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

PENERAPAN ALGORITMA RC4 UNTUK PENGAMANAN DOKUMEN PADA PT. LINARD POWER KONTRAKTOR

Mohamad Shabri Syukur[1*], Mardi Hardjianto[2]

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

Email: [1*]1711501021@student.budiluhur.ac.id, [2]mardi.hardjianto@budiluhur.ac.id
(: corresponding author)*

Abstrak- Kriptografi RC4 merupakan salah satu algoritma enkripsi simetris yang telah banyak digunakan dalam berbagai aplikasi komunikasi dan keamanan data pada suatu perusahaan. Sebagai perusahaan yang bergerak dibidang konstruksi, PT. LINARD POWER KONTRAKTOR mempunyai masalah lokal mengenai dokumen keuangan rencana anggaran biaya. Dalam konteks perusahaan, penggunaan kriptografi RC4 pada PT. LINARD POWER KONTRAKTOR dapat memiliki berbagai implikasi dan manfaat dalam melindungi informasi sensitif seperti dokumen keuangan perusahaan dari akses yang tidak sah. RC4 (Rivest Cipher 4) menggunakan kunci yang sama untuk enkripsi dan dekripsi, yang dikenal sebagai enkripsi simetris. Fungsi utama RC4 dalam perusahaan adalah untuk mengamankan komunikasi dan transmisi data. Algoritma RC4 memungkinkan penggunaan kunci rahasia yang dapat digunakan untuk enkripsi dan dekripsi data yang dikirimkan melalui jaringan komputer. Dengan menerapkan RC4, perusahaan PT. LINARD POWER KONTRAKTOR dapat memastikan bahwa data yang dikirimkan antara perangkat mereka terlindungi dan tidak dapat diakses oleh pihak yang tidak berwenang. Penelitian ini akan diwujudkan dalam bentuk aplikasi berbasis web yang dapat dengan mudah melindungi data pada PT. LINARD POWER KONTRAKTOR. Berdasarkan penelitian dan pengujian program, aplikasi ini berhasil mengatasi kebocoran, pencurian dan perubahan dokumen penting pada perusahaan dengan memanfaatkan enkripsi dan dekripsi metode RC 4.

Kata Kunci: Enkripsi, Dekripsi, RC4, Kriptografi.

APPLICATION OF THE RC4 ALGORITHM FOR DOCUMENT SECURITY AT PT. LINARD POWER KONTRAKTOR

Abstract- *RC4 cryptography is a symmetric encryption algorithm that has been widely used in various communication and data security applications in a company. As a company engaged in construction, PT. LINARD POWER KONTRAKTOR has local problems regarding the budget plan financial document. In the corporate context, the use of RC4 cryptography at PT. LINARD POWER KONTRAKTOR can have various implications and benefits in protecting sensitive information such as company financial documents from unauthorized access. RC4 (Rivest Cipher 4) uses the same key for encryption and decryption, which is known as symmetric encryption. The main function of RC4 within the enterprise is to secure communication and data transmission. The RC4 algorithm allows the use of a secret key that can be used for encryption and decryption of data sent over a computer network. By implementing RC4, PT. LINARD POWER KONTRAKTOR can ensure that the data transmitted between their devices is protected and cannot be accessed by unauthorized parties. This research will be realized in the form of a web-based application that can easily protect data at PT. LINARD POWER KONTRAKTOR. Based on research and program testing, this application has succeeded in overcoming leaks, theft and alteration of important company documents by utilizing the RC 4 encryption and decryption method.*

***Keywords**: Encryption, Decryption, RC4, Cryptography.*

1. PENDAHULUAN

Perkembangan teknologi memungkinkan setiap orang dapat dengan cepat mengakses informasi apapun, sehingga data dan informasi dapat disediakan oleh siapa saja, sehingga banyak orang yang tidak bertanggung jawab mengubah data, mencuri, membajak dan melakukan beberapa hal buruk pada PT. LINARD POWER KONTRAKTOR. Keselamatan adalah keadaan di mana tidak ada bahaya. Istilah ini dapat digunakan sehubungan dengan kejahatan, semua jenis kecelakaan, dan lainnya. Keamanan informasi merupakan topik yang luas, termasuk keamanan komputer dari serangan hacking atau cracking [1]. Masalah keamanan adalah bagian penting dari sistem informasi. Salah satu hal terpenting dalam komunikasi komputer dan jaringan komputer untuk menjamin keamanan pesan, data atau informasi apapun adalah enkripsi [2].

