

Perancangan Aplikasi Enkripsi & Deskripsi pada Dokumen File Dengan Algoritma Triple DES Berbasis Web

Muklas Adik Putra¹⁾, Dadang Iskandar Mulyana²⁾, Runi Amanda Amalia³⁾, Mirsandi⁴⁾

^{1,2,3,4} Fisikom, Sistem Informasi, Stikom CKI, Jakarta, Indonesia

¹muklas0505@gmail.com, ²mahvin2012@gmail.com, ³runiamanda44@gmail.com,

⁴mirsandiinaz09@gmail.com.



*Penulis Korespondensi

Histori Artikel:

Submit: 2022-01-28

Diterima: 2022-02-11

Dipublikasikan: 2022-02-14

Kata Kunci:

Dokumen, Keamanan, Kriptografi, Triple DES, Web.

Jurnal Pendidikan Sains dan Komputer is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).

ABSTRAK

Keamanan sangat perlu digunakan, karena data bersifat rahasia dan tidak bisa digunakan oleh pihak manapun kecuali pihak yang bersangkutan. Untuk itu, pengguna membutuhkan keamanan data dengan menggunakan kriptografi. Banyak sekali algoritma kriptografi modern yang termasuk ke dalam sistem kriptografi kunci simetri yaitu Triple-DES. Hal ini bertujuan untuk mengetahui perancangan atau desain aplikasi kriptografi pada dokumen berbasis web dengan menggunakan algoritma triple DES. Metode penelitian yang digunakan adalah metode pengumpulan data yang dimana menggunakan bahan jurnal sebagai bahan referensi, rancangan penelitian yang menggunakan gambar untuk menjelaskan bagaimana proses enkripsi dan deskripsi, rancangan aplikasi menggunakan Bahasa pemrograman yaitu PHP. Hasil penelitian menunjukkan adanya keberhasilan dalam mengamankan file dokumen pengarsipan. Dengan system keamanan dokumen berbasis web, dirancang sebuah system yang dapat melakukan proses keamanan data, pencarian, dan pengunduhan yang di proses menggunakan aplikasi berbasis web sehingga bisa dilakukan secara cepat dan efisien, pada akhirnya bisa menghasilkan suatu system keamanan dengan tepat

LATAR BELAKANG

Saat ini perkembangan teknologi informasi sangat pesat, banyak produk-produk canggih diciptakan untuk menangani berbagai masalah bagi para pengguna. Produk ini dipakai untuk membantu pengguna agar lebih mudah menangani permasalahan. Namun ada hal yang harus diperhatikan yaitu keamanan saat penukaran data. Dampak negative dari perkembangan teknologi adalah adanya pencurian data dari pihak yang tidak bertanggung jawab.

Keamanan akan digunakan, karena data bersifat rahasia dan tidak bisa digunakan oleh pihak manapun kecuali pihak yang bersangkutan. Oleh karena itu, pengguna membutuhkan keamanan data dengan menggunakan kriptografi. Pada umumnya kriptografi terdiri dari kriptografi klasik dan kriptografi modern. Kriptografi klasik melakukan enkripsi dan dekripsi karakter per karakter sedangkan kriptografi modern beroperasi pada string biner dan dipicu oleh perkembangan komputer pada saat ini.

Banyak sekali algoritma kriptografi modern yang termasuk ke dalam sistem kriptografi kunci simetri yaitu Triple-DES. Triple DES memiliki algoritma kriptografi yang termasuk ke sistem kriptografi simetri. Manfaatnya yaitu untuk mengamankan pesan tersebut dengan merancang sebuah sistem yang dapat melakukan enkripsi dan dekripsi dengan mudah.

Kriptografi adalah sebuah penyampaian pesan secara tersembunyi. Dan juga untuk menjaga kerahasiaan pesan (data atau informasi) dengan cara menggunakan sandi yang tidak mempunyai makna



dan hanya bisa dimengerti oleh orang yang berhak mengakses informasi. Pesan dirahasiakan disebut plainteks (*plaintext*) dan hasil penyamaran disebut cipherteks (*chiphertext*). Proses dari plainteks ke cipherteks disebut enkripsi (*encryption*) dan proses pembalikan dari cipherteks menjadi plainteks kembali disebut dekripsi (*decryption*) (Rodiyyah, 1994). Kriptografi juga memiliki tujuan yaitu agar informasi yang bersifat rahasia dan yang akan dikirim melalui suatu jaringan, seperti LAN, tidak dapat diketahui dan dimanfaatkan oleh orang lain atau pihak dari luar instansi atau perusahaan lain. (Adhar, 2019). Algoritma adalah sebuah langkah-langkah logis untuk menyelesaikan masalah yang disusun secara sistematis, jadi algoritma kriptografi atau sering disebut dengan cipher merupakan langkah-langkah untuk menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut (Fauzi, 2018).

