OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 07, Juli 2022
ISSN 2828-2442 (media online)
Hal 808-817

Aplikasi Pengamanan Data Menggunakan Kriptografi Dengan Metode Wake dan Algoritma Des Bebasis Java Desktop

Benny Suparman[1*], Sewaka[2]

Fakultas Teknik, Teknik Informatika, Universitas Pamulang, Kota Tangerang Selatan, Indonesia
Email: [1*]Bennysuparman10@gmail.com, [2]dosen00120@unpam.ac.id
(* : coressponding author)

Abstrak−PT.SEIV INDONESIA adalah perusahaan yang bergerak di bidang produksi cat, Perusahaan ini memiliki banyak produksi yang datanya tersimpan dalam bentuk file bernama Laporan Harian Bagian Penimbangan Produksi Cat. Data tersebut merupakan data yang penting yang berkaitan dengan data stock gudang. Masalahnya adalah data ini hanya tersimpan dalam folder yang berisi file yang belum memiliki keamanan tinggi, sehingga kemungkinan dapat di ubah oleh pihak yang tidak bertanggung jawab sehingga menimbulkan permasalahan yang menyebabkan hasil produksi tidak sama dengan data stock gudang, sehingga di butuhkan perangkat lunak untuk mengamankan data tersebut.

Kata Kunci : Kriptografi, Pengamanan Data, Metode WAKE dan Algoritma DES

Abstract−PT. SEIV INDONESIA is a company engaged in the production of paint, this company has many productions whose data is stored in a file called the Daily Report of the Cat Production Weighing Section. This data is important data related to warehouse stock data. The problem is that this data is only stored in a folder containing files that do not have high security, so it is possible that it can be changed by irresponsible parties, causing problems that cause production results to be not the same as warehouse stock data, so software is needed to secure the data.

Keywords: Cryptography, Data Security, WAKE and DES Algorithm Methods

1. PENDAHULUAN

PT. Seiv Indonesia didirikan sejak tahun 1965 oleh Bapak Husin Surriatmadja, sebagai industri yang bergerak di bidang produksi cat produk pertamanya dengan merek " Cat & Dog", dengan pesatnya kemajuan PT. Seiv Indonesia saat ini , perlu adanya laporan produski untuk mencatat proses kegiatan produksi Sehingga membutuhkan keamanan data agar tidak dapat diketahui orang lain.

Seiring dengan kemajuan teknologi dan informasi, kemanan data merupakan aspek terpenting dari sebuah sistem informasi untuk menjaga sebuah data di PT. Seiv Indonesia supaya tidak terjadinya menipulasi data dan tidak bisa diketahui orang lain. Maka sangat di perlukan sebuah keamanan data terhadap sebuah informasi yang disimpan dalam file tersebut.

Dalam dunia berkerja dibutukan kehati-hatian dan kewaspadaan termasuk menyimpan data. Seseorang yang biasa menyimpan data-data penting hanya menyimpan kedalam suatu folder saja, namun data atau isi dalam folder yang tidak terkode (plaintext), sangatlah rawan apabila tidak berhati-hati. Bisa saja data tersebut dapat berubah sehingga menyebabkan salah penafsiran.

Hal ini membuat peneliti ingin menerapkan pengamanan data yang kuat agar data tersebut aman dan sulit untuk di pecahkan orang lain, salah satu cara yang akan di lakukan peneliti adalah menerapkan suatu kriptografi dalam suatu aplikasi data txt, menggunakan java desktop.

Pada proses kriptografi haruslah terdapat 4 elemen utama didalamnya, yang berkaitan satu sama lain.plaintext merupakan sebagai data awal atau data asli yang disimpan. Plaintext ini lah yang kemudian di enkripsi dan di dekripsi. Chipertext merupakan sebuah data yang tersembunyi, yaitu data asli (plaintext) yang telah di enkripsi pada proses kriptografi.