PT. LINARD POWER KONTRAKTOR adalah perusahaan yang memiliki informasi penting yang berbahaya jika informasi tersebut diakses dan dapat diketahui isinya. Saat ini PT LINARD POWER KONTRAKTOR masih menggunakan Microsoft Excel untuk mengolah data yang kemudian disimpan di memori yaitu di harddisk atau media penyimpanan lainnya. Menyimpan data pada hard drive menyebabkan masalah, misalnya jika orang yang tidak berwenang mengubah data. PT. LINARD POWER KONTRAKTOR belum memiliki data keamanan untuk memastikan data. Kebutuhan akan keamanan data merupakan kebutuhan yang penting bagi perusahaan, terutama untuk mengamankan aset-aset yang menjadi tanggung jawab perusahaan. [3]

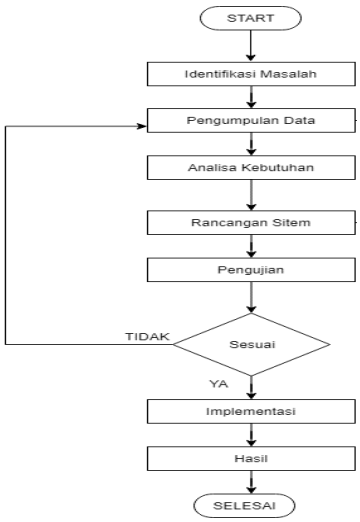
Kriptografi adalah ilmu yang mempelajari teknik matematika yang berkaitan dengan keamanan informasi. Enkripsi juga merupakan bagian dari keamanan informasi, yaitu kerahasiaan adalah layanan yang dirancang untuk melindungi konten informasi dari semua kecuali mereka yang memiliki izin atau kunci rahasia untuk membuka/mengekstraksi informasi yang dienkripsi [4]. Tujuan utama dari kriptografi adalah kerahasiaan (*confidentiality),* autentikasi (*authentication),* integritas data (*data integrity)* dan tidak ada penyangkalan (*non repudiation)* [5]. Ilmu ini terdiri dari mekanisme desain berdasarkan algoritma matematika yang menyediakan satu set keamanan informasi mendasar [6]. Enkripsi secara umum adalah teknik perlindungan data yang mengubah suatu pesan yang akan dirahasiakan menjadi pesan rahasia yang disebut *ciphertext.* Proses enkripsi dan dekripsi membutuhkan kode yang disebut kunci dalam pelaksanaannya. Kunci tersebut harus dirahasiakan dan tidak boleh diketahui oleh orang lain yang tidak berhak menerima pesan tersebut. [7]

Metode enkripsi yang digunakan dalam penelitian ini adalah algoritma *RC4*. Berdasarkan penelitian sebelumnya yang dilakukan oleh [8] diketahui bahwa, metode RC 4 merupakan algoritma enkripsi populer yang memproses data hingga sepuluh kali lebih cepat dari *DES. RC4* adalah salah satu algoritma kunci simetris berupa enkripsi aliran yang memproses unit atau input data dalam satu waktu. Unit atau data biasanya berupa *byte,* atau terkadang *bit,* dan dapat memiliki panjang variabel untuk enkripsi atau dekripsi. Ronald Rivest menemukan algoritma ini pada tahun 1987 dan menjadi keamanan *RSA. RC4* adalah enkripsi aliran simetris yang dikembangkan oleh *RSA Data Security Inc*. (RSADSI). Penyebaran dimulai dengan kode sumber diyakini *RC4* dirilis "anonim" pada tahun 1994 [9]. Sejauh ini, kode *RC4* hanya dapat dipecahkan menggunakan pencarian kunci lengkap atau pencarian *brute force,* teknik dasar yang digunakan oleh *cryptanalysts* untuk mencoba semua kunci yang mungkin sampai kunci yang benar ditemukan. [10]

Dari permasalahan di atas dapat disimpulkan bahwa sistem keamanan data diperlukan untuk melindungi data atau pesan dari orang yang tidak berwenang, menangkap bacaan dan mencegah data yang tidak sah dimasukkan, dihapus atau diubah. Salah satu tindakan pencegahan yang dapat dilakukan adalah dengan membuat suatu aplikasi kriptografi berbasis web dengan metode RC 4, agar dokumen pada PT. LINARD POWER KONTRAKTOR menjadi aman dari pihak yang tidak memiliki kepentingan.