Algoritma Triple DES (*Triple Data Encryption Standard*) salah satu algoritma simetris pada kriptografi yang digunakan untuk mengamankan data dengan cara menyandikan data. Proses yang digunakan dalam penyandian datanya, yaitu proses enkripsi dan proses dekripsi. Keamanan algoritma Triple DES lebih aman dari algoritma DES, karena mengalami enkripsi tiga kali. Awalnya, kunci sandi Algoritma DES yaitu 56 bit sudah mencukupi pada saat algoritma ini dibuat, namun, dengan meningkatnya kemampuan komputasi serangan brutal telah mungkin terjadi. (Saragih et al., 2019) Algoritma Triple DES mempunyai dua model kunci eksternal, pertama yaitu K1, K2 dan K3 merupakan kunci-kunci yang saling bebas, $K1 \neq K2 \neq K3$. Kedua K1 dan K2 yaitu pola kunci-kunci yang tidak terkait, dan K3 sama dengan K1, $K1 \neq K2$ dan $K3 = K1$. (Rantellingi & Saputra, 2020)

Berdasarkan uraian diatas, maka penulis mengkaji secara mendalam terkait “**Perancangan Aplikasi Enkripsi & Dekripsi Pada Dokumen File Dengan Algoritma Triple DES Berbasis Web**”.

STUDI LITERATUR

Kriptografi.

Kriptografi merupakan perangkat yang sangat penting untuk melindungi keamanan informasi dengan menggunakan kata sandi yang hanya bisa di mengerti oleh orang yang mempunyai hak akses. Kriptografi sebenarnya adalah metode yang di gunakan untuk melindungi data yang prosesnya menyandikan *plainteks* menjadi *chipherteks* disebut enkripsi (*encryption*) dan proses mengembalikan *chipherteks* ke *plainteks* kembali disebut dekripsi (*decryption*). Penggunaan kriptografi di kelompok juga bertujuan menjaga privasi dan keamanan informasi yang di kirim seseorang dalam keadaan jalur komunikasi nya yang sama dengan pihak lain. (Zainuddin & Mulyana, 2016) Dalam penelitian ini, enkripsi yang digunakan pada dokumen dengan mengubahnya menjadi bentuk yang tidak diketahui. Setiap dokumen yang dienkrapsikan memiliki kunci selama proses penyandian. (M. Adi Akbar, Ilhamsyah, 2016) Dapat dipastikan bahwa pembaca bisa menggunakan sebuah algoritma atau sandi untuk transmisi data yang akan menjadi jelas omong kosong. Dan orang lain tidak akan mengetahui algoritma ini, karena data di transmisi tidak bermakna. (Kartika, 2018). Tujuan pengamanan informasi menurut Paryati adalah :

1. Pihak-pihak yang diotorisasi sehingga keutuhan serta konsistensi data pada sistem tetap terjaga ketika diakses.
2. Ketersediaan yaitu menjamin pengguna yang sah untuk selalu dapat mengakses informasi dan sumberdaya yang diotorisasi.
3. Konsistensi dan menjamin data tersebut sesuai dengan aslinya, agar upaya orang lain yang berusaha merubah data akan segera dapat diketahui .

