PENGAMANAN FILE PENDAFTARAN SISWA BARU MENGGUNAKAN METODE ALGORITME RC4 DI TK NURUL IRFAN

Muhammad Apriyanda Sutejo[1*], Mardi Hardjianto[2]

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

Email: [1*]1811502168@student.budiluhur.ac.id, [2]mardi.hardjianto@budiluhur.ac.id
(* : corresponding author)

Abstrak-Pada setiap tahunnya Sekolah TK Nurul Irfan terjadi pendaftaran siswa baru yang memberikan berkas – berkas siswa yang mendaftar pada sekolah TK Nurul Irfan. Dari banyaknya siswa yang mendaftar terdapatlah dokumen – dokumen penting seperti formulir yang berisikan data diri siswa pendaftar beserta pas foto dan akte kelahiran. Dengan banyaknya dokumen tersebut maka seringkali TK Nurul Irfan terjadi kebocoran dokumen siswa pendaftar baru oleh pihak yang tidak berwajib yang amat sangat disayangkan apabila data siswa baru tersebut disalah gunakan. Maka dari itu digunakanlah pengamanan data dengan menggunakan metode algoritme RC4 (*rivest code 4*) yang diperuntukan untuk mengenkripsi serta dekripsi dokumen siswa – siswa baru, yang dimana dokumen tersebut akan dienkripsi dan diberikan password serta hanya yang mengetahui passwordnya saja yang dapat mendekripsi berkas tersebut hingga dapat membuka dokumen - dokumen tersebut. Maka dengan ini dibuatlah pengaman data menggunakan teknik kriptografi untuk mengenkrip dan dekrip dengan metode algoritme RC4 (*Rivest Code 4*) berbasis *Website*. Dengan metode ini kedepannya akan mengenkrip data - data sekolah lainnya tidak hanya mengenkrip berkas - berkas siswa baru saja, seperti data keungan sekolah yang amat sangat penting untuk diamankan. Hasil dari pengujian ini dapat berjalan baik dengan menggunakan metode algoritme *Rivest Code 4* untuk mengamankan berkas – berkas pendaftaran siswa baru.

Kata Kunci: *website*, dokumen, kriptografi, *rivest code 4*, enkripsi

SECURITY OF NEW STUDENT REGISTRATION FILES USING THE RC4 ALGORITHM METHOD IN TK NURUL IRFAN

Abstract- *Every year the Nurul Irfan Kindergarten School registers new students who provide files for students who register at the Nurul Irfan Kindergarten school. Of the many students who register, there are important documents such as a form containing the registrant student's personal data along with a photo and birth certificate. With so many documents, Nurul Irfan Kindergarten often leaks documents for new registrants by unauthorized parties, which is very, very unfortunate if the new student data is misused. Therefore, data security is used using the RC4 algorithm method (rivet code 4) which is intended to encrypt and decrypt new student documents, where the document will be encrypted and given a password and only those who know the password can decrypt the file until it can be accessed. open these documents. So with this a data security is made using cryptographic techniques to encrypt and decrypt the RC4 algorithm method (Rivest Code 4) based on the Website. With this method in the future, it will encrypt other school data, not only encrypting new student files, such as school financial data which is very, very important for safekeeping. The results of this test can run well by using the Rivest Code 4 algorithm method to secure new student registration files.*

Keywords*: website, documents, cryptography, rivest code 4, encrypt*

1. PENDAHULUAN

Taman Kanak – Kanak (TK) Nurul Irfan yang bergerak dibidang pendidikan yang diperuntukan untuk anak – anak pada usia 4 sampai 6 tahun, berlokasi di Kademangan, Setu, Tangerang Selatan, Banten. Dengan status kepemilikan yayasan. pada setiap tahunnya membuka pendaftaran yang dimana banyak data pribadi dari calon siswa baru seperti formulir yang berisi data diri dari pendaftar, Akte kelahiran, kartu keluarga, dan foto. Dengan banyaknya data yang diberikan kepada pihak sekolah TK Nurul Irfan sering terjadi kebocoran data pribadi calon siswa baru yang amat disayangkan bila data pribadi tersebut jatuh kepada orang yang salah dan disalah gunakan.

