Journal of Computer System and Informatics (JoSYC)
Volume 2, No. 1, November 2020, Page 70-76
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Implementasi Algoritma *Data Encryption Standart* (*DES*) Dalam Pengamanan Data Karyawan Ramayana Department Store

Alan Boy Sandy Damanik[1,*], Indra Gunawan[1], Bahrudi Efendi Damanik[2], Sumarno[1], Dedy Hartama[1]

[1] STIKOM Tunas Bangsa, Pematangsiantar, Indonesia
[2]AMIK Tunas Bangsa, Pematangsiantar, Indonesia
Email: [1,*]alanboysandy08@gmail.com, [2]indra@amiktunasbangsa.ac.id, [3]bahrudiefendi@gmail.com
[4]sumarno@amiktunasbangsa.ac.id, [5]dedyhartama@stikomtb.ac.id
Submitted: **10/11/2020**; Accepted: **16/11/2020**; Published: **27/11/2020**

Abstrak−Data pegawai merupakan informasi yang sangat terjaga kerahasiaannya karena berisikan informasi penting tentang pegawai maupun instansinya. Di zaman ini kerahasiaan sesuatu data seperti data karyawan menjadi sesuatu yang harus benar-benar terjaga keamanannya. Komputer saat ini merupakan komponen utama yang dapat dijadikan sebagai alat yang di gunakan perusahaan yang mampu menyimpan data, mempercepat pekerjaan, meningkatkan kualitas dan kuantitas layanan, mempermudah proses transaksi, dan lainnya. Namun dari segi keamanan komputer masih memiliki beberapa celah dan kelemahan yang memungkinkan seseorang maupun kelompok dapat dengan mudah mengambil data atau informasi didalam komputer tersebut. Untuk menghindari terjadinya hal yang dapat membuat kerugian seperti pencurian dan manipulasi data maka perlu diterapkannya sebuah system keamanan. Kriptografi merupakan ilmu yang mempelajari cara mengubah informasi dari keadaan/bentuk normal (dapat dipahami) menjadi bentuk yang tidak dapat dipahami. Salah satu metode yang dapat digunakan untuk mengamankan pesan/informasia dalah Data Encryption Standart (DES). Penerapan algoritma kriptografi DES dalam pengamanan data Karyawan Ramayana menunjukan bahwa algoritma ini dapat menghasilkan enkripsi yang tidak dapat dipahami oleh manusia dan menghasilkan dekripsi yang sama persis dengan plain text awal yang di-input-kan.

Kata Kunci: Pegawai, Keamanan, *DES*, Enkripsi, Dekripsi

Abstract−Employee data is information that is very confidential because it contains important information about employees and their institutions. Computers are currently the main component in the company that is able to store data, speed up work, improve the quality and quantity of services, simplify the transaction process, and others. But in terms of computer security still has several loopholes that allow a person or group to easily retrieve data or information on the computer. To avoid data theft and manipulation, a security system must be implemented. Cryptography is a study of how to change information from normal conditions / forms (can be understood) into a form that cannot be understood. One method that can be used to secure messages / information is the DataEncryption Standard (DES). The application of the DES cryptography algorithm in securing Civil Servants data shows that this algorithm can generate encryption that cannot be understood by humans and produces the exact decryption of the initial plaintext input.

Keywords: Employee, Security, DES, Encryption, Decryption

1. PENDAHULUAN

Teknologi komputer selalu memberikan kemudahan yang baik bagi pengguna dalam pelayanan di berbagai bidang kehidupan dan membantu dalam menyelesaikan sebuah pekerjaan menjadi lebih akurat, lebih cepat dan lebih efisien. Maka dari itu komputer menjadi sarana yang wajib dan penting bagi kehidupan sehari-hari. PT Ramayana Lestari Sentosa Tbk bergerak di dalam bidang ilmu komputer yang digunakan dalam kegiatan produksi pelayanan jasanya.

