P-ISSN:2527-5321
E-ISSN:2527-5941

SISTEM PENGAMANAN FILE MENGGUNAKAN ALGORITMA RC4 BERBASIS WEBBASE STUDI KASUS : PT. TJIPTA JAYA BERSAMA

Sejati Waluyo[1], Denny Victor Kanahebi[2]

[1,2]Universitas Budi Luhur
Jln. Ciledug Raya Petukangan Utara Jakarta Selatan
[1]sejati.waluyo@budiluhur.ac.id, [2]dennykanahebi@gmail.com

ABSTRAK

Perkembangan teknogi informasi yang pesat, menjadi solusi dalam menyelesaikan permasalahan yang dihadapi. Salah satu teknologi yang berkembang dalam masalah keamana adalah kriptografi. Kriptografi adalah proses pensandian data maupun file sehingga data tersebut tidak dapat dibaca oleh orang yang tidak punya kepentingan terhadap data tersebut. PT. Tjipta Jaya Bersama merupakan perusahaan yang bergerak dibidang konsultasi design grafis yang meliputi arsitektur, design interior, lanscape dan enginering. Data dan dokumen yang dimiliki merupakan asset bagi perusahaan yang harus dilindungi kerahasiannya tetap terjaga. Permasalahan yang dihadapi oleh PT. Tjipta Jaya Bersama adalah bagaimana pengamanan dan pengarsipan file dapat dilakukan sehingga data-data penting perusahaan dapat tersimpan dengan baik, namun juga keamanan data tersebut dapat terjaga dengan baik. Oleh sebab itu penulis mengembangan sistem pengamanan file menggunakan algoritma RC4 pada PT. Tjipta Jaya Bersama untuk memudahkan pengarsipan data maupun penyandian data file dokumen untuk menjaga kerahasian file dokumen yang merupakan asset bagi perusahaan.

Kata Kunci: Keamanan File, Kriptografi, Algoritma RC4, Pengarsipan dan Pengaman File Dokumen

ABSTRACT

The rapid development of information technology has become a solution for solving the problems faced. One of the technologies that are developing in security issues is cryptography. Cryptography is the process of encrypting data and files so that the data cannot be read by people who have no interest in the data. PT. Tjipta Jaya Bersama is a company engaged in graphic design consulting which includes architecture, interior design, landscaping, and engineering. Data and documents that are owned are assets for the company that must be kept confidential. The problems faced by PT. Tjipta Jaya Bersama is how to to file security and archiving can be done so that important company data can be stored properly, but also the data security can be properly maintained. Therefore, the authors developed a file security system using the RC4 algorithm at PT. Tjipta Jaya Bersama to facilitate data archiving and document file data encryption to maintain the confidentiality of document files which are assets for the company.

Keyword: File Security, Cryptography, RC4 Algorithm, Archiving, and Document File Security

PENDAHULUAN

Dalam era kemajuan teknologi yang sangat pesat saat ini, banyak merubah pola maupun kebiasaan dalam suatu instansi atau perusahaan dalam menjalankan bisnis mereka. Dalam prakteknya penggunaan dokumentasi penting perusahaan tidak hanya dalam bentuk print out atau berupa cetakan dokumen. Akan tetapi sudah banyak memanfaatkan dokumen digital yang tidak hanya efektif dalam penyimpanan namun juga lebih efektif dalam hal pengarsipan data maupun dokumen penting perusahaan.

PT. Tjipta Jaya Bersama merupakan perusahaan yang bergerak dalam bidang konsultan design grafis yang meliputi arsitektur, design interior, lanscape dan enginering. Serta rancang bangun ruang yang dikelola oleh tenaga ahli dan profesional di bidangnya. Dalam menjalankan bisnisnya sebagai konsultan design grafis PT. Tjipta Jaya Bersama memiliki aset dokumen design dan model-model design yang selalu diupdate sesuai dengan perkembangan jaman sehingga dapat menarik pasar dan dapat menjalankan bisnisnya dengan baik. Dokumen-dokumen tersebut tidak hanya dalam bentuk master atau contoh design yang sudah pernah dibuat sebelumnya akan tetapi juga tersimpan dalam bentuk file dokumen elektronik. Kerena dokumen ini juga merupakan aset bagi perusahaan ataupun PT. Tjipta Jaya Bersama

maka dalam hal penyimpanan data perlu juga di perhatikan keamanan dan kerahasian data tersebut. Agar tidak mudah diambil dan didistribusikan oleh pihak yang tidak bertanggung jawab sehingga dapat merugikan PT. Tjipta Jaya Bersama baik secara material maupun non material karene dokumen yang merupakan asset perusahaan dicuri oleh orang lain. Inilah yang menjadi alasan keamanan penyimpanan file arsip design grafis pada PT. Tjipta Jaya Bersama penting untuk dilakukan.