Data - data siswa baru yang disimpan belum memiliki keamanan untuk menjaga data - data terbut dari kebocoran data, yang sering terjadi kebocoran data dan disalah gunakan oleh pihak yang tidak bertanggung jawab. Maka dari itu penulis menyarankan untuk menggunakan teknik kriptografi dengan metode algoritme RC4 (*Rivest Code 4*) untuk mengenkripsi dan dekripsi supaya dapat mengamankan data yang disimpan kedalam database. Peneliti lebih memilih *stream chiper* RC4 (*Rivest code 4*) dari pada *stream chiper* lainnya dikarenakan sampai saat

ini tidak ada yang dapat memecahkan RC4 sehinggat dapat dikatakan sangat kuat serta cocok dalam enkripsi berkas dikarenakan derajat keabuan 0 sampai 255.

Pada kali ini peneliti menggunakan teknik kriptografi dengan digunakannya metode RC4 (*Rivest Code 4*). Data yang di input banyak terdapat data pribadi yang sangat penting, maka dari itu di tambahkan kriptografi dalam file pendaftaran siswa baru agar data yang disimpan oleh guru dapat diamankan. Dengan menggunakan keamanan seperti ini maka akan memperkecil kemungkinan keborcoran data. Dimana metode tersebut berfungsi untuk mengenkripsi plainteks secara byte per byte dengan cara mengkombinasi operasi biner dengan sebuah angka semi acak. Dengan adanya ini maka dokumen yang akan diinput oleh guru sekolah Tk Nurul Irfan akan aman.

Dari uraian diatas peneliti ingin mengimplementasikan penggunaan metode RC4 (Rivest Code 4) untuk melakukan enkripsi dokumen pendaftar baru. Serta menggunakan mySQL sebagai database.

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi terdapat dua konsep dasar yang penting yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana data di ubah menjadi sulit untuk di ketahui atau tidak bisa di baca (Chipertext). Dekripsi adalah proses dimana mengembalikan data yang sudah di enkripsi data akan menjadi kembali seperti awal dimana data menjadi data yang asli (Plaintext).

a. Enkripsi dan Dekripsi
   Enkripsi adalah proses yang dilakukan untuk mengubah file yang tidak rusak pesan (teks biasa) kedalam bentuk yang tidak terbaca (teks chip),dekripsi adalah proses mengubah pesan yang tidak dapat dibaca menjadi bentuk yang dapat dibaca dan dipahami. Proses enkripsi dan dekripsi diatur oleh satu atau lebih kunci kriptografi (Dhany et al., 2018).
b. Tujuan Kriptografi
   Dari penjelasan awal dapat disimpulkan bahwa kriptografi bertujuan untuk memberikan layanan keamanan. Yang disebut aspek keamanan:
   1. Kerahasiaan (confidentiality) Merupakan layanan yang dipergunakan untuk menjaga supaya pesan tidak bocor kepada pihak yang tidak bertanggung jawab.
   2. Integritas data (data integrity) Merupakan layanan yang menjamin bahwa dokumen itu asli atau tidak dimanipulasi selama transmisi.
   3. Otentikasi (authentication) Merupakan layanan yang berkaitan dengan identifikasi, baik mengidentifikasi kebenaran dari pihak yang berkomunikasi.
   4. Non-repudiation Adalah layanan untuk menjaga entitas yang berkomunikasi agar tidak menyangkal (Pabokory et al., 2016).