Data atau informasi merupakan salah satu hal aset yang sangat penting dalam berlangsungnya suatu perusahaan, institusi- institusi pendidikan, instansi-instansi pemerintahan dan untuk pribadi. Masalah keamanan merupakan salah satu aspek terpenting dalam suatu sistem informasi. Sehingga memerlukan berbagai macam pertimbangan untuk melakukan penyimpanan data, terlebih dalam segi keamanan dan kerahasiaannya. Sering sekali terjadi kasus pembocoran data rahasia oleh pihak-pihak tidak berwenang seperti *hacker* maupun *cracker* yang menyebabkan kerugian besar bagi sang pemilik data. Oleh sebab itu, untuk menjaga kerahasiaan informasi tersebut dibutuhkan sebuah teknologi yang dapat merahasiakan informasi yang dikirim, seperti kriptografi. Kriptografi adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim, dapat tersampaikan dengan aman pada penerima dengan cara menyamarkannya dalam bentuk sandi yang tidak mempunyai makna. Banyak sekali teknik kriptografi yang digunakan untuk proses enkripsi dan dekripsi pesan. Salah satu kriptografi ini adalah *Data Encryption Standard (DES)*. Metode *Data encryption Standart (DES)* merupakan algoritma kriptografi yang paling banyak digunakan [1]. *Data Encryption Standart (DES)* banyak digunakan dalam di dalam dunia penyebaran informasi sebagai pengamanan data agar tidak dapat dibaca atau diretas oleh orang lain. *Data Encryption Standart (DES)* banyak digunakan dalam di dalam dunia penyebaran informasi sebagai pengamanan data agar tidak dapat dibaca atau diretas oleh orang lain.

Pada penelitian sebelumnya, [2] melakukan penelitian yang berjudul "Aplikasi Enkripsi pesan *SMS* dengan Algoritma Kriptografi *Block Chiper DES* Berbasis *Android*" tentang pengembangan perangkat lunak aplikasi ponsel pada *platform smartphone* khususnya *Android.* Salah satu fasilitas yang disediakan ponsel adalah pengiriman data berupa pesan singkat melalui *Short Message Service (SMS).* Dalam penelitian tersebut harus ada penambahan fungsi pengambilan nomor tujuan dari *contacs phone* agar tidak ada penyadapan yang terjadi serta

Journal of Computer System and Informatics (JoSYC)
Volume 2, No. 1, November 2020, Page 70-76
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

penambahan fungsi untuk pembacaan SMS yang berbentuk *content* agar pembacaan SMS tidak bersifat sementara. penelitian selanjutnya, [1] dalam judul "*Prototype* Model Keamanan Data Menggunakan Kriptografi *Data Encryption Standart (DES)* dengan operasi *Chiper Block Chaining (CBC)"* melakukan penelitian yang bertujuan untuk dapat membuat suatu *prototype* model keamanan data pada suatu aplikasi yang berfungsi sebagai pengamanan suatu data atau informasi. Dalam penelitian tersebut hasil penguji menunjukkan bahwa model enkripsi dekripsi suatu data dapat dilakukan dengan baik pada *file* dengan format *txt, rtf, dan doc.*

2. METODOLOGI PENELITIAN

2.1 Implementasi

Implementasi adalah proses untuk memastikan terlaksananya suatu kebijakan dan tercapainya kebijakan tersebut. Impelementasi juga dimaksudkan menyediakan sarana untuk membuat sesuatu dan memberikan hasil yang bersifat praktis terhadap sesama [3].