Oleh sebab itu agar hal tersebut tidak terjadi penulis menggunakan metode kriptografi (Word Auto Key Encryption) WAKE dan (Data Encryption Standar) DES untuk proses enkripsi dan dekripsi data.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 07, Juli 2022
ISSN 2828-2442 (media online)
Hal 808-817

2. METODOLOGI PENELITIAN

Metode penelitian yang digunakan dalam penulisan tugas akhir sebagai berikut :

a. Metode pengumpulan data
Dimana penulis melakukan pengumpulan data dengan cara komukasi secara langsung dengan salah satu phak terkait pada PT. Seiv Indonesia. Dan juga mencari materi-materi yang berhubungan dengan kriptografi mulai dari jurnal, makalah, buku, dan yang lainnya sehingga terkumpulah suatu materi yang diterapakan pada aplikasi ini.

b. Metode analisa algoritma
Untuk menganalisa permasalahan pengamanan data yang di butuhkan pada saat ini, dalam hal ini analisa di lakukan dengan cara pengambilan fungsi-fungsi dari algoritma yang diterapkan untuk diimplementasikan pada aplikasi
keamanan data. Dan juga membahas bagaimana alur algoritma ini berjalan.

c. Metode pengujian aplikasi
Aplikasi akan di uji apakah aplikasi ini dapat dijalankan dengan baik atau tidak, di aplikasi ini akan di masukan dua buah algoritma yang nantinya akan mengamankan data txt. untuk melindungi data agar tidak dapat di rubah atau ingin mengetahui isi data tersebut.

3. ANALISA DAN PEMBAHASAN

3.1 Analisa Pembahasan

Aplikasi keamanan data ini digunakan untuk mengenkripsi dan mendeskripsikan data laporan *Docx,*XLs yang telah di simpan atau diinput. Aplikasi pengamanan data ini akan mengenkripsi data laporan yang asli (plaintext) menjadi (ciphertext) dan aplikasi pengamanan data akan mengdekeripsikan ciphertext menjadi data laporan txt yang asli (plaintext).

Beberapa kebutuhan sistem antara lain:

1. Mempunyai kemampuan mengenkripsi dan dekripsi data laporan *Docx,*XLs.
2. Menyimpan hasil enkripsi dan dekripsi dalam bentuk folder baru.

3.2 Analisa Kebutuhan

Kebutuhan perangkat lunak merupakan faktor penting yang harus dipenuhi dalam penelitian ini, sehingga perangkat lunak tersebut sesuai dengan maksud dan tujuan dalam penelitian.

Adapun perangkat lunak yang dibutuhkan dalam penelitian ini adalah sebagai berikut:

a. Kebutuhan perangkat lunak
   1. Windows 10
   2. Xampp for windows version 3.2.4
   3. Netbeans IDE 8.2

b. Kebutuhan perangkat keras
   1. Prosesor Intel Celeron N3350/BGA 4Ghz
   2. Kapasitas Ram 4 GB
   3. Kapasitas hardisk 500 GB
   4. Resolution Display 1366 x 768
   5. Windows 10 64-bit Operating System

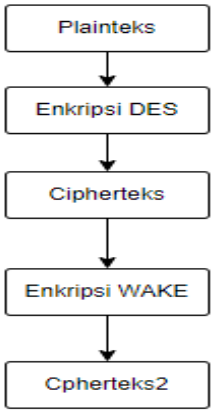
3.3 Analisa Algoritma

Algoritma yang digunakan dalam penelitian ini adalah penggabungan antara algoritma DES dan algoritma WAKE.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 07, Juli 2022
ISSN 2828-2442 (media online)
Hal 808-817

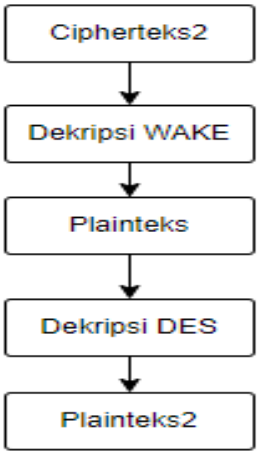
Cara kerja dari penggabungan kedua algoritma tersebut adalah:

1. Proses Enkripsi
   Pertama plaintext akan di enkripsi dengan algoritma DES terlebih dahulu dengan kunci yang di pilih minimal 8 karkater, kemudian hasil enkripsi tersebut (ciphertext) di enkripsi kembali menggunakan algoritma WAKE dengan kunci internal 16 karakter dan menghasilakan ciphertext yang ke dua (ciphertext akhir).
   Diagram proses enkripsi penggabungan algoritma DES dan algoritma WAKE.