4. Pemakaian yang sah yaitu menjamin kepastian bahwa sumber daya tidak bisa digunakan oleh orang yang tidak berhak.(Febriani et al., 2020)

Menurut Stalling, ada beberapa tuntutan yang terkait dengan isu keamanan data, yaitu(Stallings, 1995):

1. Confidentiality. Menjamin bahwa data-data tersebut hanya bisa diakses oleh pihak-pihak tertentu saja.
2. Authentication. Baik pada saat pengiriman atau penerimaan informasi, kedua belah pihak harus mengetahui bahwa pengirim dari pesan tersebut adalah orang yang benar seperti yang diklaim.
3. Integrity. menjamin setiap pesan yang dikirim pasti akan sampai pada penerimanya tanpa ada bagian dari pesan tersebut yang diganti, diduplikasi, dirusak, diubah urutannya, dan ditambahkan.
4. Nonrepudiation. Pencegahan pengirim maupun penerima meningkari bahwa mereka telah mengirim atau menerima suatu pesan/informasi. Jika pesan dikirim, penerima dapat membenarkan bahwa pesan tersebut memang dikirim oleh pengirim yang tertera. Sebaliknya, jika sebuah pesan diterima, pengirim dapat membuktikan bahwa pesannya telah diterima oleh pihak yang ditujunya.
5. Access Control. Menyaring atau memfilter sumber-sumber data hanya kepada orang-orang tertentu.
6. Availability. Jika diperlukan kapanpun semua informasi pada sistem komputer harus ada bagi semua pihak yang berhak atas informasi tersebut. Dari keenam aspek keamanan data tersebut, empat diantaranya dapat diatasi dengan menggunakan cryptography yaitu confidentiality, integrity, authentication, dan nonrepudiation.(Fauzi, 2018)

Algoritma Kriptografi.

Menurut Ariyus (2006) Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu :

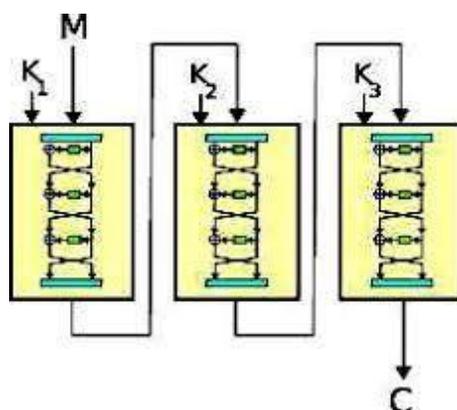
1. Enkripsi, merupakan pengamanan data yang dikirim agar terjaga kerahasiaannya. Pesan asli disebut plainteks diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan sebagai cipher atau kode.
2. Kunci, merupakan kunci yang digunakan untuk proses enkripsi dan deskripsi. Kunci terbagi menjadi dua bagian yaitu kunci rahasia (*private key*) dan kunci umum (*public key*).
3. Deskripsi, kebalikan dari enkripsi. Pesan yang di enkripsi kembali ke bentuk awal. Algoritma yang digunakan berbeda untuk enkripsi. Algoritma Triple DES (*Triple Data Encryption Standard*) adalah algoritma simetris pada kriptografi yang digunakan untuk pengamanan data dengan cara menyandikan data. Proses yang digunakan dalam penyandian datanya, yaitu proses enkripsi dan proses dekripsi. Triple DES lebih aman dari DES, dikarenakan mengalami enkripsi tiga kali. Awalnya ukuran kunci sandi DES yaitu 56 bit sudah cukup pada saat algoritma ini dibuat, namun, dengan meningkatnya kemampuan komputasi serangan brutal telah mungkin terjadi.[4]

Algoritma Triple DES (*Triple Data Encryption Standar*)

Algoritma Triple DES merupakan salah satu algoritma simetris pada kriptografi untuk melindungi data dengan menyandikan data. Prosesnya dilakukan dalam penyandian data yaitu menggunakan proses

enkripsi dan deskripsi. Algoritma Triple DES adalah pengembangan dari salah satu algoritma DES (Data Encryption Standar) yang sudah di enkripsi sebanyak tiga kali. (Rantellinggi & Saputra, 2020) Triple DES menggunakan kunci tiga kunci yang panjangnya 168 bit (tiga kali kunci 56 dari algoritma DES). Algoritma Triple DES mempunyai tiga tahap, setiap tahapnya merupakan implementasi algoritma DES. (Saragih et al., 2019)

- Tahap pertama, plainteks yang diinputkan dioperasikan dengan kunci eksternal pertama (K_1) dan dienkripsi dengan menggunakan algoritma DES
- Tahap kedua, pra-cipherteks pertama yang dihasilkan dari tahap pertama, kemudian dioperasikan dengan menggunakan kunci eksternal kedua (K_2) dan melakukan proses enkripsi atau proses dekripsi (tergantung cara pengenkripsian yang digunakan) dengan menggunakan algoritma DES agar menghasilkan pra-cipherteks kedua.
- Tahap ketiga, pra-cipherteks kedua yang dihasilkan pada tahap kedua, dan dioperasikan dengan menggunakan kunci eksternal ke 3 (K_3) dan melakukan proses enkripsi dengan menggunakan algoritma DES, sehingga menghasilkan cipherteks (C).