2. METODE PENELITIAN

Melakukan penelitian dengan berpedoman pada metode penelitian agar hasil penelitian tidak menyimpang dari sasaran, sehingga mencapai hasil yang lebih baik. Dengan demikian seperti terlihat pada Gambar 1 menggambarkan metodologi penelitian yang dilakukan yaitu analisis kebutuhan, desain sistem, pengujian, implementasi dan hasil.



Gambar 1 Metode Penelitian

2.1 Pengumpulan Data

Pada tahap ini pengumpulan data dilakukan melalui studi literatur, diskusi dan wawancara.

a. Studi Literatur
   Dilakukan dengan membaca, mempelajari buku dan artikel terkait keamanan, kriptografi, aplikasi RC4 yang mendukung topik yang sedang dibahas.
b. Wawancara
   Melakukan wawancara dengan pihak-pihak terkait untuk mengetahui permasalahan yang ada, sehingga dapat dirumuskan suatu sistem yang dapat mengatasi permasalahan tersebut.
c. Studi Dokumentasi
   Studi dokumentasi bertujuan untuk memahami bentuk doku-mentasi yang digunakan oleh PT. LINARD POWER KONTRAKTOR. Karena dokumentasi yang digunakan mempengaruhi perancangan sistem..

2.2 Rancangan Penguji

Rancangan pengujian yang diimplementasikan akan menggunakan algoritma enkripsi Rivest Cipher 4 (RC4) untuk setiap format yang terdapat pada aplikasi berbasis web yang akan dirancang. Tujuan dari pengujian ini adalah untuk mengetahui apakah data yang diuji akan dienkripsi dengan benar dalam database. Untuk memeriksa apakah file terenkripsi dengan benar, dapat dilakukan dengan mencoba membuka file terenkripsi. Jika file terenkripsi tidak dapat dibuka, berarti file berhasil dienkripsi.

2.3 Rancangan Basis Data

Berikut adalah struktur database yang akan digunakan untuk merancang aplikasi enkripsi RC4. Struktur tabel lihat Tabel 1 dan Tabel 2.

Tabel 1 Spesifikasi Database Login

NO	Nama_Field	Type	Lebar	Keterangan
1	Id	Int	11	Kode *User*
2	*Username*	Varchar	255	Nama *User*
3	*Password*	Varchar	255	*Password User*

Tabel 2 Spesifikasi Database File

NO	Nama_Field	Type	Lebar	Keterangan
1	kode_*file*	Int	11	Kode *file*
2	Nama_*file*	Varchar	255	Nama *file* yang telah di upload
3	*Password*	Varchar	255	*Password file*
4	tanggal	*timestamp*	-	Tanggal dan waktu upload *file*
5	*Size*	*Float*	-	Ukuran *file* yang di upload

3. HASIL DAN PEMBAHASAN

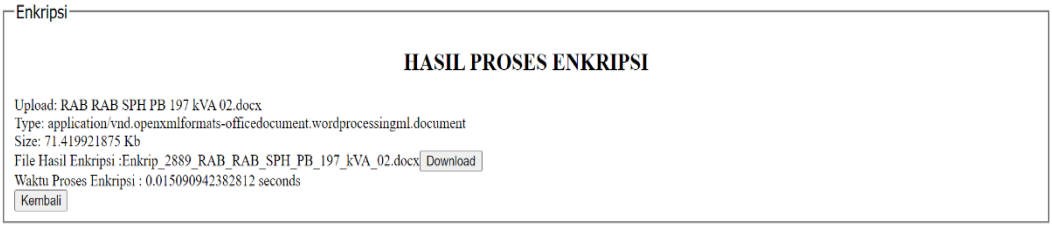
3.1 Implementasi Metode *Rivest Code 4* (RC4)