Gambar 1 Diagram Proses Enkripsi

2. Proses Dekripsi
   Awalnya suatu ciphertext akan didekripsi mengunakan algoritma WAKE Terlebih dahulu, kemudian hasil dekripsi tersebut (plaintext 1) di dekripsi kembali menggunakan algoritma DES Sesuai dengan kunci yang digunakan pada saat proses enkripsi. Diagram proses dekripsi penggabungan algoritma DES dan WAKE.



Gambar 2 Diagram Proses Dekripsi

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 07, Juli 2022
ISSN 2828-2442 (media online)
Hal 808-817

3.4 Metode Word Auto Key Encryption (WAKE)

Metode WAKE merupakan salah satu algoritma stream cipher yang telah digunakan secara komersial. WAKE merupakan singkatan dari Word Auto Key Encryption. Metode ini ditemukan oleh David Wheeler pada tahun 1993.

Metode WAKE menggunakan kunci 128 bit dan sebuah tabel 256 x 32 bit. Dalam algoritmanya, metode ini menggunakan operasi XOR, AND, OR dan Shift Right. Metode WAKE ini telah digunakan pada program Dr. Solomon Anti Virus. Proses utama WAKE terdiri dari 4 :

1. Proses pembentukan tabel S-Box (Substitution Box), berfungsi untuk membentuk tabel S-Box sebesar 256 x 32 bit. Isi dari tabel S-Box ini akan digunakan pada proses pembentukan kunci.
2. Proses pembentukan kunci, berfungsi untuk membangkitkan bit-bit kunci yang akan digunakan pada proses enkripsi dan dekripsi.
3. Proses enkripsi, berfungsi untuk menyandikan (encoding) data dan menghasilkan cipherteks.
4. Proses dekripsi, berfungsi untuk mengembalikan cipherteks menjadi teks asli kembali.

Proses pembentukan tabel S-Box adalah sebagai berikut :

1. Inisialisasi nilai TT[0] … TT[7] :

TT[0] : 726A8F3B (dalam heksadesimal)
TT[1] : E69A3B5C (dalam heksadesimal)
TT[2] : D3C71FE5 (dalam heksadesimal)
TT[3] : AB3C73D2 (dalam heksadesimal)
TT[4] : 4D3A8EB3 (dalam heksadesimal)
TT[5] : 0396D6E8 (dalam heksadesimal)
TT[6] : 3D4C2F7A (dalam heksadesimal)
TT[7] : 9EE27CF3 (dalam heksadesimal)

2. Inisialisasi nilai awal untuk T[0] … T[3] :

T[0] = K[0]
T[1] = K[1]
K[0], K[1], K[2], K[3] dihasilkan dari kunci yang dipecah menjadi 4 bagian yang sama panjang.

3. Untuk T[4] sampai T[255], lakukan proses berikut :
   X = T[n-4] + T[n-1]
   T[n] = X >> 3 XOR TT(X AND 7)
4. Untuk T[0] sampai T[22], lakukan proses berikut :
   T[n] = T[n] + T[n+89]
5. Set nilai untuk beberapa variabel di bawah ini :
   X = T[33]
   Z = T[59] OR (01000001h)
   Z = Z AND (FF7FFFFFh)
   X = (X AND FF7FFFFFh) + Z
6. Untuk T[0] … T[255], lakukan proses berikut :
   X = (X AND FF7FFFFFh) + Z
   T[n] = T[n] AND 00FFFFFFh XOR X
7. Inisialisasi nilai untuk beberapa variabel berikut ini :
   T[256] = T[0]
   X = X AND 255
8. Untuk T[0] … T[255], lakukan proses berikut :
   Temp = (T[n XOR X] XOR X) AND 255
   T[n] = T[Temp]
   T[X] = T[n+1]

Simbol “>>” adalah operasi geser kanan (shift right) yaitu operasi yang menggeser sejumlah bit ke kanan (right) dan mengisi tempat kosong dengan nilai bit “0” (nol). Operasi shift right dilambangkan dengan “>>”.