Gambar 1.

Pada pemilihan kunci ada dua kunci eksternal dalam Algoritma Triple DES

a. K_1, K_2, K_3 adalah kunci yang bersifat saling bebas

- $K_1 \neq K_2 \neq K_3 \neq K_1$

b. K_1 dan K_2 adalah kunci yang bersifat saling bebas, dan K_3 sama K_1

- $K_1 \neq K_2$ dan $K_3 = K_1$. (Hidayat, 2009)

Proses Enkripsi dan Deskripsi pada Algoritma Triple DES

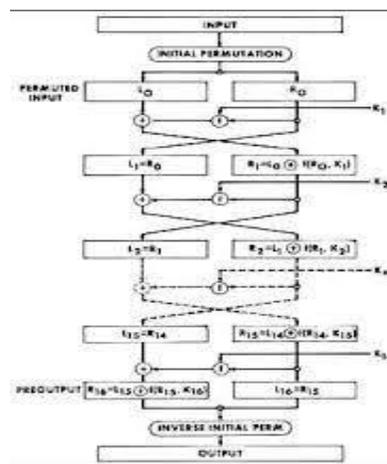
a. Proses Deskripsi

Proses dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal

yang digunakan adalah k_1, k_2, \dots, k_{16} maka pada proses dekripsi urutan kunci internal yang digunakan adalah $k_{16}, k_{15}, \dots, k_1$.

b. Proses Enkripsi Dokumen

Plainteks yang diinputkan pertama akan disubstitusikan dalam matriks permutasi awal atau IP panjangnya 64bit. Kemudian dibagi dua bagian,yaitu kiri (L) dan kanan (R) masing masing 32 bit.



Gambar 2. Proses Enkripsi

Berbasis Web

Aplikasi berbasis web ini menggunakan Bahasa pemrograman PHP, HTML, CSS dan JS. Aplikasi ini membutuhkan web server dan juga menggunakan browser seperti Google chrome, Opera dan lain-lain. Untuk menyambungkan aplikasi web dan perangkat komputer dibutuhkan koneksi internet dan bisa juga intranet. Jenis-jenis aplikasi yang berbasis web yaitu web media social, web berbasis sistem informasi, web e-commerce dan lain-lain.

METODE

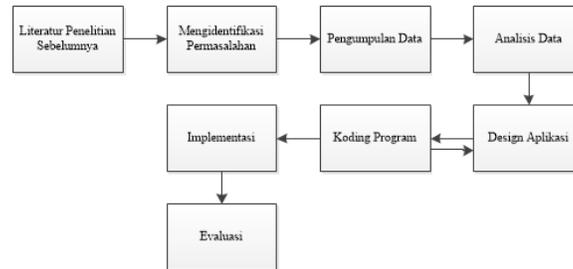
Metode Pengumpulan Data

Metode penelitian menggunakan studi literatur. Studi literatur merupakan studi yang menggunakan bahan sebagai referensi tertulis untuk mengumpulkan data dengan membaca seperti buku, skripsi, jurnal dan berbagai sumber sumber internet manapun yang berkaitan dengan Algoritma Triple DES dan Perancangan Kriptografi .(Satria et al., 2020) Adapun teknik analisa data Miles and Huberman terdapat tahapan- tahapan pengumpulan data, reduksi data, penyajian data dan penarikan kesimpulan atau verifikasi.

Rancangan Penelitian

Dalam penelitian ini penulis menggunakan gambaran berupa diagram dan table. Diagram tersebut

menjelaskan bagaimana proses awal untuk log in, mendeskripsikan dokumen, mengenkripsikan dokumen sampai proses tersebut selesai. Dan untuk tabel menjelaskan bagaimana hasil uji pada aplikasi tersebut.