a. Enkripsi

Algoritme 1 Algoritme Enkripsi RC4

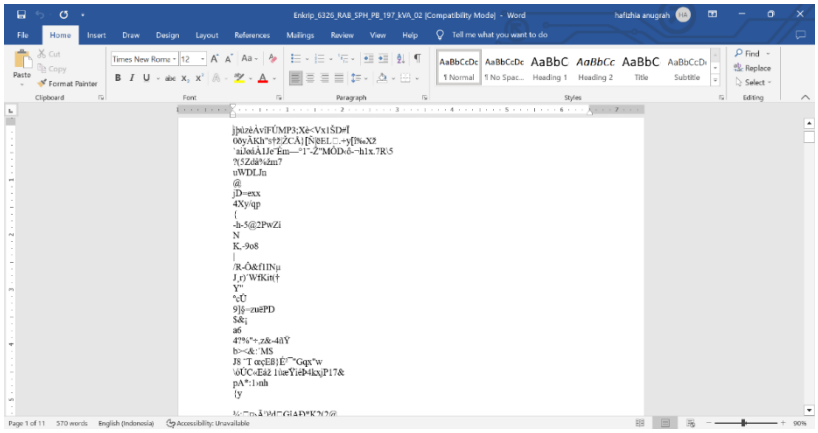
```
1.  Plaintext
2.  Inisialisai kunci
3.  Inisialisasi sBox array
4.  Inisialisasi kBox array
5.  Proses pengacakan sBox dengan Panjang kunci
6.  s = [];
7.  for (i=0; i<256; i++)
8.  s[i] = $i;
9.  Proses swapping sBox [i] dengan sBox [j]
10. j=0;
11. for (i=0; i<256; i++) {
12. j = (j + s[i] + key ( i mod  Panjang kunci) mod  256;
13. Swap array i dengan j
14. s[i] = s[j];
15. s[j] = j;
16. }
17. Proses Pseudo Random
18. i=0;
19. j=0;
20. for (idx=0; idx<strlen(pt); idx++) {
21. i = (i + 1) % 256;
22. j = (j + s[i]) % 256;
23. s[i] = s[j];
24. t= (s[i] + s[j]) % 256;
25. k = s[t];
26. Hasil = chr(ord(substr(pt, idx, 1)) XOR k);
27. Hasil berupa ciphertext
```

Pada algoritme 1, merupakan algoritme enkripsi metode *Rivest Cipher 4* (RC 4) dalam melakukan pengamanan data.



Gambar 2 Hasil Proses Enkripsi

Pada Gambar 2, menunjukkan hasil proses enkripsi untuk pengamanan *file* yang berukuran 71.41992 Kb, serta waktu proses enkripsi *file* tersebut adalah 0.01509 detik.



Gambar 3 Hasil Enkripsi

Pada Gambar 3, terlihat apabila *file* hasil enkripsi bisa dibuka akan berubah menjadi karakter atau huruf-huruf acak.

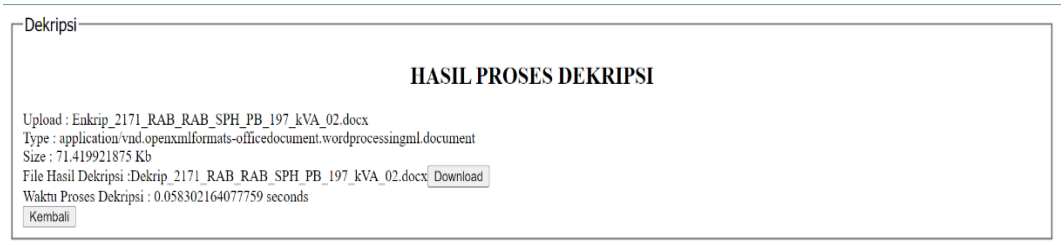
b. Dekripsi

Algoritme 2 Algoritme Proses Dekripsi

```
1.  Inisialisai kunci
2.  Inisialisasi sBox array
3.  Inisialisasi kBox array
4.  Proses pengacakan sBox dengan Panjang kunci
5.      s = [];
6.    for (i=0; i<256; i++)
7.    s[i] = $i;
8.  Proses swapping sBox [i] dengan sBox [j]
9.     j=0;
10.   for (i=0; i<256; i++) {
11.     j = (j + s[i] + key (i mod  Panjang kunci) mod 256;
12.     Swap array i dengan j
13.     s[i] = s[j];
14.     s[j] = j;
15.   }
16. Proses Pseudo Random
17.    i=0;
18.   j=0;
19.   for (idx=0; idx<strlen(pt); idx++) {
```