Contoh operasi shift right :

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 07, Juli 2022
ISSN 2828-2442 (media online)
Hal 808-817

11000110 >> 1 : 01100011

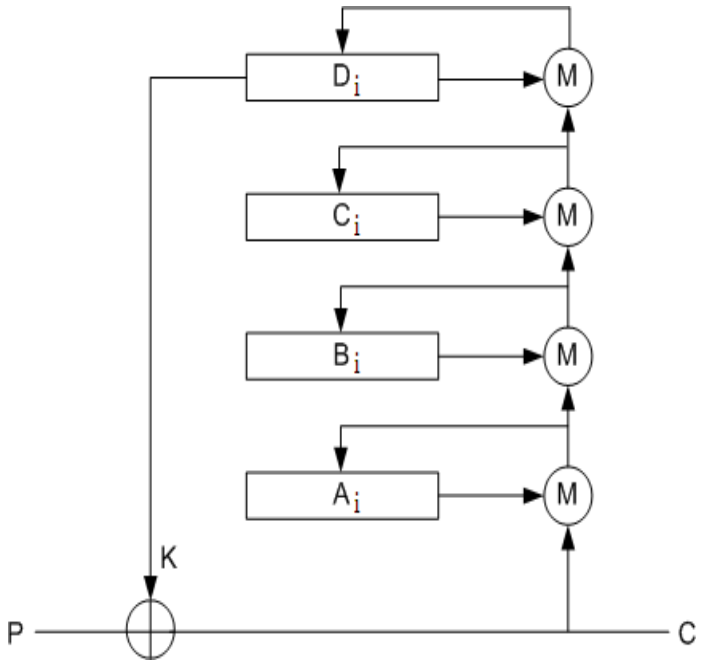
11000110 >> 2 : 00110001

Proses pembentukan kunci dari algoritma WAKE dapat ditentukan sendiri yaitu sebanyak n putaran. Semakin banyak putaran dari proses pembentukan kunci, maka keamanan datanya akan semakin terjamin. Fungsi yang digunakan dalam proses pembentukan kunci adalah :

M(X, Y) = (X + Y) >> 8 XOR T[(X + Y) AND 255].

Pertama-tama, kunci yang di-input akan dipecah menjadi 4 bagian dan di-set sebagai nilai awal dari variabel A_0, B_0, C_0, dan D_0. Nilai dari variabel ini akan diproses dengan melalui langkah berikut:

$A_{i+1} = M(A_i, D_i)$
$B_{i+1} = M(B_i, A_{i+1})$
$C_{i+1} = M(C_i, B_{i+1})$
$D_{i+1} = M(D_i, C_{i+1})$
Nilai dari D_i merupakan nilai dari kunci K_i.
Lebih detail dapat diperhatikan pada bagan proses pembentukan kunci pada gambar berikut.



Gambar 3 Proses pembentukan kunci WAKE

Keterangan :
P = Plaintext
K = Key
C = Ciphertext
M = Fungsi M
i = Dimulai dari 0 sampai n.
Ai = Bagian pertama dari pecahan kunci
Bi = Bagian kedua dari pecahan kunci
Ci = Bagian ketiga dari pecahan kunci
Di = Bagian keempat dari pecahan kunci
Inti dari algoritma WAKE tidak terletak pada proses enkripsi dan dekripsinya, karena proses enkripsi dan dekripsinya hanya berupa operasi XOR dari plaintext dan kunci untuk menghasilkan ciphertext atau operasi XOR ciphertext dan kunci untuk menghasilkan plaintext.