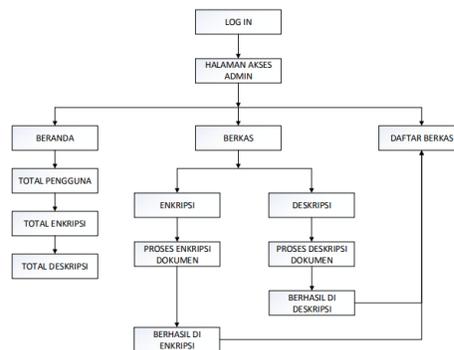


Gambar 1. Tahapan Penelitian

Tahapan penelitian dimulai dari literatur penelitian sebelumnya lalu mengidentifikasi masalah serta mengumpulkan data data dan menganalisis data.Selanjutnya membuat design aplikasi dengan menggunakan koding program berbahasa PHP lalu di implementasikan.Tahapan terakhir yaitu evaluasi koding program tersebut yang sudah di implementasikan.

Rancangan Aplikasi

Penelitian ini penulis merancang sebuah aplikasi proses enkripsi dan deskripsi pada dokumen berbasis web menggunakan Bahasa pemrograman yaitu PHP (Hypertext Preprocessor).



Gambar2. Tampilan rancangan aplikasi

Rancangan aplikasi ini di mulai dari log in sebagai admin kemudian akan tampil beranda dimana terdapat total pengguna, total enkripsi dan total deskripsi. Selanjutnya ada berkas yang akan di proses untuk di enkripsikan dan di deskripsikan. Jika proses berjalan dengan lancar maka akan menghasilkan sebuah dokumen yang sudah di enkripsi dan di deskripsi. File tersebut akan ada di daftar berkas.

HASIL

No	Pengujian	Keterangan
1	Login	Valid
2	Menu Beranda ((total pengguna,total enkripsi,total dekripsi)	Valid
3	Menu Berkas	Valid
4	Menu Enkripsi Dokumen	Valid
5	Menu Deskripsi Dokumen	Valid
6	Menu Daftar Berkas	Valid

Tabel 1.Hasil Uji

Pada pembahasan ini menghasilkan aplikasi kriptografi berbasis web yang dapat melindungi file dokumen dari pihak orang luar dan ingin mengambil data dokumen tersebut untuk di salah gunakan.

PEMBAHASAN

Pada penulisan ini mengkaji mengenai “**Perancangan Aplikasi Enkripsi & Deskripsi Pada Dokumen File Dengan Algoritma Triple DES Berbasis Web**”. Metode yang akan digunakan yaitu :

- a. Metode Pengumpulan data

Metode pengumpulan data menggunakan studi literature yang mengenai Perancangan Kriptografi dan Algoritma Triple DES

- b. Rancangan Penelitian

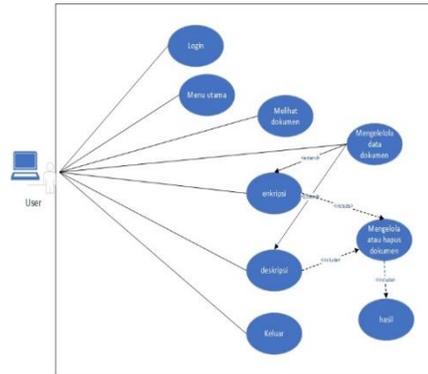
Menggunakan gambaran enkripsi dan dekripsi perancangan sistem kriptografi.

- c. Rancangan Aplikasi.

Menggunakan Bahasa pemrograman PHP .