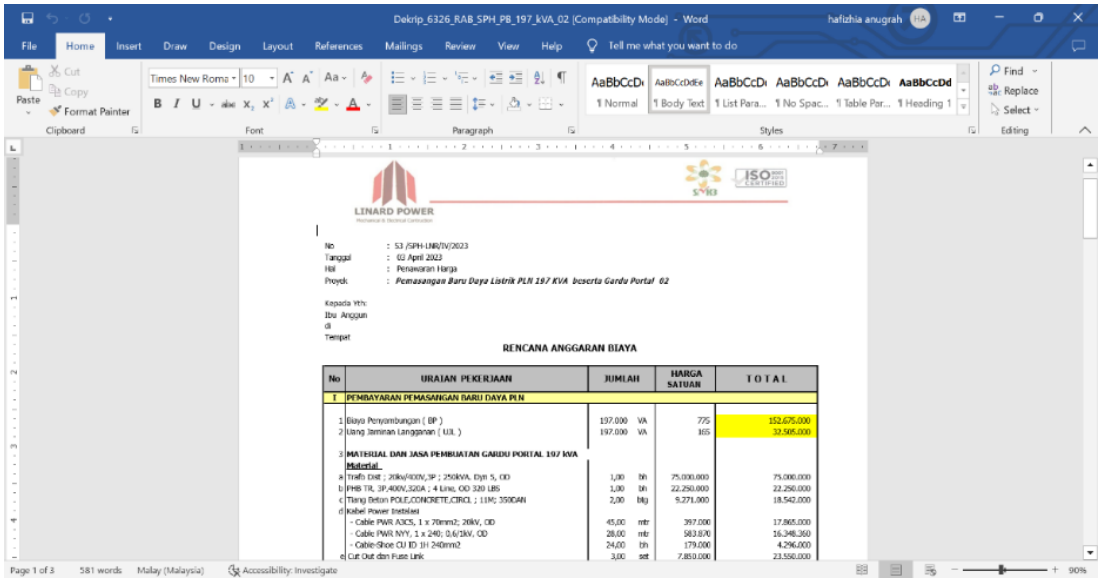
```
20.      i = (i + 1) % 256;
21.      j = (j + s[i]) % 256;
22.      s[i] = s[j];
23.      t= (s[i] + s[j]) % 256;
24.      k = s[t];
25.  Hasil = chr(ord(substr(ct, idx, 1)) XOR k);
26.  Hasil berupa plaintext
```

Algoritme 2 merupakan proses dekripsi dengan metode *Rivest Cipher 4 (*RC 4), yaitu proses mengembalikan *ciphertext* menjadi *plaintext* kembali.



Gambar 4 Hasil Proses Dekripsi

Pada Gambar 4 bagian dekripsi *file*, terlihat hasil proses dekripsi untuk mengembalikan *file* yang telah di enkripsi dengan ukuran *file* sebesar 71.42992 Kb, serta memerlukan waktu 0.05830 *detik*.



Gambar 5 Hasil Dekripsi

Pada Gambar 5, terlihat hasil dari proses dekripsi sehingga *file* akan kembali seperti semula.

3.2 Pengujian

Pada bagian ini merupakan tahap uji enkripsi dan dekripsi *file*, pengujian tersebut nantinya akan mendapatkan hasil perbandingan *file* asli dengan *file* hasil enkripsi.

a) Pengujian *Website*

Pada tahap ini, dilakukan pengujian langsung apakah setiap fungsi dapat berjalan dengan baik. Berikut adalah tabel pengujian *Website* pada Tabel 3.

Tabel 3 Pengujian *Website*

No	Pengujian	Hasil	Kesimpulan
1	Menampilan Halaman *Login*	Dapat memasuki halaman utama	Berhasil
2	*Button "reset"* pada halaman *login*	Dapat menghapus *username* dan *password*	Berhasil
3	Enkripsi	Dapat mengamankan *file*	Berhasil
4	Dekripsi	Dapat mengembalikan *file* hasil enkripsi	Berhasil
5	*Button "Log out"*	Keluar dari *website*	Berhasil

b) Pengujian Enkripsi

Pada tahap ini, terlihat hasil pengujian enkripsi pada beberapa *file* yang dapat dilihat pada Tabel 4.