2.2 Kriptografi

Kriptografi (cryptography) berasal dari bahasa Yunani dan terdiri dari dua suku kata, yaitu "*cryptos"* yang artinya rahasia (*secreet*) dan *"graphein"* artinya tulisan (writing). Kriptografi diartikan sebagai ilmu dan seni untuk menjaga keamanan pesan. Suatu proses penyandian yang melakukan perubahan sebuah kode (pesan) dari yang bisa dimengerti atau plainteks menjadi sebuah kode yang tidak bisa dimengerti atau cipherteks disebut enkripsi. Sedangkan proses kebalikannya untuk mengubah cipherteks menjadi plainteks disebut dekripsi (Liwandouw and Wowor, 2017).
Algoritma kriptografi yang baik tidak di tentukan oleh kerumitan dalam mengolah data atau pesan yang akan disampaikan. Yang penting, algoritma harus memenuhi 4 persyaratan berikut :

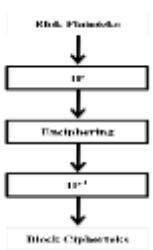
a. Kerahasian Pesan (*Plaintext*) hanya dapat dibaca oleh pihak yang memiliki kewenangan.
b. Autentikasi. Pengirim pesan harus dapat diidentifikasi dengan pasti, penyusup harus dipastikan tidak bisa berpura pura menjadi orang lain.
c. Integritas. Penerima pesan harus dapat memastikan bahwa pesan yang dia terima tidak dimodifikasi ketika sedang dalam proses transmisi data.
d. *Non-Repudiiation.* Pengirim pesan harus tidak bisa menyangkal pesan yang dia kirimkan.

Kriptografi pada dasarnya terdiri dari dua proses yaitu proses enkripsi dan proses dekripsi. Proses enkripsi dapat diartikan sebagai kode atau *chipher.* Sedangkan dekripsinya merupakan suatu proses kebalikan dari proses enkripsinya. Pada dasarnya algoritma terdiri dari fungsi dasar yaitu:

a. Enkripsi, merupakan hal yang sangat penting dalam kriptografi yang merupkan pengamanan data yang dikirimkan terjaga kerahasiaannya, pesan aslinya disebut *plaintext* yang dirubah menjadi kode kode yang tidak dimengerti.
b. Dekripsi, merupakan kebalikan dari enkripsi. Pesan yang telah di enkripsi dikembalikan ke bentuk aslinya (*plain text).*
c. Kunci yang dimaksud disini adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi yang terbagi menjadi 2 (dua) yaitu kunci pribadi *(private key*) dan kunci umum (*public key*).

2.3 Data Encryption Standard (DES)

Menurut (Abdala and Budiman, 2015) *DES* merupakan *blockcipher* simetris yang beroperasi pada blok 64 bit yang menggunakan sebuah kunci 56 bit adalah. Algoritma *DES* dibuat di *IBM,* dan merupakan modifikasi daripada algoritma terdahulu yang bernama *Lucifer. Lucifer* merupakan algoritma *cipher block* yang beroperasi pada blok masukan *64-bit* dan kuncinya berukuran *28-bit.* Pengurangan jumlah *bit* kunci pada *DES* dilakukan dengan alasan agar mekanisme algoritma ini bisa diimplementasikan dalam satu *chip.*
Algoritma *DES* dalam mengenkrip satu blok data *64- bit.* Untuk dekripsi, proses yang sama dilakukan kembali, hanya saja digunakan kunci K[j] dalam urutan yang berlawanan, yaitu memasukkan K[16] terlebih dahulu, kemudian K[16], seterusnya hingga K[1] [1]. Algoritma *DES* pertama kali di publikasikan di Federal Register pada 17 maret 1975. Setelah dilakukannya diskusi algoritma *DES* diangkat sebagai algoritma standart yang digunakan oleh *NBS (National Bureau of Standart)* pada 15 januari 1977. Sejak saat itu DES banyak digunakan di dunia informasi untuk melindungi data agar tidak bisa dibaca oleh orang lain.



Gambar 1. Skema Global Algoritma DES

Journal of Computer System and Informatics (JoSYC)
Volume 2, No. 1, November 2020, Page 70-76
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

2.4 *Flowchart*

Menurut [6]**,** *Flowchart* adalah gambaran dalam bentuk diagram alir dari algoritma dalam suatu program yang menyatakan arah alur program dalam menyelesaikan suatu masalah.

