[i] & s[j]
19.     k=k+1
20.  else
21.       plaintext
22.  i=0
23.  j=0
24.  y=0
25.  if  y<plaintext length then
26.       i=(i+1) mod 256
27.       j=(j+s[i] mod 256 swap s[i] & s[j]
28.       s=(s[i]+s[j]) mod 256
29.     y=y+1
30.  else
31.       ciphertext
32.   End
```



Gambar 3. File yang Dienkripsi

3.2.2 Proses Dekripsi

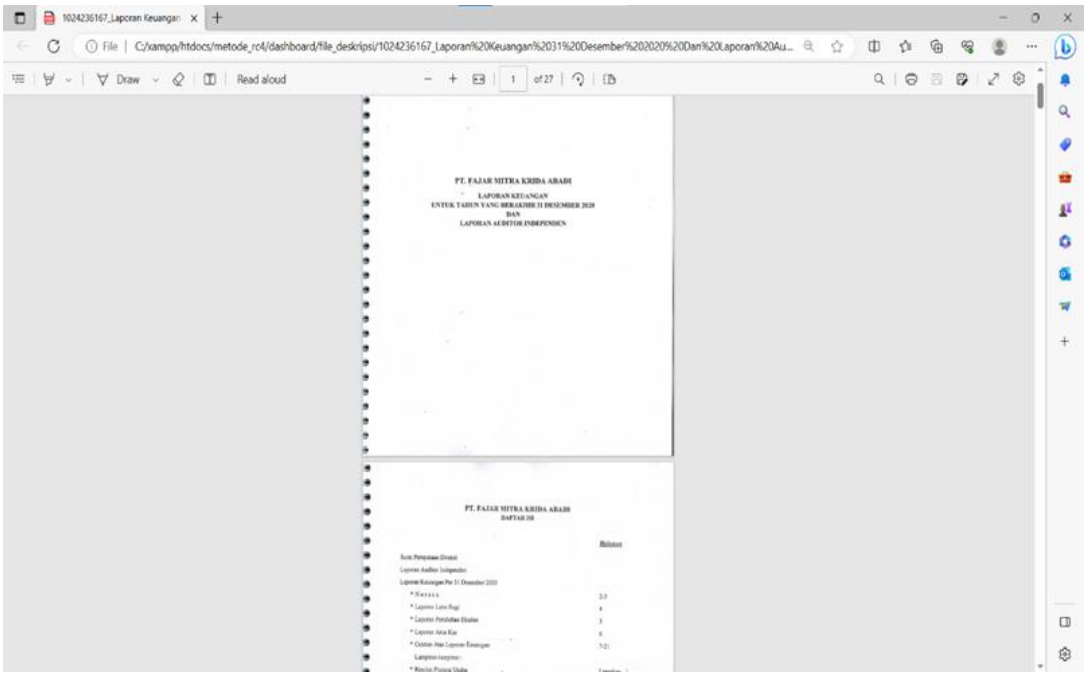
Pada Algoritme 2, dijelaskan bagaimana proses dekripsi dilakukan. Terdapat modifikasi yang di tambahkan pada bagian KSA yang dibagian kotak merah. Modifikasi yang dilakukan terdapat pertambahan iterasi menjadi 10 kali. Karena proses dekripsi harus sama dengan proses enkripsi. Pada Gambar 4 merupakan hasil dari *ciphertext* pada Gambar 3 menjadi *plaintext*.

Algoritme 2. Form Deskripsi

```
1.  Start
2.  Input key dekripsi
3.  I=0
4.  if i<256 then
5.       S[i]=i
6.       Key[i]=key[i]
```

```
7.      Modkey length j
8.      i=i+1
9.    i=0
10.   j=0
11.   if  i<256 then
12.       j=(s[i]+key[i] mode key lengtht) mod 256
13.       swap s[i] & s[j]
14.   else
15.     k=0
16.   jika (k<10) then
17.       i=(i+1)mod 256
18.       j=(j+s[i] mod 256 swap s[i] & s[j]
19.       k=k+1
20.   else
21.     chipertext
22.   i=0
23.   j=0
24.   y=0
25.   if  y<ciphetext length then
26.       i=(i+1) mod 256
27.       j=(j+s[i] mod 256 swap s[i] & s[j]
28.       s=(s[i]+s[j]) mod 256
29.     y=y+1
30.   else
31.     plaintext
32.   End
```

Modifikasi RC4 Pada Proses Dekripsi



Gambar 4. Hasil Proses Dekripsi

3.3 Hasil Pengujian

Pada Tabel 2 Disajikan hasil dari pengujian aplikasi dengan metode *black box* yang dilakukan pada sistem yang dibangun. Terdapat 5 komponen dan 24 poin pengujian.