Tabel 4 Hasil Enkripsi

File	*Password*	*Size*	*Output*	Waktu Proses
RAB SPH PB 197 kVA 02 REV.xlsx	11223344	24 KB	Enkrip_1976_RAB_SPH_PB_197_kVA_02_REV.xlsx	0.049498
27. SPH PT. SUN BRIGHT LESTARI.pdf	11223344	1.638 KB	Enkrip_5167_27._SPH_PT._SUN_BRIGHT_LESTARI	0.00867
RAB SPH PB 197 kVA 02.docx	11223344	72 KB	Enkrip_6326_RAB_SPH_PB_197_kVA_02.docx	0.01753

c) Pengujian Dekripsi

Pada tahap ini, dilakukan pengujian dekripsi kepada *file* yang sebelumnya sudah di enkripsi. Hasil dekripsi dapat dilihat pada Tabel 5.

Tabel 5 Hasil Dekripsi

File	*Password*	*Size*	*Output*	Waktu Proses
Enkrip_1976_RAB_SPH_PB_197_kVA_02_REV.xlsx	11223344	24 KB	Dekrip_1976_RAB_SPH_PB_197_kVA_02_REV.xlsx	0.020010
Enkrip_5167_27._SPH_PT._SUN_BRIGHT_LESTARI	11223344	1.638 KB	Dekrip_5167_27._SPH_PT._SUN_BRIGHT_LESTARI.pdf	1.195923
Enkrip_6326_RAB_SPH_PB_197_kVA_02.docx	11223344	72 KB	Dekrip_6326_RAB_SPH_PB_197_kVA_02.docx	0.060254

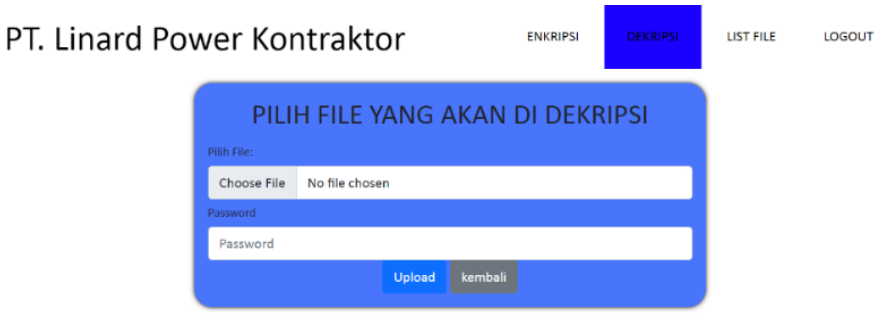
3.3 Tampilan Layar

Bagian ini menjelaskan proses tampilan layar pada aplikasi untuk enkripsi, dekripsi, serta melihat hasil file yang telah dienkripsi dan didekripsi.

a. Tampilan Enkripsi adalah tampilan menu yang digunakan untuk memasukkan *file* yang ingin diamankan lalu memberikan *password.* Tampilan menu enkripsi dapat dilihat pada Gambar 6.

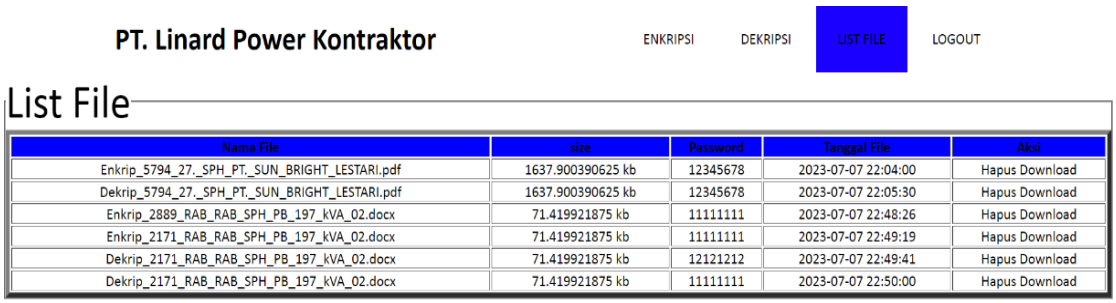
Gambar 6 Tampilan Enkripsi

b. Tampilan Dekripsi adalah tampilan halaman yang digunakan untuk memasukkan *file* yang sudah di enkripsi untuk dilakukan proses dekripsi. Tampilan halaman dapat dilihat pada Gambar 7.



Gambar 7 Tampilan Dekripsi

c. Tampilan *List File* merupakan halaman yang akan menampilkan hasil *file* yang sudah di enkripsi maupuin di dekripsi. Tampilan halaman dapat dilihat pada Gambar 8.