2.2 Rivest Code 4 (RC 4)

Secara umum pada sistem keamanan seperti protokol SSL (Secure Socket Layer). Algoritma kriptografi ini sederhana dan mudah untuk digunakan. RC4 dibuat oleh Ron Rivest dari RSA Labs (RC adalah singkatan dari Ron's Code). RC4 menghasilkan keystream setelah itu di-XOR dengan plaintext pada saat enkripsi (atau di-XOR dengan bit ciphertext pada saat dekripsi). RC4 memproses data dalam byte (1 byte = 8 bit). Untuk menghasilkan aliran kunci, cipher menggunakan keadaan internal yang terdapat pada 2 bagian yaitu:

a. Permutasi bilangan 0 sampai 255 pada larik S0, S1, ..., S255. Permutasi adalah kunci U dengan panjang variabel.
b. Dua penghitung indeks, i dan j [6]. Sistem cipher RC4 menggunakan status, yang merupakan array 256 byte yang diubah, dan dicampur dengan kunci. Kunci enkripsi juga dan dicampur dengan kunci. Kunci enkripsi juga merupakan array 256 byte. Sebelum melakukan enkripsi dan dekripsi, sistem cipher RC4 menginisialisasi keadaan dengan suatu algoritma, algoritma ini disebut penjadwalan kunci.

Metode inisialisasi S-Box (Array S) dapat dilihat pada berikut ini:

1. Proses Inisialisasi S-Box(Array S)
   for i = 0;i<256;i++;
   S[i] = i

Metode inisialisasi S-Box (Array K) dapat dilihat pada berikut ini:

2. Proses Inisialisasi S-Box (Array K) array Kunci // Array dengan panjang kunci “length”.
   j = 0
   for i = 0; I <256; i++;

```
j =  (j +  S[i] + (this → key[i % strlen ( this → key)])) % 256
x = S[i]
S[i] = S[j]
S[j] = x
```

Setelah melakukan langkah pengacakan S-Box yang dapat dilihat sebagai berikut:

3. Proses Pengacakan S-Box

```
i = 0; j = 0; res = 0;
for y = 0 ; y < strlen (this → str) ;  y ++;
```

Lalu buat pseudo random byte dengan langkah sebagai berikut:

4. Pseudo Random Byte

```
i =  (i + 1) % 256;
j = (j + S[i]) % 256;
x = S[i];
S[i] = S[j];
S[j] = x;
Res = this → str[y] ^ chr(S[(S[i] + S[j]) % 256]);
```

2.3 Penerapan Metode

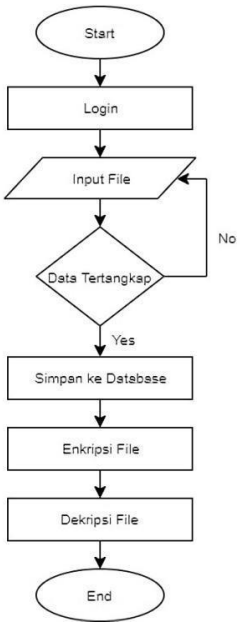
Metode penelitian yang digunakan pada penelitian ini adalah model waterfall. Menurut Pressman (2003) model waterlfall adalah model klasik yang bersifat sistematis, berurutan dalam membangun software.

a. Komunikasi
Langkah pertama dalam membangun sistem adalah menganalisis dan mengkomunikasikan kebutuhan sistem berdasarkan hasil pengumpulan data. Dari tahap komunikasi disimpulkan bahwa diperlukan suatu sistem untuk mengamankan dokumen file penting yang ada di file TK – Nurul Irfan.

b. Perencanaan
Tahap perencanaan menggambarkan tugas-tugas teknis yang harus dilakukan mulai dari pengumpulan data hingga pengujian sistem, risiko yang mungkin terjadi saat melaksanakan tugas tersebut, dan hasil yang akan diperoleh yaitu terciptanya sistem keamanan untuk dokumen file penting yang berada di sekolah dengan menggunakan algoritma RC4.

c. Pemodelan
Tahap pemodelan bertuju kepada perancangan skema sistem keamanan dokumen digital untuk soal-soal ujian dan kemudian perancangan database menggunakan MySQL sebagai sistem basis data. Selanjutnya merancang antarmuka sistem keamanan file dokumen. Sistem Flowcart dapat dilihat pada gambar berikut.