2.5 Java

Menurut [7] Java merupakan bahasa pemrograman berorientasi objek daan bebas platform, dikembangkan oleh SUN Micro System dengan jumlah keunggulan yang memungkinkan java dijadikan sebagai bahasa pengembang entreprise. Java adalah mereupakan bahasa pemrograman yang bersifat umum/non-spesifik (general-purpose).

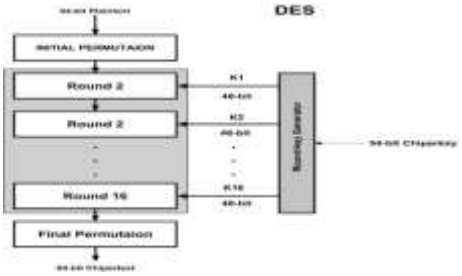
2.6 NetBeans

Menurut [7] NetBeans merupakan salah satu IDE yang dikembangkan dengan bahasa pemrograman java. NetBeans adalah sebuah perangkat lunak open source sehingga dapat digunakan secara gratis untuk keperluan komersial maupun nonkomerisal yang didukung oleh sun microsystem.

3. HASIL DAN PEMBAHASAN

3.1 Rancangan Penelitian

Rancangan yang digunakan penulis dlam menyelesaikan permasalahan ini adalah dengan menggunakan *flowcart*:



Gambar 2. *Flowchart* Proses Dekripsi Algoritma *DES*

Ramayana Department Store bergerak didalam bidang pelayanan barang dan jasa, dimana dalam perusahaan atau instansi tersebut tidak bisah jauh-jauh dari teknologi ilmu komputer dalam melakukan pelayanannya. Walaupun menggunakan teknologi yang sudah sangat maju, semua perusahaan tetap memiliki kode etik yang harus dirahasiakan ataupun dokoumen-dokumen penting yang kerahasiaannya harus terjaga salah satunya keamanan Data Karyawan. Karena dalam pengamanan data karyawan tersebut belum terjaga baik maka penulis ingin membuat sebuah aplikasi yang nantinya bisa digunakan dan membantu meperketat keamanan data karyawan.

3.2 Penerapan Kriptografi

Untuk melakukan implementasi sistem keamanan kedalam program aplikasi maka dibutuhkan sebuah algoritma atau langkah-langkah atau intruksi yang digunakan untuk mengenkripsi dan mendekripsikan data-data yang dianggap rahasia. Dalam hal ini algoritma yang digunakan penulis dalam penelitian adalah *algoritma kriptografi DES*.
Hasil konversi *plaintext* dan kunci diatas adalah sebagai berikut:

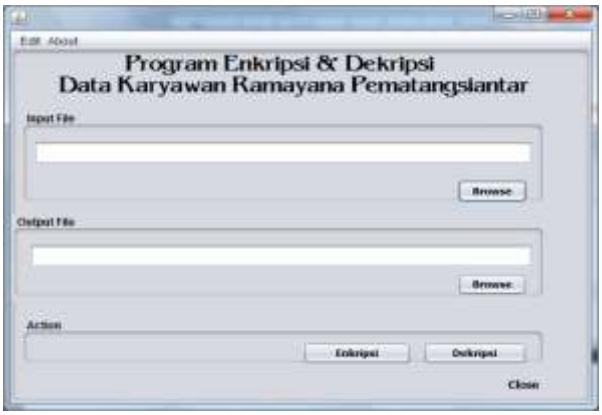
Plaintext : “4B 61 72 79 61 77 61 6E”
Kunci : “41 6C 67 6F 2D 44 45 53”
Selanjutnya menkonversi *plaintext* dan kunci kedalam bentuk heksadesimal maka selanjutnya:

a. Langkah pertama yang dilakukan adalah mengubah *plaintex* menjadi bilangan *biner*
b. Langkah kedua yang dilakukan adalah *Initian Permutation (IP)* pada *plaintext*
c. Langkah ketiga adalah *Generate* kunci menggunakan tabel permutasi kompresi PC-1. Kompresi 64 *bit* menjadi 54 *bit* dengan membuang 1 *bit (parity bit)* tiap block kunci :
d. Langkah keempat lakukan pergeseran pada C0 dan D0 menggunakan tabel pergeseran *bit* 16 putaran.
e. Langkah kelima ini kita akan meng-espansi data R_{i-1} 32 *bit* menjadi R_i 48 *bit*sebanyak 16 kali putaran dengan nilai perputaran 1<=i<=16 menggunakan Tabel Ekspansi (E).
f. Langkah keenam setiap *vector* Ai disubsitusikan ke 8 buah *S-box* (subtitusi *box)*,dimana blok ke 1 disubtiusikan ke S1, blok ke 2 disubtitusikan ke S2 dan seterusnya menghasilkan output vektor *Bit* 32 bit.
g. Langkah ketujuh setelah didapatkan vektor Bi, lalu permutasikan bit vektor Bi dengan tabel P-Box, lalu kelompokkan menjadi 4 blok dimana tiap-tiap blok memiliki 32 bit.
h. Langkah kedelapan gabungkan R16 dengn L16 lalu permutasikan untuk terakhir kali dengan tabel invers initial permutation (IP-1).

Journal of Computer System and Informatics (JoSYC)
Volume 2, No. 1, November 2020, Page 70-76
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

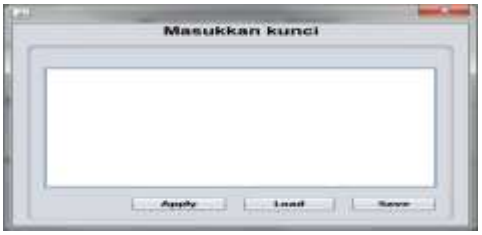
3.3 Implementasi Program

Terdapat dua fungsi utama pada aplikasi ini, yaitu fungsi enkripsi dan fungsi dekripsi, yang mana keduanya dapat kita akses melalui menu utama, seperti gambar 3 :



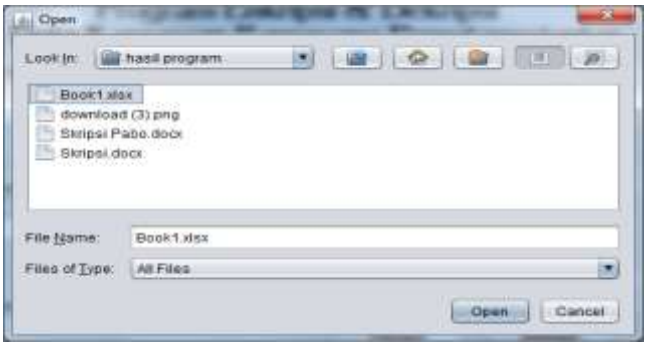
Gambar 3. Tampilan Menu Utama

Langkah selanjutnya selanjutnya masukkan kunci terlebih dahulu sebelum memilih file yang akan dienkripsi, dapat dilihat pada gambar 4 :



Gambar 4. Tampilan Masukkan Kunci

Selanjutnya pilih *file* yang akan di eknkripsi seperti terlihat dalam gambar 5:



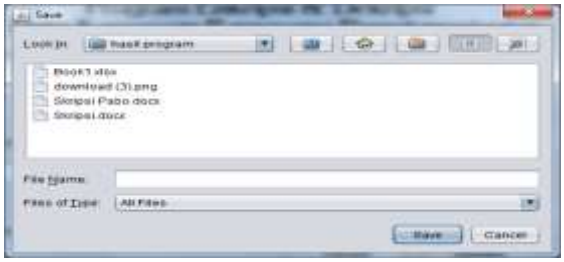
Gambar 5. Tampilan Pilih File Untuk Enkripsi

Setelah *file* inputnya telah dipilih maka akan muncul tampilan seperti berikut:

Gambar 6. Tampilan File Input Telah Dipilih

Journal of Computer System and Informatics (JoSYC)
Volume 2, No. 1, November 2020, Page 70-76
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Setelah memilih file yang akan di-*input* untuk dienkripsi lalu pilih output file untuk meyimpan file. Tampilannya dapat dilihat pada gambar 7**:**



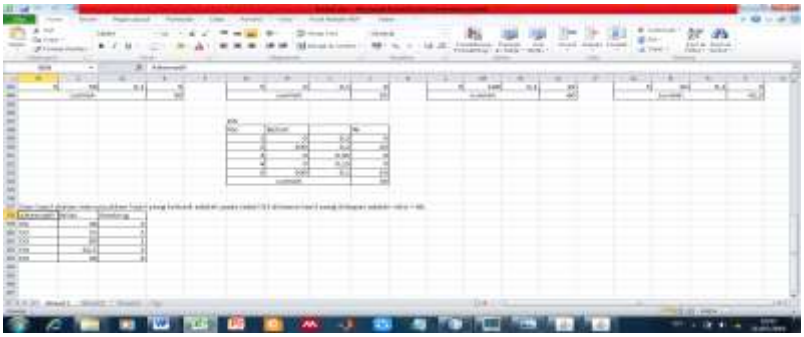
Gambar 7. Tampilan Pilih File Output Untuk Enkripsi

Setelah *output file* dipilih maka akan muncul tampilan seperti gambar 8 :

Gambar 8. Tampilan Pilih *Output File* Telah Dipilih

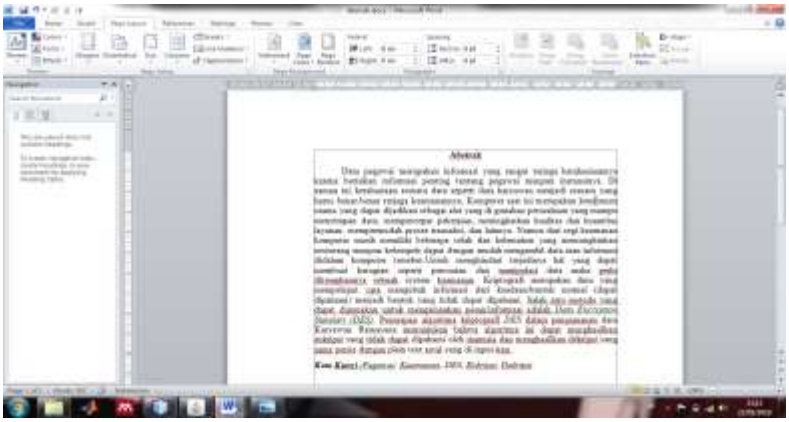
Sebelum dijalankannya program pastikan file yang akan dienkripsi dan dekripsi benar-benar masih bisa di buka.

1. File *.xls*



Gambar 9. Tampilan File yang Akan di Enkripi dan di Dekripsi (Dalam bentuk *.xls*)

2. File *.doc*



Gambar 9. Tampilan File yang Akan di Enkripsi dan Dekripsi (Dalam bentuk *.doc*)

3. File *.jpg dan .png*

Journal of Computer System and Informatics (JoSYC)
Volume 2, No. 1, November 2020, Page 70-76
ISSN 2714-8912 (media online)
ISSN 2714-7150 (media cetak)

Gambar 10. Tampilan File yang Akan di Enkripsi dan Dekripsi (Dalam bentuk *.jpg dan .png*)

Setelah semua file yang akan dienkripsi dan didekripsi di pastikan masih bisa, maka lakukan proses enkripsi pada beberapa file yang telah dipilih, apabila berhasil maka akan muncul tampilan pada gambar 11**.** :

Gambar 11. Tampilan Proses Enkripsi Telah Berhasil

4. Hasil file *.xls* setelah dienkripsi

Apabila proses enkripsi telah berhasil maka file yang tadi dipilih tidak dapat lagi di buka karena telah dienkripsi, terlihat pada gambar 12:

Gambar 12. Tampilan File Yang Telah Dienkripsi (Dalam bentuk *.xls*)