P = C □ K
C = P □ K

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 07, Juli 2022
ISSN 2828-2442 (media online)
Hal 808-817

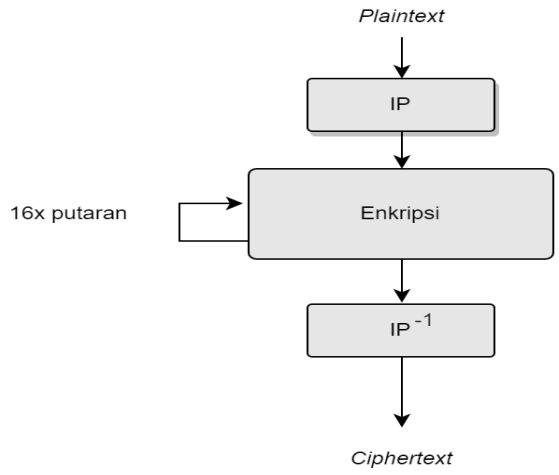
dengan : P = Plaintext
K = Key
C = Ciphertext

3.5 Metode Algoritma Data Encryption Standard (DES)

Pada tahun 1972 sebuah perusahaan National Bureau Standard (NBS) di Amerika Serikat, yang sekarang dikenal dengan National Institute of Standard and Technology (NIST), memulai sebuah projek dalam mengamankan data dan komunikasi komputer. Mereka ingin mengembangkan algoritma kriptografi tunggal. Setelah dua tahun kemudian, NBS menyadari bahwa IBM's Lucifer dapat menjadi kandidat yang bagus, dari pada mengembangkan algoritma baru dari awal. Setelah beberapa diskusi, pada tahun 1975 NBS mengumumkan detail dari algoritma tersebut. Pada akhir tahun 1976, pemerintah federal Amerika Serikat mengadopsi algoritma ini dan kemudian mengganti namanya menjadi Data Encryption Standard (DES).

Algoritma DES terdiri dari tiga proses, yaitu pembangkitan kunci internal, enkripsi data, dan dekripsi data. Algoritma DES dirancang untuk mengenkripsi dan mendekripsi data dalam blok data yang terdiri atas 64 bit di bawah kontrol kunci 64 bit. Dekripsi data harus dikerjakan menggunakan kunci yang sama dengan yang dipakai untuk mengenkripsi data.

DES mengenkripsikan 64 bit plaintext menjadi 64 bit ciphertext dengan menggunakan 56 bit kunci internal yang dibangkitkan dari 64 bit kunci eksternal. Kunci eksternal merupakan kunci yang dimasukkan oleh pengguna pada sistem, sedangkan kunci internal merupakan kunci yang digunakan untuk melakukan enkripsi pada setiap putaran DES (ada 16 putaran) yang diperoleh dari kunci eksternal yang telah diproses.



Gambar 4 Rancangan Global Algoritma DES

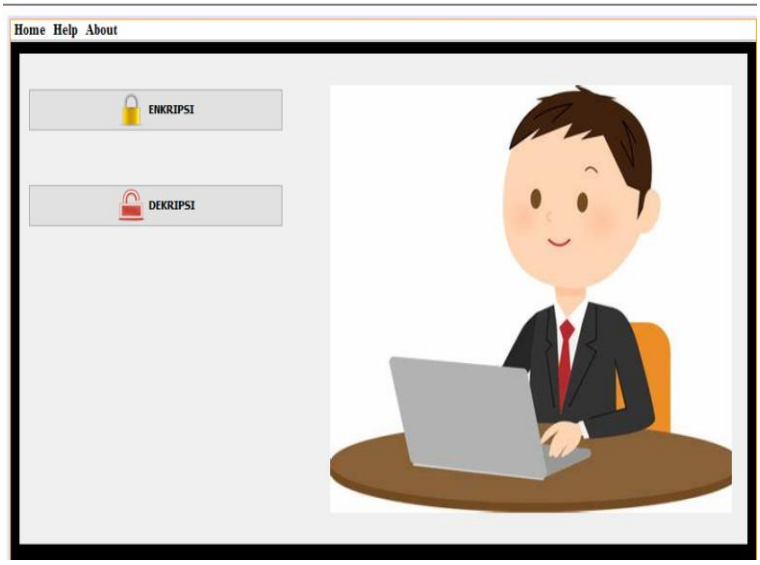
4. IMPLEMENTASI

4.1 Implementasi User Interface

User Interface adalah tampilan aplikasi yang memudahkan pengguna untuk berinteraksi dengan aplikasi. Berikut ini adalah implementasi dari rancangan user interface yang telah dibuat :