Nama File	size	Password	Tanggal File	Aksi
Enkrip_5794_27._SPH_PT._SUN_BRIGHT_LESTARI.pdf	1637.900390625 kb	12345678	2023-07-07 22:04:00	Hapus Download
Dekrip_5794_27._SPH_PT._SUN_BRIGHT_LESTARI.pdf	1637.900390625 kb	12345678	2023-07-07 22:05:30	Hapus Download
Enkrip_2889_RAB_RAB_SPH_PB_197_kVA_02.docx	71.419921875 kb	11111111	2023-07-07 22:48:26	Hapus Download
Enkrip_2171_RAB_RAB_SPH_PB_197_kVA_02.docx	71.419921875 kb	11111111	2023-07-07 22:49:19	Hapus Download
Dekrip_2171_RAB_RAB_SPH_PB_197_kVA_02.docx	71.419921875 kb	12121212	2023-07-07 22:49:41	Hapus Download
Dekrip_2171_RAB_RAB_SPH_PB_197_kVA_02.docx	71.419921875 kb	11111111	2023-07-07 22:50:00	Hapus Download

Gambar 8 Tampilan *List File*

4. KESIMPULAN

Berdasarkan pembuatan, pengujian, metode dan analisis pemrograman aplikasi ini, dapat ditarik kesimpulan sebagai berikut. Pertama, dengan bantuan aplikasi kriptografi, penyimpanan data dan pertukaran data menjadi lebih aman dan terhindar dari kebocoran, pencurian dan pengubahan data. Kedua, langkah dekripsi mengembalikan file ke keadaan semula tanpa perubahan jika kata sandinya benar. Ketiga, aplikasi enkripsi yang dirancang ramah pengguna sehingga pengguna dapat dengan mudah menyesuaikan dan menggunakan aplikasi ini. Keempat, waktu yang dibutuhkan untuk proses enkripsi dan dekripsi berbanding lurus dengan ukuran file yang sedang diproses. Oleh karena itu, semakin kecil ukuran file yang diproses, semakin cepat proses enkripsi atau dekripsinya. Pada saat yang sama, ukuran file yang lebih besar membuat proses enkripsi dan dekripsi menjadi lebih lama.

DAFTAR PUSTAKA

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

[2] Y. "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan RSA Berbasis Android," *Jurnal Teknik Informatika Kaputama (JTIK),* vol. 3, no. 2, Juli 2019.

[3] N. Taliasih and I. Afrianto, "Sistem Keamanan Basis Data Klien P.T. Infokes Menggunakan Kriptografi Kombinasi RC4 Dan Base64," *Jurnal Nasional Teknologi dan Sistem Informasi,* vol. 06, no. 01, pp. 009-018, 2020.

[4] M. D. Irawan, "Implementasi Kriptografi Vigenere Cipher Dengan PHP," *JURNAL TEKNOLOGI INFORMASI (JurTI),* vol. I, no. 1, 2017.

[5] D. R. Saragi, J. M. Gultom, J. A. Tampubolon and I. Gunawan, "Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4," *Jurnal Sistem Komputer dan Informatika (JSON),* vol. I, no. 2, pp. 114-119, 2020.

[6] V. Siahaan and R. H. Sianipar, Database Dan Kriptografi Menggunakan JAVA/MYSQL, Sparta Publishing, 2019.

[7] M. Diana and T. Zebua, "Optimalisasi Beaufort Cipher Menggunakan Pembangkit Kunci RC4 Dalam Penyandian SMS," *Jurnal Sains Komputer & Informatika (J-SAKTI),* pp. 12-22, 2018.

[8] E. L. Hakim, K. and F. H. Utami, "Aplikasi Enkripsi Dan Dekripsi Data Menggunakan Algoritma RC4 Dengan Menggunakan Bahasa Pemrograman PHP," *Jurnal Media Infotama,* vol. X, no. 1, 2014.

[9] A. Algoritma Rivest Code 6 Rekayasa Perangkat Lunak SMS (Short Message Service), 1st ed., Medan: CV. Sentosa Deli Mandiri, 2020.

[10] R. S. Siregar, M. S. Asih and N. Wulan, "Penerapan Algoritma RC4 Dan RAIL FENCE Untuk Enkripsi," *JITEKH,* vol. 7, no. 2, pp. 51-56, 2019.