5. Hasil File *.doc* telah berhasil di enkripsi

Gambar 13. Tampilan File Yang Telah di Enkripsi (Dalam bentuk *.doc*)

6. Hasil File *.jpg* dan *.png* berhasil di enkripsi

Gambar 14. Tampilan File Yang Telah di Enkripsi (Dalam bentuk *.jpg* dan *.png*)

4. KESIMPULAN

Berdasarkan dari penelitian ini yang dilakukan pada rancangan aplikasi Kriptografi Keamanan Data Karyawan Ramayana Pematangsiantar menggunakan metode *Data Encryption Standart (DES)* dapat disimpulkan algoritma *DES* berhasil digunakan atau di aplikasikan untuk mengamankan atau mengenkripsi *file* dengan berbagai jenis, seperti *file* dokumen, gambar (*jpg*), video dan musik dapat mengembalikan *plaintext* seperti semula. Data yang diamankan melalui metode *DES* tetap aman dan terjaga dengan keamanan pasword yang hanya *user* pengguna yang mengetahuinya. Algoritma *DES* juga memiliki kelebihan yaitu memasukkan kunci terlebih dahulu baru bisa menjalankan aplikasi atua mengenkrip atau mendekrip *file* atau data yang akan diamankan. Dan harus memasukkan kunci terlebih dahulu sebelum melakukan *browse file* yang akan di enkripsi dan didekrpisi.

Dari penelitian yang telah dilakukan, saran yang diberikan yang nantinya dapat mengembangkan penelitian ini adalah sebagai berikut.

a. Memperbaiki menu utama dengan menambahkan menu *login* agar tidak bisa melakukan *browse* sebelum masuk.
b. Dapat mengembangkan keamanan kunci atau kode program algoritma *DES* agar keamanannya jauh lebih kuat.
c. Memberikan menu bantuan agar dapat membantu user dalam melakukan enkripsi dan dekripsi saat dalam kesulitan.
d. Dapat mengembangkan *DES* agar dapat mengamnkan data dalam ukuran besar.
e. Algoritma *DES* memiliki kelemahan, yaitu kunci nya yang lemah yang menyebabkan kunci-kunci internal pada setiap putaran sama.

REFERENCES

[1] A. Muzakir, “PROTOTYPE MODEL KEAMANAN DATA MENGGUNAKAN KRIPTOGRAFI DATA ENCRYPTION STANDAR (DES) DENGAN MODE OPERASI CHIPER BLOCK CHAINING,” hal. 33–36, 2014.
[2] A. Abdullah, “Aplikasi Enkripsi pesan.”
[3] A. S. Putra, O. M. Febriani, dan B. Bachry, “Implementasi Genetic Fuzzy System untuk Mengidentifikasi Hasil Curian Kendaraan di Polda Lampung,” *J. Sist. Inf. Manaj. Basis Data*, vol. 1, no. 1, hal. 21–30, 2018.
[4] V. B. Liwandouw dan A. D. Wowor, “Desain Algoritma Berbasis Kubus Rubik dalam Perancangan Kriptografi Simetris,” no. April 2015, 2017.
[5] P. Abdala dan M. A. Budiman, “Implementasi Algoritma Kriptografi Vernam Cipher dan DES (Data Encryption Standard) pada Aplikasi Chatting berbasis Android,” *J. Ilm. Core It*, hal. 1–19, 2015.
[6] H. Nurdiyanto dan H. Meilia, “SISTEM PENDUKUNG KEPUTUSAN PENENTUAN PRIORITAS PENGEMBANGAN INDUSTRI KECIL DAN MENENGAH DI LAMPUNG TENGAH MENGGUNAKAN ANALITICAL HIERARCHY PROCESS (AHP),” hal. 6–7, 2016.
[7] A. Rusmayanti, “Sistem Informasi Pengelolaan Keuangan Pada Desa Ngadirejan,” vol. 6, no. 2, hal. 35–39, 2014.