1. Tampilan Halaman *Menu* (Menu Utama)

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 07, Juli 2022
ISSN 2828-2442 (media online)
Hal 808-817



Gambar 5 Halaman Menu Utama

Keterangan gambar :

a. Jika menekan jmenu “Home” maka akan menampilkan tombol Log out.
b. Jika menekan jmenu “Help” maka akan menampilkan petunjuk penggunaan.
c. Jika menekan jmenu “About” maka akan menampilkan tentang aplikasi.
d. Jika menekan button “Enkripsi” maka akan menampilkan form enkripsi.
e. Jika menekan button “Dekripsi” maka akan menampilkan form dekripsi.

2. Tampilan Halaman Enkripsi

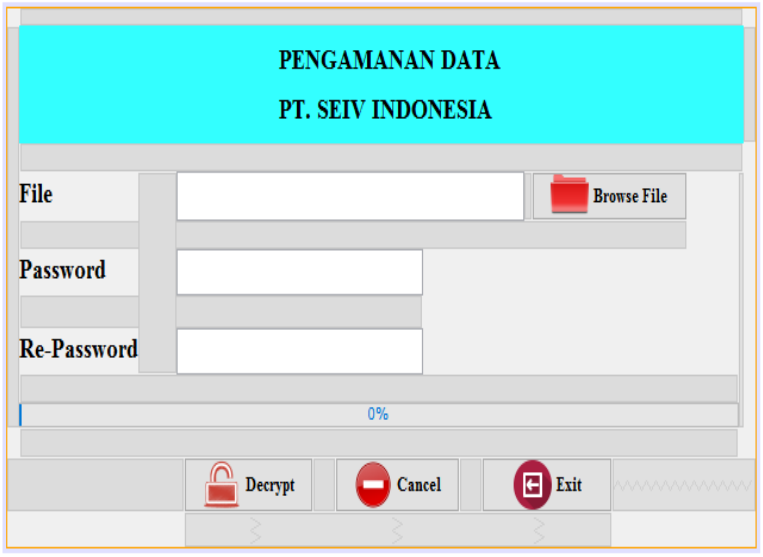
Gambar 6 Halaman Enkripsi

Keterangan gambar :

a. Jika menekan button “ Browse File” maka akan menampilkan data yang ingin dienkripsi.
b. Jika menekan button encrypt maka akan memporses data untuk dienkripsi.
c. Jika menekan button “Cancel” maka akan membatalkan .
d. Jika menekan button “Exit” maka akan keluar dari form enkripsi.

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 07, Juli 2022
ISSN 2828-2442 (media online)
Hal 808-817

3. Tampilan Halaman Dekripsi



Gambar 7 Halaman Dekripsi

Keterangan gambar :

a. Jika menekan button " Browse File" maka akan menampilkan data yang ingin dienkripsi.
b. Jika menekan button decrypt maka akan memporses data untuk didekripsi.
c. Jika menekan button "Cancel" maka akan membatalkan .
d. Jika menekan button "Exit" maka akan keluar dari form enkripsi.