Tabel 2. Hasil Black Box Testing

No	Komponen	Pengujian	Hasil yang diharapkan	Hasil
1	Login	Tidak mengisi Username dan Password kemudian klik tombol Login	Sistem akan menolak dan akan menampilkan pesan "Harap isi bidang ini" pada kolom Username	Berhasil
		Mengisi Username dan tidak mengisi Password kemudian klik tombol Login	Sistem akan menolak dan akan menampilkan pesan "Harap isi bidang ini" pada kolom Password	Berhasil
		Tidak mengisi Username dan mengisi Password kemudian klik tombol Login	Sistem akan menolak dan akan menampilkan pesan "Harap isi bidang ini" pada kolom Username	Berhasil
…	…	…	…	…

Pengujian file dapat dilihat pada tabel 3 dan tabel 4 enkripsi dan dekripsi berdasarkan ukuran file dan waktu yang dibutuhkan pada saat melakukan proses enkripsi dan dekripsi.

Tabel 3. Pengujian File Enkripsi Dan Dekripsi Sebelum Modifikasi

Nama File	Ukuran File (Kilobyte)			Waktu (Detik)	
	Asli	Enkripsi	Dekripsi	Enkripsi	Dekripsi
Laporan Keuangan 31 Desember 2020 Dan Laporan Auditor Independen-1	5.578	5.578	5.578	2.71	2.58
Laporan Laba Rugi Untuk Tahun Yang Berakhir 31 Desember 2020 (Dalam Rupiah)	98	98	98	0.06	0.06
Laporan Auditor Independen	1.770	1.770	1.770	0.82	0.78
Laporan Keuangan 31 Desember 2020	2.548	2.548	2.548	1.25	1.09
…	…	…	…	…	…
Laporan Keuangan 20 Oktober 2019	1.770	1.770	1.770	0.92	0.82

Pada Tabel 3 disajikan proses enkripsi dan dekripsi dengan menggunakan algoritma RC4 sebelum dimodifikasi. Pada file laporan keuangan Desember 2020 Dan Laporan Auditor Inderpenden-1 dalam bentuk pdf dengan ukuran file 5.578 KB , setelah dilakukan proses enkripsi dan dekripsi ukuran file sama dengan file asli dengan kecepatan waktu proses enkripsi 2.71 detik dan proses dekripsi dengan kecepatan waktu 2.58 detik. Proses dekripsi lebih cepat dengan proses enkripsi.

Tabel 4. Pengujian File Enkripsi Dan Dekripsi Sesudah Modifikasi

Nama File	Ukuran File (Kilobyte)			Waktu (Detik)	
	Asli	Enkripsi	Dekripsi	Enkripsi	Dekripsi
Laporan Keuangan 31 Desember 2020 Dan Laporan Auditor Independen-1	5.578	5.578	5.578	3.03	1.71
Laporan Laba Rugi Untuk Tahun Yang	98	98	98	0.06	0.06

Berakhir 31 Desember 2020 (Dalam Rupiah)					
Laporan Auditor Independen	1.770	1.770	1.770	0.52	0.79
Laporan Keuangan 31 Desember 2020	2.548	2.548	2.548	0.82	0.73
…	…	…	…	…	…
Laporan Keuangan 20 Oktober 2019	1.770	1.770	1.770	1.16	0.8

Pada Tabel 4 disajikan proses enkripsi dan dekripsi dengan menggunakan algoritma RC4 sesudah dimodifikasi. Pada *file* laporan keuangan Desember 2020 Dan Laporan Auditor Inderpenden-1 dalam bentuk pdf dengan ukuran *file* 5.578 KB , setelah dilakukan proses enkripsi dan dekripsi ukuran *file* sama dengan *file* asli dengan kecepatan waktu proses enkripsi 3.03 detik dan proses dekripsi dengan kecepatan waktu 1.71 detik. Proses dekripsi lebih cepat dibandingkan dengan proses enkripsi .

Berdasarkan Tabel 3 yang merupakan tabel waktu kecepatan proses enkripsi dan dekripsi dengan algoritma RC4 sebelum dimodifikasi, dan Tabel 4 yang menampilkan tabel waktu kecepatan proses enkripsi dan dekripsi dengan algoritma RC4 yang sudah dimodifikasi terlihat perbedaan dari kecepatan waktu proses enkripsi dan dekripsi. Proses enkripsi pada Tabel 4 lebih lama dan proses dekripsi pada Tabel 4 lebih cepat dibandingkan proses pada Tabel 3. Hasil pengujian menunjukkan kecepatan waktu modifikasi RC4 pada proses dekripsi lebih cepat.

4. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan mengenai pengembangan aplikasi keamanan data dengan pengimplementasian algoritma Kriptografi *Rivest Code* 4 (RC4) pada PT. Fajar Mitra Krida Abadi, berikut adalah bebrapa kesimpulan yang dapat diambil yaitu Dalam melakukan enkripsi dan dekripsi ukuran file semakin besar maka waktu yang dibutuhkan untuk proses enkripsi dan dekripsi semakin lama. Pengamanan file dengan menggunakan metode RC4 merupakan salah satu metode yang membantu dalam mengamankan file data keuangan pada PT. Fajar Mitra Krida Abadi. Berdasarkan pengujian aplikasi dengan menggunakan black box testing dilakukan, maka aplikasi yang dibuat berjalan dengan baik. Berdasarkan kesimpulan yang telah dijelaskan, berikut adalah beberapa saran yang dapat diberikan untuk penelitian ini yaitu Melakukan pelatihan dan sosialisasi aplikasi yang dibuat kepada karyawan mengenai penggunaan aplikasi keamanan data ini. Perlu dilakukan evaluasi dan pemantauan secara berkala terhadap sistem keamanan data yang telah diterapkan. Hal ini bertujuan untuk memastikan bahwa sistem tersebut tetap efektif dan dapat mengatasi ancaman keamanan yang terus berkembang. Dalam pengembangan aplikasi keamanan data di masa depan, peneliti atau pengembang dapat mempertimbangkan penggunaan agoritma kriptografi lainnya selain RC4 atau meggunakan lebih dari satu metode.

DAFTAR PUSTAKA

[1] A. S. Sitio, “Implementasi Keamanan Data Keuangan di SMK Swasta Musda Perbaungan Menggunakan Metode RC4,” vol. 3, no. 3, pp. 60–66, 2021.

[2] W. R. Maya, A. Azanuddin, and E. Elfitriani, “Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES,” *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 21, no. 1, p. 1, 2022, doi: 10.53513/jis.v21i1.4764.

[3] S. Vivi Wahdini, D. Hartama, and I. Okta Kirana, “Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Algoritma Kriptografi,” *J. Informatics Manag. Inf. Technol.*, vol. 1, no. 3, pp. 101–107, 2021, [Online]. Available: https://hostjournals.com/

[4] Hendrawati, Hamdani, and A. H. K, “KEAMANAN DATA DENGAN MENGGUNAKAN ALGORITMA RIVEST CODE 4 (RC4) DAN STEGANOGRAFI PADA CITRA DIGITAL,” *Inform. mulawarman*, vol. 9, no. 1, 2014.

[5] A. Setiawan *et al.*, “KEAMANAN DATABASE APLIKASI PENGGAJIAN KARYAWAN,” vol. 4, no. 1, pp. 66–71, 2021.

[6] A. Z. F. Rangkuti and H. Fahmi, “Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5,” *J. Nas. Komputasi dan Teknol. Inf.*, vol. 3, no. 2, pp. 170–175, 2020, doi: 10.32672/jnkti.v3i2.2384.

[7] R. Nuari and N. Ratama, “Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping,” *J. Artif. Intell. Innov. Appl.*, vol. 1, no. 2, pp. 2716–1501, 2020, [Online]. Available: http://openjournal.unpam.ac.id/index.php/JOAIIA

[8] L. Silalahi and A. Sindar, “Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati

Menggunakan SHA-1," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 3, no. 2, pp. 182–186, 2020, doi: 10.32672/jnkti.v3i2.2413.

[9] 2007 Pramantyo, Adhi, "Keamanan Data Dengan Kriptografi Einstein," *J. Teknol. Inf. MURA*, vol. 11, no. 1, pp. 29–36, 2019.

[10] A. Amrulloh and E. I. H. Ujianto, "Kriptografi Simetris Menggunakan Algoritma Vigenere Cipher," *J. CoreIT*, vol. 5, no. 2, pp. 71–77, 2019.

[11] D. R. Saragi, J. M. Gultom, J. A. Tampubolon, and I. Gunawan, "Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4," vol. 1, pp. 114–119, 2020, doi: 10.30865/json.v1i2.1745.

[12] J. Prayudha, O. Krianto Sulaiman, I. Mariami, and J. Halim, "Implementasi Revest Code 4 (RC4) Untuk Data Resep Obat Di RSUP H.Adam Malik," *J. Penerapan Sist. Inf. (Komputer Manajemen)*, vol. 2, no. 3, pp. 174–181, 2021.

[13] N. M. D. Febriyanti, A. A. K. O. Sudana, and I. N. Piarsa, "Implementasi Black Box Testing pada Sistem Informasi Manajemen Dosen," *J. Ilm. Teknol. dan Komput.*, vol. 2, no. 3, pp. 1–10, 2021.