Flowchart Sistem Pengamanan Data Digital



Gambar 1. *Flowchart System*

dengan login, di mana pengguna memasukkan nama pengguna dan kata sandi. Kemudian, pengguna dapat menginput file tersebut ke dalam sistem, yang kemudian sistem akan menangkap file tersebut dan menyimpannya ke dalam database. Selanjutnya, file tersebut dapat dienkripsi dan kemudian didekripsi lagi jika diperlukan oleh pengguna.

d. Konstruksi
Konstruksi adalah tahap pembuatan kode, untuk membuat sistem yang sudah dirancang. Bahasa pemrograman yang digunakan untuk membangun sistem adalah HTML, PHP dan menggunakan database MySQL sebagai penyimpanan datanya. Algoritma RC4 digunakan untuk mengamankan data yang dimasukkan pada database. Dan kemudian bisa kembali seperti semula saat dibutuhkan. Setelah proses coding selesai maka akan dilakukan pengujian pada sistem yang dibangun. Pengujian sistem dilakukan dengan menggunakan blackbox. Pengujian blackbox dilakukan untuk mengetahui apakah fungsi-fungsi pada program dapat berjalan dengan baik, mulai dari menerima input, memproses dan memberikan output. Pengujian terakhir menggunakan perangkat lunak penyerang yang berfokus pada hasil penerapan algoritma enkripsi RC4 pada konten file dokumen.

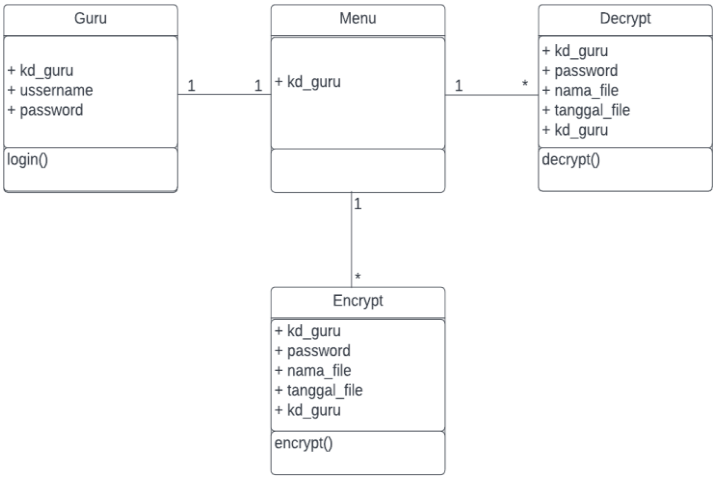
e. Deployment
Deployment yaitu tahap sistem siap digunakan oleh pengguna. Kemudian untuk menjaga agar sistem tetap berjalan dengan baik, maka perlu dilakukan perawatan berkala sesuai kebutuhan.

2.4 Rancangan Basis Data

a. Class Diagram
Pada gambar dibawah ini merupakan gambaran class diagram kepala sekolah.

Gambar 2. Class Diagram Kepala Sekolah

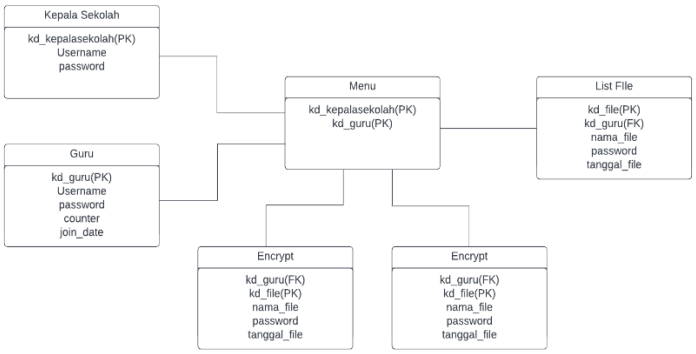
Pada gambar tersebut terdapat *field* kepala sekolah yang berisikan *kd_kepalasekolah*, *username*, dan *password*. Terdapat *field* Menu yang berisikan kd_kepalasekolah. Selanjutnya terdapat *field* List File yang berisikan *nama_file, password, tanggal_size*.
Pada gambar dibawah ini merupakan gambaran class diagram guru.



