Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI) p-ISSN: 2620 – 5327
Volume 7 Nomor 1, April 2024 e-ISSN: 2715 – 5501
DOI : 10.57093/jisti.v7i1.221

Implementasi Algoritma Advanced Encryption Standard Untuk Keamanan Data Customer Pegadaian UPC Pacongkang

Radus Batau
Program Studi Teknik Informatika, Universitas Indonesia Timur
Jl. Rappocini Raua No. 174 Makassar, Sulawesi Selatan, 90231, Indonesia
radus.kinzha@gmail.com

Kata Kunci :
Aplikasi Kriptografi; Keamanan File; Metode *AES*.

ABSTRAK

Permasalahan yang ada pada Pegadaian UPC Pacongkang adalah sering terjadi kebocoran data customer yang membuat perubahan data secara tiba-tiba, seperti jangka waktu peminjaman customer berubah dan bahkan jumlah peminjaman customer berubah. Hal ini tentunya merugikan pihak Pegadaian UPC Pacongkang dan *customer*. Melihat permasalahan tersebut pihak Pegadaian UPC Pacongkang membutuhkan metode pengamana data yang dapat membantu menjaga kerahasiaan data *customer*. Melindungi data perusahaan adalah dengan menggunakan teknik kriptografi. metode matematis yang berkaitan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, dan autentikasi. penelitian yang akan dilakukan yaitu mengamankan file dokumen. Untuk menerapkan kriptografi pada sistem keamanan data dibutuhkan suatu algoritma mesin autentukasi data. Salah satu metode yang dapat digunakan adalah *Advanced Encryption Standard (AES)*. Keuntungan menggunakan algoritma *Advanced Encryption Standard* pada kriptografi Sistem Keamanan data *customer* pada Pegadaian UPC Pacongkang dapat menyembunyikan informasi asli dari data sehingga tidak mudah diketahui oleh orang yang tidak berkepentingan. Dengan diimplementasikan Implementasi Kriptografi Superenkripsi Menggunakan Metode *Advanced Encrytion Standard* Pada Pengamatan Data *Customer* Pegadaian UPC Pacongkang. File data nasabah Pegadaian UPC Paconggkang menjadi aman dan tidak mudah dimanipulasi oleh orang lain karena pesan asli sudah diubah menjadi file acak yang tidak bisa dimengerti.

Keywords
Cryptography Applications; File Security; AES Method.

ABSTRACT

The problem that exists at Pegadaian UPC Pacongkang is that customer data leaks often occur which make sudden changes to data, such as the customer's loan period changes and even the amount of customer loans changes. This is certainly detrimental to the Pacongkang UPC Pawnshop and the customer. Seeing this problem, Pegadaian UPC Pacongkang needs a data security method that can help maintain the confidentiality of customer data. Protecting company data is by using cryptographic techniques. mathematical methods related to information security aspects such as confidentiality, data integrity, and authentication. the research to be done is securing document files. To apply cryptography to data security systems, a data authentication engine algorithm is needed. One method that can be used is Advanced Encryption Standard (AES). The advantage of using the Advanced Encryption Standard algorithm in the cryptography of the customer data security system at Pegadaian UPC Pacongkang can hide the original information from the data so that it is not easily known by unauthorized people. With the implementation of Superencryption Cryptography Implementation Using the Advanced Encrytion Standard Method on Pacongkang UPC Pawnshop Customer Data Observation. Paconggkang UPC Pegadaian customer data files are safe and not easily manipulated by

others because the original message has been converted into a random file that cannot be understood.

PENDAHULUAN

Pegadaian atau rumah gadai adalah sebuah individu atau lembaga yang menawarkan jasa peminjaman uang kepada masyarakat dengan jaminan benda milik masyarakat yang ingin melakukan pinjaman uang. Bila suatu barang digadaikan untuk mendapatkan pinjaman dari pegadaian, maka pada waktu yang telah ditentukan oleh pegadai boleh membeli kembali atau menebus kembali barang yang telah digadaikan dengan biaya tambahan atau bunga sebagai keuntungan pihak pegadaian. Dalam menjalankan aktifitas pelayanan pegadaian, membutuhkan administrasi baik data administrasi *customer* atau data peminjaman dipegadaian (Lestari et al., 2015).

Data pegadaian merupakan suatu hal yang sangat berharga di zaman teknologi informasi saat ini. Khusunya jika data tersebut sangat rahasia dan tidak semua orang boleh mengaksesnya. Perusahaan atau lembaga lainnya memiliki data yang sangat penting sehingga data tersebut tidak boleh diakses setiap orang, terutama perusahaan atau lembaga yang bergerak dibidang jasa pegadaian.