Gambaran Proses Deskripsi dan Enkripsi

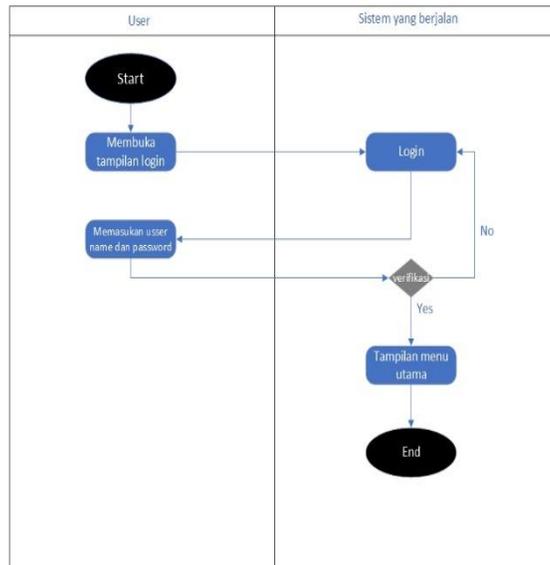
Use Case Diagram



Gambar 1. Use Case Diagram

Pada gambar di atas menjelaskan tentang use case diagram. Dimulai dari user log in lalu tampil menu utama, user dapat melihat dokumen, user dapat mengenkripsi dan mendeskripsi dokumen, user dapat mengelola atau menghapus dokumen, dan user mendapatkan hasil dokumen.

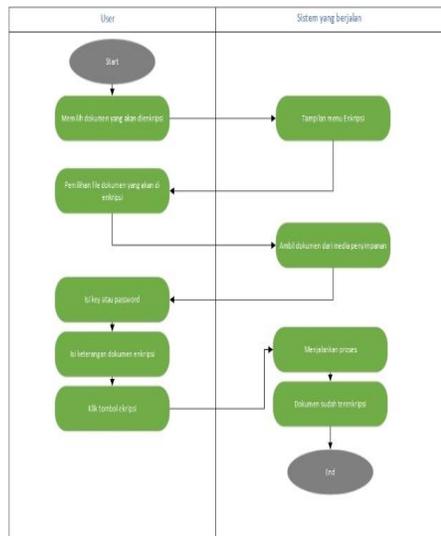
a. Diagram Login Masuk ke Aplikasi



Gambar 2. Diagram Login untuk masuk ke aplikasi

Pada gambar di atas menjelaskan tentang diagram log in. Di mulai dari user untuk log in, memasukkan username dan password, kemudian akan ada verifikasi berhasil dan setelah itu tampilan menu utama akan tampil.

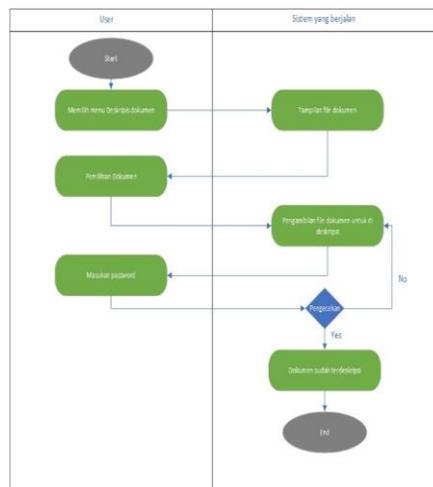
b. Diagram Deskripsi File Dokumen



Gambar 3. Diagram Deskripsi Dokumen

Pada gambar di atas menjelaskan tentang diagram deskripsi. Dimulai dari user memilih menu dokumen , lalu akan ada tampilan menu utama, user dapat memilih file dokumen, user memasukkan kunci atau password, setelah itu user memproses deskripsi kemudian akan ada pengecekan dan jika berhasil maka dokumen sudah deskripsi.

c. Diagram Enkripsi File Dokumen

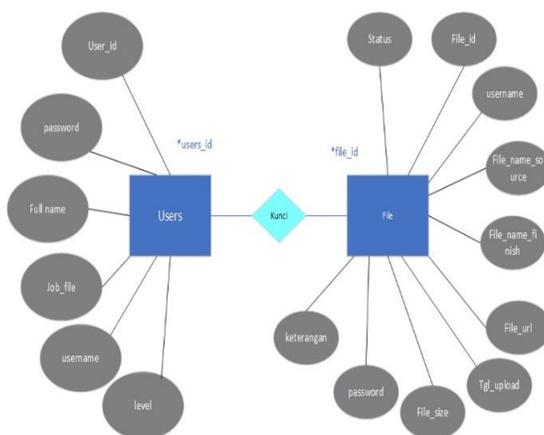


Gambar 4. Diagram Enkripsi Dokumen

Pada gambar di atas menjelaskan tentang diagram enkripsi. Dimulai dari user memilih menu dokumen, lalu akan ada tampilan menu utama, user dapat memilih file dokumen, user memasukkan kunci atau password, setelah itu user memproses enkripsi, kemudian proses akan berjalan dan jika berhasil maka dokumen sudah enkripsi.