Gambar 2.4 Class Diagram Guru

Pada gambar class digram diatas , terdapat *field* Guru yang berisikan, yaitu *kd_guru* , *username*, *password.* Lalu ada field Menu yang berisikan, *kd_guru.* Lalu terdapat *Encrypt* dan *Decrypt* yang berisi hampir sama, yaitu kd_file, *password*, nama_*file*, tanggal_*file*, dan kd_*guru*.

b. *Logical Record Structur* (LRS)
Pada gambar dibawah ini merupakan gambaran LRS program ini.



Gambar 2.4e

Pada gambar diatas tabel Kepala sekolah yang berisi kd_kepalasekolah sebagai *primary key*, *username*, dan *password.* Tabel Guru yang berisi kd_*guru* sebagai *primary key*, *username*, dan *password*. Tabel Menu yang mempunyai kd_kepalasekolah sebagai *primary key*, dan kd_*guru* sebagai *primary key*. Tabel *List File* mempunyai kd_file sebagai *primary key*, nama_file, *password*, tanggal_file, dan kd_guru sebagai *foreign key*. Tabel *Encrypt* dan *Decrypt* mempunyai isi yang sama , yaitu kd_*user* sebagai *foreign key*, kd_file sebagai *primary key*, *password*, dan tanggal_file.

2.5 Spesifikasi Basis Data

Dalam pembuatan aplikasi, terdapat juga rancangan basis data yang digunakan. Berikut spesifikasi basis data pada aplikasi ini :

Tabel 1. Kepala Sekolah

Nama	Jenis Data	Keterangan
Kd_kepalasekolah	varchar (15)	Kode kepalasekolah
Username	varchar (50)	Username kepalasekolah
Password	varchar (50)	Password kepalasekolah

Tabel 2. 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_Guru	Int(5)	Kode User

Tabel 3. Guru

Nama	Jenis Data	Keterangan
Kd_Guru	int (5)	Kode Guru
Username	Varchar(30)	Username
Password	Varchar(20)	Password
Tanggal_file	timestamp	Penanda
Join_Date	Timestamp	Tanggal Bergabung

Terdapat 3 tabel diantaranya Tabel 1 Kepala Sekolah yang mempunyai field kd_kepalasekolah dengan jenis data varchar, username dengan jenis data varchar, dan password dengan jenis data varchar. Lalu pada tabel 2 Tabel File ini mempunyai kd_file dengan jenis data int, nama_file dengan jenis data text, password dengan jenis data varchar, tanggal_file dengan jenis data timestamp, dan kd_u\guru dengan jenis data int. Dan pada tabel terakhir yaitu 3 Tabel Login mempunyai isi field kd_guru dengan jenis data int, username dengan jenis data varchar, password dengan jenis data varchar, counter dengan jenis data char, dan join_date dengan jenis data timesamp.

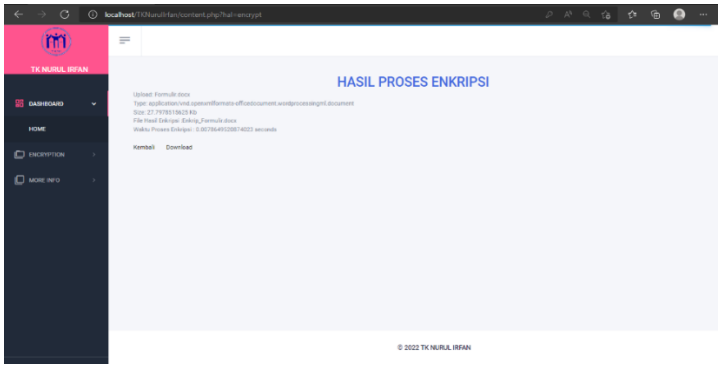
3. HASIL DAN PEMBAHASAN

Pada tahap ini akan berisikan hasil implementasi dari topik penelitian yang di bahas. Beserta penjelasan yang merupakan gambar, tabel,serta penjelasannya.