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Salah satu hal yang penting dalam komunikasi menggunakan komputer dan dalam jaringan komputer untuk menjamin keamanan pesan, data, ataupun informasi adalah enkripsi. Disini enkripsi dapat diartikan sebagai kode atau chipper. Sebuah sistem pengkodean menggunakan suatu tabel atau kamus yang telah didefinisikan untuk kata dari informasi atau yang merupakan bagian dari pesan, data, atau informasi yang dikirim. Sebuah chipper menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (stream) bit dari suatu pesan asli (plainteks) menjadi cryptogram yang tidak dimengerti. Karena sistem chipper merupakan suatu sistem yang telah siap untuk diautomasi, maka teknik ini digunakan dalam sistem keamanan jaringan computer(Sihombing & Ginting, 2020).

Kriptografi merupakan persamaan dari kata "enkripsi" yaitu penyandian dari kata-kata yang dituliskan dan dapat dipahami menjadi kata-kata atau kalimat yang tidak dapat dipahami dan merubahnya dari kalimat yang tidak dapat dipahami menjadi kalimat awal. Kriptografi dibagi menjadi 2, yaitu kriptografi asimetris dan simetris. Kriptografi modern sangat didasari pada teori matematis dan pengaplikasian komputer. Kriptografi itu susah, karena dalam mengenkripsikan sebuah file, kita dahulunya harus mengetahui rumus-rumus terlebih dahulu. Oleh karena itu kriptografi ini sangat aman digunakan untuk merahasiakan dokumen atau file penting. Teknik kriptografi ini sulit untuk diimplementasikan, karna pada kritografi ini menggunakan sebuah penyandian angka dan huruf sehingga orang lain tidak bisa mengkasesnya(Yuliandesi et al., 2020).

Berikut ini adalah algoritma RC4, RC4 mempunyai sebuah S-Box, S0,S1,...,S255, yang berisi permutasi dari bilangan 0 sampai 255, dan permutasi merupakan fungsi dari kunci dengan panjang yang variabel. Terdapat dua indeks yaitu i dan j, yang diinisialisasi dengan bilangan nol. Untuk menghasilkan random byte langkahnya adalah sebagai berikut: (Pandiangan, 2016)

i = (i + 1) mod 256
j = (j + Si) mod 256
swap Si dan Sj
t = (Si + Sj) mod 256
K = St

Byte K di XOR dengan plaintexs untuk menghasilkan cipherteks atau di XOR dengan cipherteks untuk menghasilkan plainteks. Enkripsi sangat cepat kurang lebih 10 kali lebih cepat dari DES. Inisialisasi S-Box juga sangat mudah. Pertama isi secara berurutan S0 = 0, S1 = 1,...,S255 = 255. Kemudian isi array 256 byte lainnya dengan kunci yang diulangi sampai seluruh array K0, K1,...,K255 terisi seluruhnya. Set indeks j dengan nol, Kemudian lakukan langkah berikut :

for i = 0 to 255
j = (j + Si + Ki) mod 256
swap Si dan Sj

METODE PENELITIAN

Metode penelitian menjelaskan desain penelitian, rancangan kegiatan, ruang lingkup atau objek penelitian (populasi dan sampel), tempat penelitian, teknik pengumpulan data, dan teknik analisis penelitian.

Adapun metode penelitian yang digunakan dalam memecahkan permasalahan yang ada adalah sebagai berikut:

1. Metode Pengumpulan Data
   Dalam pengumpulan data yang dilakukan penulis melakukan beberapa hal diantaranya:
   Pertama Studi Literatur, Berdasarkan permasalahan yang dihadapi oleh Tjipta Jaya Bersama yaitu bagaimana penyimpanan data file dokumen dan pengamanan file dilakukan. Penulis perlu melihat referensi yang ada guna memberikan masukan berupa literatur yang berhubungan dengan pengamanan dan penyandian file sehingga sistem yang dibangun dapat menyelesaikan permasalahan yang ada.
   Kedua Tinjauan Lapangan, tinjauan kelapangan ini dilakuan dengan cara :