Perancangan Basis Data

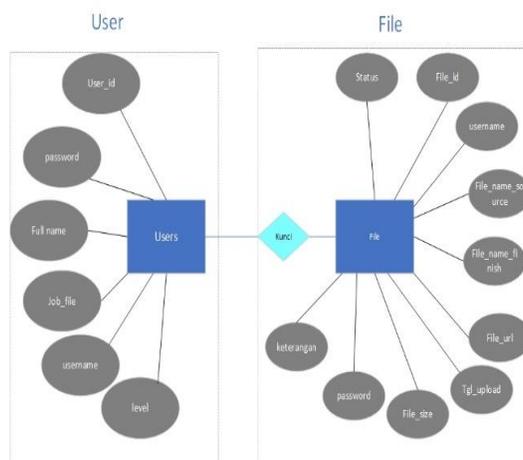
a. ERD (*Entity Relationship Diagram*)



Gambar 1. ERD (*Entity Relationship Diagram*)

Pada gambar ERD ini merupakan diagram untuk merancang basis data. Gambar diatas ada 2 komponen ada user dan juga file, masing-masing komponen memiliki item-item seperti gambar diatas.

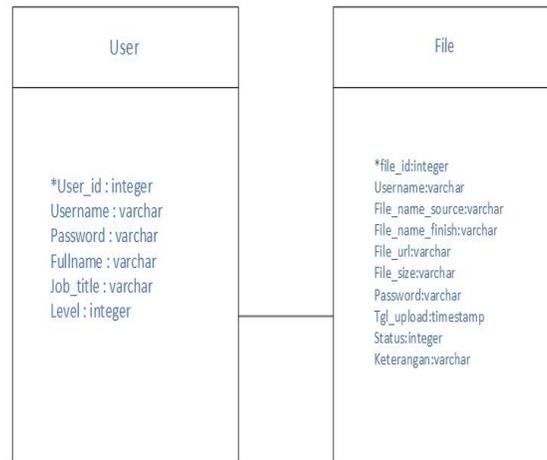
b. Transformasi ERD ke LRS



Gambar 2 Transformasi ERD ke LRS

Gambar di atas merupakan transformasi dari ERD ke LRS untuk membentuk data-data dari diagram penghubung dari entitas ke suatu LRS.

c. LRS (*Logical Record Structure*)



Gambar 3 LRS (*Logical Record Structure*)

Gambar diatas merupakan LRS (*Logical Record Structure*) objek yang diambil dari struktur rekaman pada tabel yang terbentuk dari relasi antar himpunan komponen di atas.

Rancangan Aplikasi.

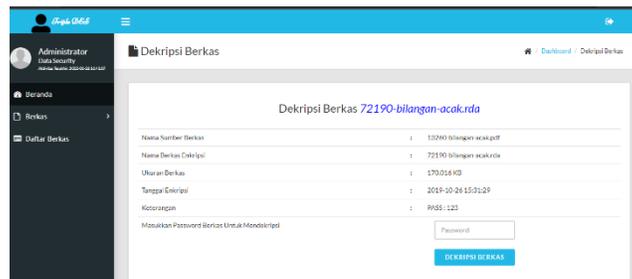
a. Tampilan Login Aplikasi Web



Gambar 1. Tampilan Login

Pada gambar diatas merupakan tampilan login, dimana user harus login terlebih dahulu sebelum melakukan proses enkripsi dan dekripsi, setelah menekan tombol login maka akan diarahkan menuju tampilan dashboard.

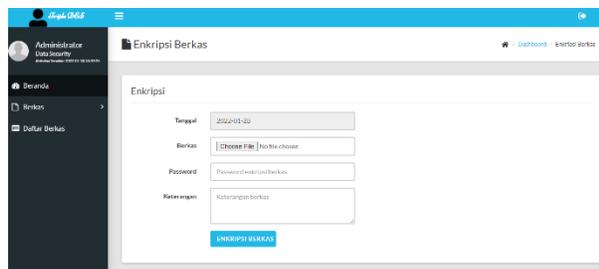
b. Tampilan Deskripsi Aplikasi Web



Gambar 2. Tampilan Deskripsi

Pada gambar diatas merupakan tampilan deskripsi dokumen,dimana user memilih file yang akan di deskripsikan ,kemudian memasukkan password dan jika password benar maka deskripsi dokumen berhasil dan jika password salah maka akan muncul pemberitahuan password yang dimasukkan salah lalu klik deskripsi maka file akan berhasil di deskripsi.