3.1 Implementasi Rivest Code 4 (RC4)

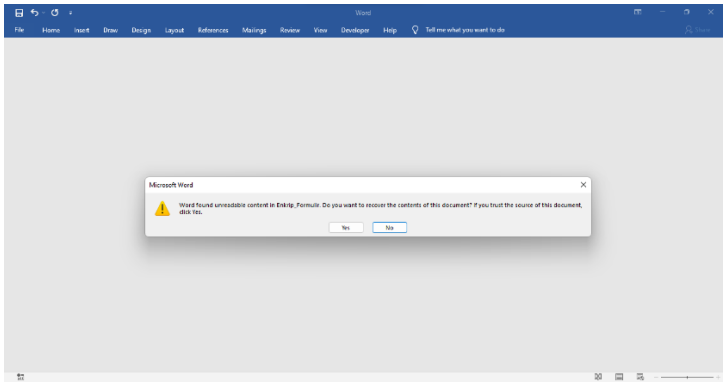
Berdasarkan penerapan metode yang diusulkan di bab sebelumnya maka berikut adalah hasil implementasi pada web yang dibuat.

a. Implementasi Encrypt



Gambar 5. Implementasi Encrypt

Pada bagian encrypt file ini terlihat telah berhasil untuk mengaman kan file tersbut dengan file yang berukuran 27.7978515625 Kb atau 277978515,625 Mb, serta memiliki waktu untuk melakukan proses encrypt file tersebut adalah 0.0078649520874023 seconds.



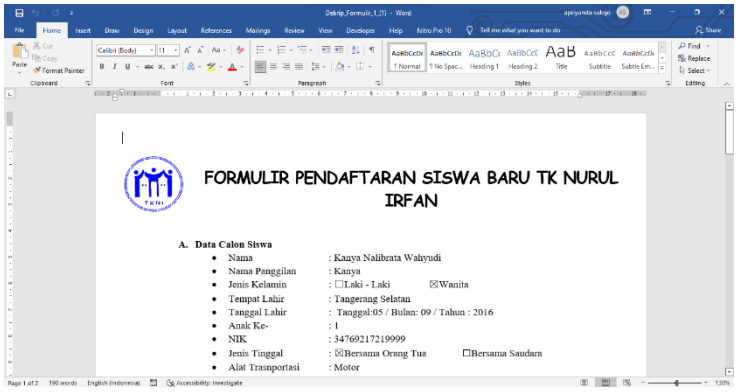
Gambar 6. Hasil File Encrypt

Pada gambar diatasmerupakan hasil file yang telah di encrypt, file yang telah di encrypt tidak dapat di buka.

b. Implementasi *Decrypt*

Gambar 7. Implementasi *Decrypt*

Pada bagian Decrypt file ini telah berhasil untuk mengembalikan file yang telah di Encrypt dengan file yang berukuran 27.7978515625 Kb dan memiliki waktu proses untuk melakukan Decrypt yaitu 0.011245965957642 seconds.



Gambar 8. Hasil File Decrypt

Pada gambar diatas merupakan file yang telah di decrypt sehingga file tersebut dapat dibuka, serta tidak ada perubahan.

Berikut adalah hasil dari implementasi Rivest Code 4 Berdasarkan bab sebelumnya tentang penerapan Rivest Code 4 yang akan dijabarkan melalui tabel berikut.