P-ISSN:2527-5321
E-ISSN:2527-5941

a. Wawancara
Guna mendalami permasalahan yang ada perlu adanya komunikasi dua arah yang harus dilakukan berupa tanya jawab guna mengetahui dan pengembangan sistem. Sehingga output sistem yang dihasilkan dapat menyelesaikan permasalahan yang ada dan tentunya sesuai dengan kebutuhan user.

b. Studi Dokumentasi
Diperlukan juga dalam pengembangan sistem melihat bentuk-bentuk dokumen yang digunakan di Tjipta Jaya Bersama, Karena file yang digunakan akan mempengaruhi design sistem yang digunakan.

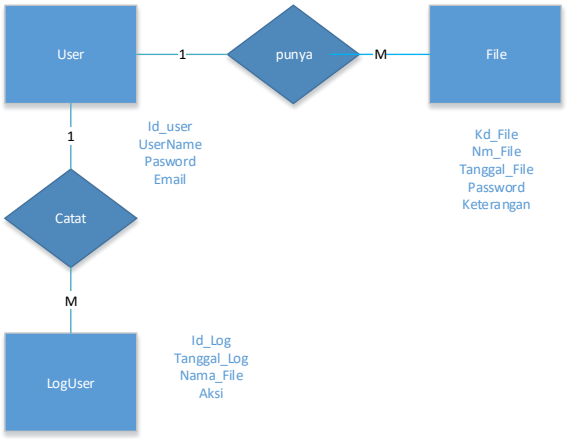
c. Analisa Kebutuhan Sistem
Berdasarkan permasalahan yang dikemukanan sebelumnya yaitu bagaimana pengarsipan dan pengamanan file dokumen dilakukan. Maka, kebutuhan sistem yang diperlukan adalah sebuah sistem yang dapat melakukan penyimpanan dan pengarsipan file serta sistem tersebut dapat melindungi informasi file tersebut dengan melakukan penyandian menggunakan algoritma kriptografi sehingga file yang disimpan di server tetap aman karena dalam keadaan terenkripsi.

d. Perancangan Sistem
Setelah kebutuhan sistem diketahui langkah selanjutnya adalah membuat design sistem yang akan dikembangkan untuk menyelesaikan permasalahan diatas.

e. Pembuatan dan implementasi program
Tahap terakhir yang penulis lakukan setelah mengetahui kebutuhan sistem serta melakukan perancangan sistem adalah pembuatan dan implementasi sistem yang dibuat sebelumnya. Sehingga dapat diketahui apakah sistem berjalan dengan baik atau tidak.

HASIL DAN PEMBAHASAN

Entity Relation Diagram(ERD)

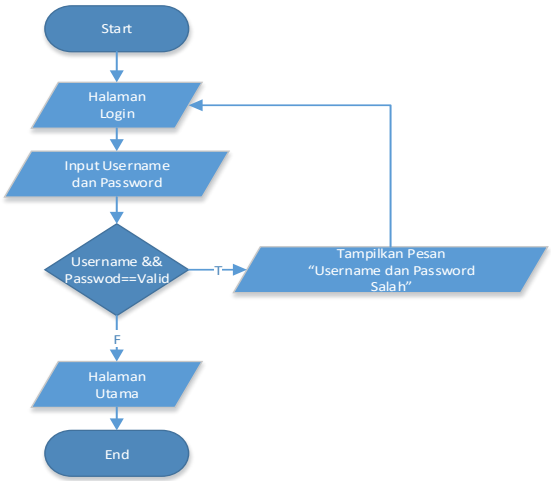


Gambar 1. Entity Relation Diagram (ERD)

Gambar 1. Menujukkan ERD yang merupakan design database digunakan, semua informasi terkait sistem pengamanan file akan di simpan didalam tabel user, file dan loguser yang strukturnya ditunjukkan pada gambar diatas.