4. Tampilan Menu Help (bantuan)

Gambar 8 Halaman Menu Help

Keterangan gambar :

a. Jika menekan tabbed pane "Help Encript" akan menampilkan cara mengenkripsi data
b. Jika menekan tabbed pane "Help Decrypt" akan menampilkan cara mendekripsikan data yang sudah terenkripsi sebelumnya.
c. Jika menekan button "Exit" akan keluar dari form help

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 1, No. 07, Juli 2022
ISSN 2828-2442 (media online)
Hal 808-817

5. Tampilan Menu About (tentang)

Gambar 9 Halaman Menu About

Keterangan gambar :

a. Jika menekan tabbed pane "About Author" maka akan menampilkan data diri.
b. Jika menekan tabbed pane "About System" maka akan menampilkan judul skripsi dan nama dosen pembimbing.
   Jika menekan button "Exit" akan keluar dari form About

5. KESIMPULAN

Berdasarkan hasil yang didapat dari aplikasi ini maka dapat ditarik kesimpulan dalam permasalahan yang terjadi, Penentuan proses enkripsi dan dekripsi data laporan harian bagian penimbangan Produksi cat di Pt.Seiv Indonesia dengan melakukan testing plaintext 200 karakter dilakukan dengan baik dan cepat. Pembuatan aplikasi dengan menggabungkan metode (Word Auto Key Encryption) WAKE dan algoritma (Data Encryption Standard) DES sangatlah membantu para pengguna dalam pengamanan data laporan mereka pada saat berkerja, sehingga memperkecil kemungkinan isi data tersebut dapat dilihat dan diubah oleh orang lain yang tidak mempunyai hak atas data tersebut.

REFERENCES

Allwine, J. H. P. S. (2019). Perangkat Lunak Pembelajaran Metode Kriptografi WAKE (Word Auto Key Encryption). Jurnal Bisantara Informatika, 3(1), 33–42.

Basim, Z., & Painem, P. (2020). Implementasi Kriptografi Algoritma RC4 Dan 3DES dan Steganografi Dengan Algoritma EOF Untuk Keamanan Data Berbasis Desktop Pada SMK As-Su'udiyyah. Skanika, 3(4), 45–52.

Erlangga, T., & Kusumaningsi, D. (2018). Implementasi Algoritma Advanced Encryption Standard-128 (AES-128) Untuk Pengamanan Database Berbasis Desktop Pada Icaltoys. Skanika, 1(2), 565–569.

Harbani, A., & Fahreza, M. A. (2019). Aplikasi Keamanan Data Gambar Menggunakan Algoritma RSA (Rivest Shamir Adleman) Berbasis Desktop. Teknois : Jurnal Ilmiah Teknologi Informasi dan Sains, 9(1), 1–9.

Jaya, P., & Juanita, S. (2018). Aplikasi Pengamanan Basis Data dengan Algoritma RSA dan WAKE Berbasis Desktop. Skanika, Vol 1(1), 352–358.

Maya, W. R., Azanuddin, A., & Elfitriani, E. (2022). Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES. Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer), 21(1),

Pradypta, A. A., Studi, P., Informatika, T., As-syafi, U. I., Gede, P., & Barat, J. (2022). PERANCANGAN APLIKASI DATA SECURITY DALAM MELINDUNGI INFORMASI DIGITAL MENGGUNAKAN TEKNIK ALGORITMA RIJNDAEL BERBASIS DESKTOP. 9(1), 68–76.

Rifa'i, A., & Sumartini, L. C. (2019). Implementasi Kriptografi Menggunakan Metode Blowfish Dan Base64 Untuk Mengamankan Database Informasi Akademik Pada Kampus Akademi Telekomunikasi Bogor Berbasis Web-Based. Jurnal E-Komtek (Elektro-Komputer-Teknik), 3(2), 87–96.

Rizki, M., & Farida Ariyani, P. (2021). Penerapan Kriptografi Dengan Menggunakan Algoritma Rsa Untuk Pengamanan Data Berbasis Desktop Pada Pt Trias Mitra Jaya Manunggal. Skanika, 4(2), 1–6.

Siswanto, A., Syukur, A., & Husna, I. (2018). Perbandingan Metode Data Encryption Standard (Des) Dan Advanced Encryption Standard (Aes) Pada Steganografi File Citra. Seminar Nasional Teknologi Informasi Dan Komunikasi, October, 229–236.