Tabel 4. Implementasi Encrypt Rivest Code 4

Percobaan	Upload	Size (KB)	Hasil Encrypt	Waktu Proses
1	Formulir 1.docx	28.302734375	Enkrip_Formulir_1.docx	0.011664152145386/s
2	foto 3 x 4 kanya.jpg	323.33203125	Enkrip_foto_3_x_4_kanya.jpg	0.070194959640503/s
3	foto 3 x 4 brillant.jpg	348.05078125	Enkrip_foto_3_x_4_brillant.jpg	0.072494029998779/s
4	Akte Kanya.jpg	1018.0224609375	Enkrip_Akte_Kanya.jpg	0.19817614555359/s
5	Akte Brillant.jpg	774.7666015625	Enkrip_Akte_Brillant.jpg	0.15137505531311/s

Tabel 5. Implementasi Decrypt Rivest Code 4

Percobaan	Upload	Size (KB)	Hasil Encrypt	Waktu Proses
1	Enkrip_Formulir_1.docx	28.302734375	Dekrip_Formulir_1.docx	0.0098159313201904/s
2	Enkrip_foto_3_x_4_kanya.jpg	323.33203125	Dekrip_foto_3_x_4_kanya.jpg	0.078453063964844/s
3	Enkrip_foto_3_x_4_brillant.jpg	348.05078125	Dekrip_foto_3_x_4_brillant.jpg	0.073812961578369/s
4	Enkrip_Akte_Kanya.jpg	1018.0224609375	Dekrip_Akte_Kanya.jpg	0.20158100128174/s
5	Enkrip_Akte_Brillant.jpg	774.7666015625	Dekripsi Dekrip_Akte_Brillant.jpg	0.16773080825806/s

4. KESIMPULAN

Setelah melakukan proses perancangan dan pembuatan website serta berdasarkan permasalahan yang telah disebutkan pada bab sebelumnya maka dapat disimpulkan sebagai berikut:

a. Dengan membuat website dengan pengamanan menggunakan metode RC4 (*Rivest Code 4*) dapat mengamankan dokumen dan dapat mengembalikan dokumen seperti semula.
b. Dengan adanya RC4 (Rivest Code 4) yang berbasis website dapat mengamnkan file – file pendaftaran yang penting, dan file lebih terjaga karena hanya yang mengetahui passwordnya saja yang dapat membuka file tersebut.
c. Dengan Website yang dibuat pada penelitian ini dapat dijadikan salah satu contoh untuk mengamankan sebuah file.

DAFTAR PUSTAKA

[1] J. M. G. J. A. T. I. G. Dedy Ronald Saregi, "Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4," *Jurnal Sistem Komputer Dan Informatika (JSON)*, vol. 1, no.2, pp. 114-119, 2020.

[2] D. Irwansyah, "Pengamanan Data Teks Dengan Algoritma Modifikasi RC4," *Jurnal Pelita Informatika*, vol. 6, no.3, pp. 309-312, 2018.

[3] K. Kirman, "Implementasi Algoritma Rc4 Untuk Proteksi File Mp3," *Pseudocode*, vol. 5, no. 1, pp. 80-86, 2018.

[4] H. J. Muhammad Syahril, "Aplikasi Steganografi Pengamanan Data Nasabah Di Standard Chartered Bank Menggunakan Metode Least Significant Bit Dan RC4," *Seminar Nasional Sains & Teknologi Informasi (SENSASI)*, pp. 505-509, 2019.

[5] 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.

[6] Rista and A. S. Sitio, "Implementasi Keamanan Data Keuangan SMK Swasta Musda Perbaungan Menggunakan Metode RC4," *JIKOMSI: Jurnal Ilmu Komputer Dan Sistem Informasi*, vol.3, no.3, pp. 60-66, 2020.

[7] 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. 788-789, 2018.

[8] A. Setiawan and T. Fatimah, "Implementasi Algoritma Kriptografi untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web Pada PT. Trans Intra Asia," *SKANIKA*, vol. 4, no. 1, pp. 66-71, 2021.

[9] W. Pramusinto, N. Wizaksono and A. Saputro, "Aplikasi Pengamanan File Berbasis Web Dengan Metode Kriptografi AES 192, RC4 dan Metode Kompresi Huffman," *Jurnal BIT*, vol. 16, no. 2, pp. 47-53, 2019.

[10] W. E. Winanto and M. Mufti, "Aplikasi Keamanan Email Data Produksi PT Kunyun Gravure Industries Indonesia Dengan RC4 Dan Base64," *SKANIKA*, vol. 1, no. 1, pp. 303-308, 2018.