Flowchart

a. Login Sistem

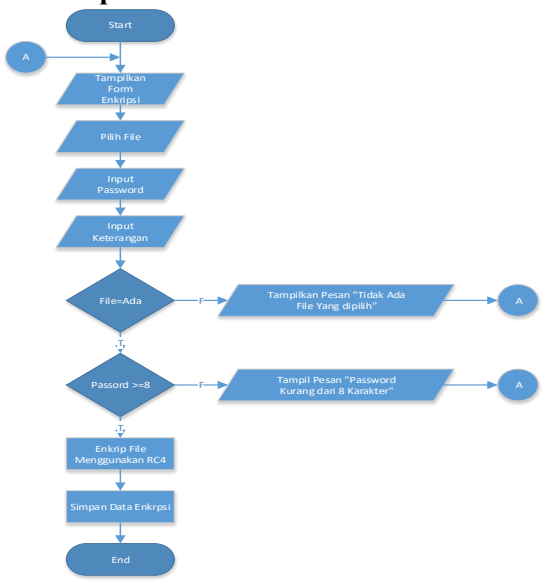


Gambar 2. Flowchart Login Sistem

Gambar 2. Menunjukan proses login ke sistem pengamanan file, dimana user mengakses halaman login serta memasukan user dan password mereka apabila user terdaftar maka sistem akan mengarahkan ke Halaman Utama.

P-ISSN:2527-5321
E-ISSN:2527-5941

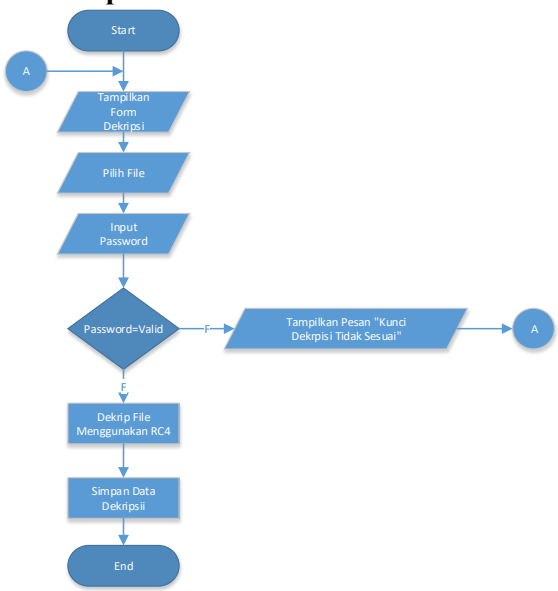
b. Enkripsi File



Gambar 3. Flowchart Enkripsi File

Gambar 3. Menunjukan proses enkripsi file, user memilih menu enkripsi file selanjutnya pilih file yang akan dienkrip, memasukan password enkripsi serta menambahkan keterangan file. Sistem akan mengecek file sudah dipilih apa belum kemudian apakah Panjang password tidak kurang dari 8 digit. Apabila sesuai sistem akan mengenkripsi file menggunakan algoritma RC4 dan menyimpan data serta berkas file enkrip ke server.

c. Dekripsi File

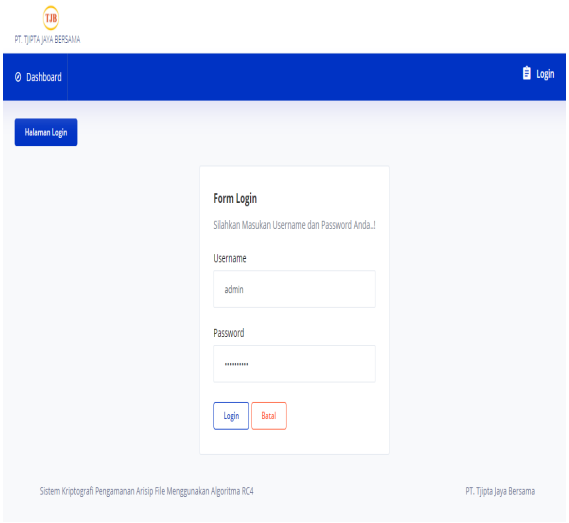


Gambar 4. Flowchart Dekripsi File

Gambar 4. Menunjukkan proses dekripsi file. untuk mendekripsi file, user memilih file yang akan didekrip selanjutnya user akan diminta untuk memasukan kunci dekripsi. Kunci ini adalah kunci yang sama yang digunakan untuk mengenkrip file sebelumnya apabila sesuai kunci yang dimasukan file akan dienkrip serta data dekripsi file akan di simpan kedalam database.