c. Tampilan Enkripsi Aplikasi Web



Gambar 3.Tampilan Enkripsi

Pada gambar 3 diatas merupakan tampilan enkripsi,dimana user memilih file yang akan dienkripsikan,kemudian memasukkan password ,isi keterangan dan jika password benar maka dokumen berhasil dienkripsikan, dan jika password yang dimasukkan salah maka ada pemberitahuan password yang dimasukkan salah, dan setelah itu klik enkripsi maka dokumen akan dienkripsi.

KESIMPULAN

Pada kesimpulan mengenai penulisan yang berjudul “Perancangan Aplikasi Enkripsi & Deskripsi Pada Dokumen File Dengan Algoritma Triple DES Berbasis Web”, bertujuan untuk perancangan aplikasi kriptografi pada dokumen. Dengan adanya system keamanan dokumen berbasis web dirancang sebuah system yang dapat melakukan proses keamanan data, pencarian, dan pengunduhan yang di proses menggunakan aplikasi berbasis web sehingga bisa dilakukan secara cepat dan efisien, pada akhirnya bisa menghasilkan suatu system keamanan dengan tepat. Aplikasi ini juga menjadi solusi untuk keamanan dokumen karena sudah menggunakan algoritma kriptografi.

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung jurnal ini. seperti teman teman yang sudah membantu dan para penulis lain nya.

REFERENSI

- Adhar, D. (2019). Implementasi Algoritma Des (Data Encryption Standard) Pada Enkripsi Dan Deskripsi Sms Berbasis Android. *Jurnal Teknik Informatika Kaputama (JTIK)*, 3(2), 53–60.
- Fauzi, M. (2018). *Jurnal Teknik Informatika Kaputama (JTIK) Vol. 2 , No. 1, Jan 2018*. 2(1), 98–104.
- Febriani, S. I., Juanita, S., & Hardjianto, M. (2020). Implementasi Kriptografi Teks pada SMS Menggunakan Algoritme Multiple Encryption dengan Metode RSA dan 3DES. *Jurnal Telematika, Institut Teknologi Harapan Bangsa, Bandung*, 15(2), 77–84.
- Hidayat, A. (2009). *Enkripsi dan Dekripsi Data Dengan Algoritma 3DES (Triple Data Encryption Standard)*. 1–11.
- Kartika, K. H. (2018). Perancangan Sistem Kriptografi Pada Document Menggunakan Algoritma Triple Des Dan Rsa. *Masitika*, 1–11.
- M. Adi Akbar, Ilhamsyah, I. R. (2016). Jurnal Coding Sistem Komputer Untan. *Jurnal Coding Sistem Komputer Untan*, 04(2), 184–194.
- Rantelinggi, P. H., & Saputra, E. (2020). Algoritma Kriptografi Triple Des dan Steganografi LSB sebagai Metode Gabungan dalam Keamanan Data. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, 7(4), 661. <https://doi.org/10.25126/jtiik.2020741838>
- Rodiyah, H. (1994). *MENGAMANKAN PESAN RAHASIA*. 0736.
- Saragih, E. D., Hasibuan, N. A., & ... (2019). Implementasi Algoritma Triple Des Dan Algoritma Advanced Encryption Standard Dalam Penyandian File Teks. *Informasi Dan ...*, 6, 29–35.
- Satria, M., Satria, M., Rosnelly, R., Teknik, J., Universitas, I., Utama, P., Jurusan, D., Informatika, T., Potensi, U., & Utama, U. P. (2020). Perancangan Aplikasi Keamanan Data Dokumen Word dengan Menggunakan Algoritma Triple DES. *Jurnal FTIK*, 1(1), 463–475.
- Zainuddin, M. A., & Mulyana, D. I. (2016). Penerapan Algoritma RSA untuk Keamanan Pesan Instan Pada Perangkat Android. *Jurnal CKI On SPOT*, 9(2), 105–114.