Tampilan Sistem

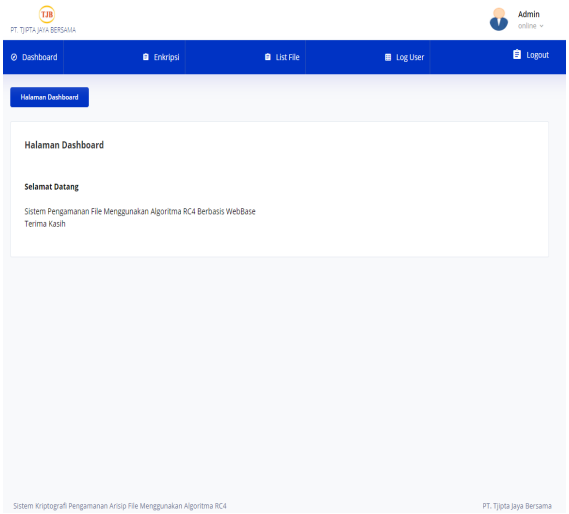
a. Halaman Login



Gambar 5. Halaman Login Sistem

Menu login, digunakan untuk akses kedalam sistem pengamanan file untuk dapat menggunakan fitur yang ada.

b. Halaman Utama

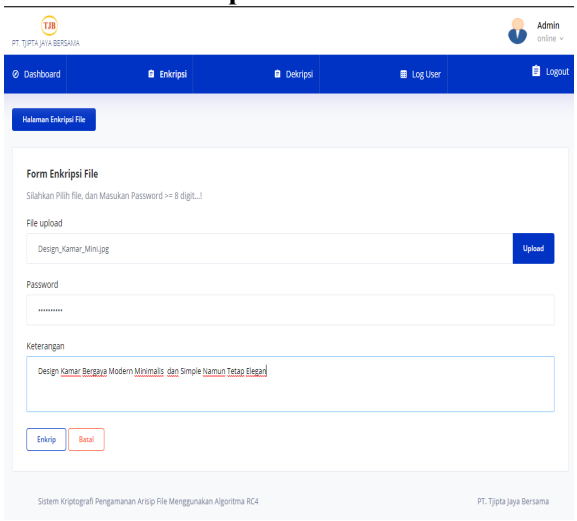


Gambar 6. Halaman Utama

Halaman utama sistem pengamanan file terdiri dari Dashbord, Enkripsi File, List File dan Log user.

P-ISSN:2527-5321
E-ISSN:2527-5941

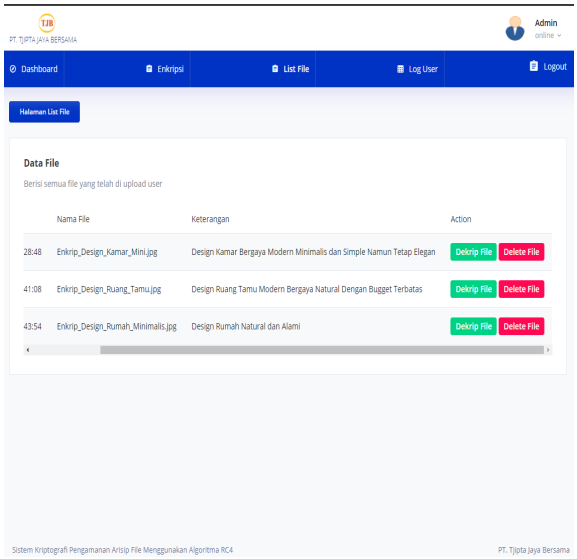
c. Halaman Enkrpisi File



Gambar 7. Halaman Enkripsi File

Halaman Enkripsi file, digunakan untuk mengenkripsi file menggunakan algoritma RC4. Serta juga dilakukan pengarsipan file dan password kunci file yang sudah dienkrip. Sehingga dapat dibuka Kembali atau didekripsi apabila diperlukan, meskipu pemilik file lupa password.

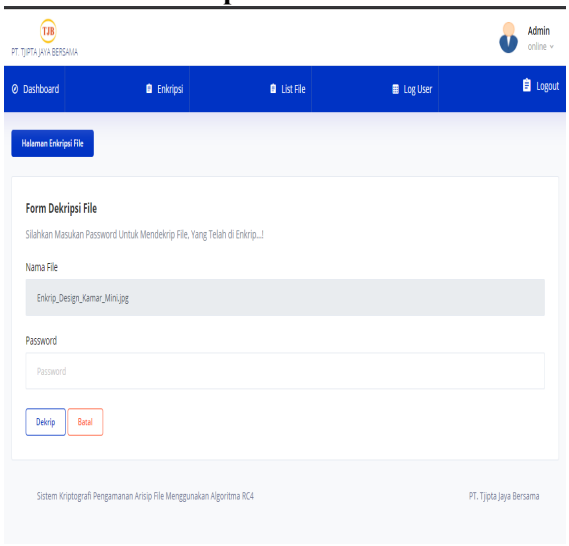
d. Halaman List File



Gambar 8. Halaman List File

Halaman List File, akan menampilkan semua file yang telah dienkrip dan diarsip di server. Di menu ini, dapat dilakukan penghapusan file dan juga dekripsi file.

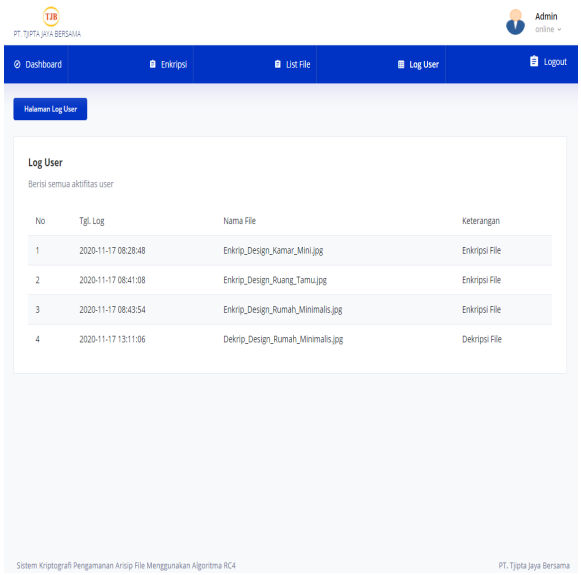
e. Halaman Dekrip File



Gambar 9. Halaman Dekrip File

Halaman dekrip file, digunakan untuk mendekripsi file yang telah dienkrip sebelumnya. Setelah didekrip dengan memasukan kunci yang digunakan untuk mengenkripsi file sebelumnya.

f. Halaman Log File



Gambar 10. Halaman Log File

Halaman log file, akan menampilkan semua aktivitas user. Baik pada saat enkripsi, dekripsi maupun pada saat menghapus file enkripsi.

P-ISSN:2527-5321
E-ISSN:2527-5941

SIMPULAN DAN SARAN

Adapun kesimpulan yang dapat diambil berdasarkan hasil dan pembahasan diatas adalah: Dengan adanya sistem pengamanan file dapat memudahkan dalam hal pengarsipan file dokumen penting pada PT. Tjipta Jaya Bersama dengan tetap memperhatikan keamanan file dengan menerapkan kriptografi menggunakan algoritma RC4. Semua file yang dienkrip akan disimpan dalam server sehingga proses enkripsi ini juga dapat berfungsi sebagai arsip dokumen sehigga memudahkan dalam hal pencarian dokumen apabila dibutuhkan dikemudian hari. Algoritma RC4 termasuk algoritma yang dapat digunakan untuk mengenkripsi semua jenis file. Namun tetap ringan dalam proses enkripsi dan dekripsi file sehingga tidak memberatkan sistem webbase pada saat enkrip maupun dekripsi file dokumen. Setiap enkripsi file dokumen pasword enkripsi file disimpan didalam database sehingga pada saat lupa password dapat menggunakan password yang tersimpan untuk mendekripsi file.

Saran untuk penelitian selanjutnya adalah perlu adanya pengembangan sistem ke arah Mobile Aplikasi mengingat tren saat ini adalah hampir setiap sistem Webbase yang ada selalu ada versi mobilenya. sehingga lebih memberikan kepraktisan dari sisi penggunaan karena semua dapat diakses secara langsung melalui aplikasi yang ada di mobile masing-masing.

DAFTAR PUSTAKA

Pandiangan, H. (2016). Perancangan Media Pengiriman Pesan Teks Dengan Penyandian Pesan Menggunakan Algoritma RC4 Berbasis WEB. *Jurnal Mantik Penusa*, *19*(1).

Sihombing, P., & Ginting, W. (2020). Perancangan dan Implementasi Enkripsi dan Dekripsi File dengan Algoritma RC4–One Time Pad pada Jaringan LAN. *KAKIFIKOM: Kumpulan Artikel Karya Ilmiah Fakultas Ilmu Komputer*, *2*(1), 1–10.

Yuliandesi, A., Sitompul, D. R., AJF, A. P., & Hasan, M. A. (2020). *Implementasi Algoritma Md5 Dan Rc4 Untuk Keamanan Data File*.