Salah satu pegadaian yang ada di Kabupaten Soppeng adalah Pegadaian UPC Pacongkang. Pegadaian UPC Pacongkang memiliki data yang sangat rahasia yang tidak boleh diketahui oleh setiap orang, khususnya data *customer*. Hal ini disebabkan data ini hanya ditujukan untuk pihak perusahaan dan tidak boleh terpublikasi. Maka diperlukan suatu keamanan data. Keamanan dalam penyimpanan suatu data atau informasi adalah hal yang sangat penting dan tidak dapat diabaikan. Salah satu dampak negatif dalam perkembangan teknologi adalah pencurian data. Pencurian data ini tentunya merugikan bagi pemilik data, untuk menghindari kejahatan tersebut maka dibutuhkan pengamanan dalam penyimpanan data yang dianggap penting agar terhindar dari kejahatan teknologi informasi atau tidak mudah dapat diakses oleh orang yang tidak memiliki hak.

Permasalahan yang ada pada Pegadaian UPC Pacongkang adalah sering terjadi kebocoran data customer yang membuat perubahan data secara tiba-tiba, seperti jangka waktu peminjaman customer berubah dan bahkan jumlah peminjaman customer berubah. Hal ini tentunya merugikan pihak Pegadaian UPC Pacongkang dan *customer*. Melihat permasalahan tersebut pihak Pegadaian UPC Pacongkang membutuhkan metode pengamana data yang dapat membantu menjaga kerahasiaan data *customer*.

Perkembangan teknologi dibidang pengamanan data sudah banyak yang dapat digunakan oleh pihak perusahaan. Salah satu metode teknologi keamanan data adalah kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data**.** Kriptografi bertujuan untuk mengamankan isi data atau menjaga kerahasiaan informasi dari orang yang tidak berhak untuk mengetahui isi data tersebut (Han & goleman, daniel; boyatzis, Richard; Mckee, 2019). Untuk menerapkan kriptografi pada sistem keamanan data dibutuhkan suatu algoritma mesin autentukasi data. Salah satu metode yang dapat digunakan adalah *Advanced Encryption Standard (AES)*.

Algoritma *Advanced Encryption Standard* (AES) merupakan algoritma *cryptographic* yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok *chipertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut *ciphertext* sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai *plaintext*.

Keuntungan menggunakan algoritma *Advanced Encryption Standard* pada kriptografi Sistem Keamanan data *customer* pada Pegadaian UPC Pacongkang dapat menyembunyikan informasi asli dari data sehingga tidak mudah diketahui oleh orang yang tidak berkepentingan. Dengan sistem keamanan *Advanced Encryption Standard* orang lain tidak dapat mengerti dengan isi data didalam file sehinggah susah untuk merubah data.

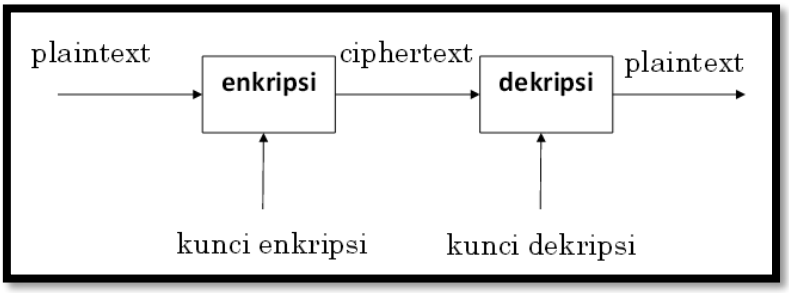
KAJIAN PUSTAKA

1. Pengertian Aplikasi.

Definisi umum aplikasi adalah perangkat komputasi yang siap digunakan pengguna yang menjalankan fungsi tertentu dan merupakan alat terapan yang terintegrasi sesuai dengan fungsinya. Aplikasi adalah aplikasi yang menyimpan sesuatu dalam bentuk data, soal, media yang dapat Anda gunakan untuk bekerja atau menerapkan dalam bentuk baru. Aplikasi adalah perangkat lunak yang dikembangkan oleh perusahaan komputer untuk melakukan tugas tertentu, seperti: Contoh: Microsoft Word, Microsoft Excel (Siregar & Melani, 2019). Aplikasi berasal dari kata aplikasi dan artinya pelaksanaan penggunaan aplikasi. Aplication (sering disebut sebagai aplikasi) adalah perangkat lunak yang mengambil fitur tertentu dan membuatnya tersedia untuk pengguna. App Store dan Android App Store memiliki jutaan aplikasi yang menyediakan layanan aplikasi. aplication itu sendiri adalah fondasi ekonomi seluler(Nursakti, 2019)

2. Konsep Kriptografi

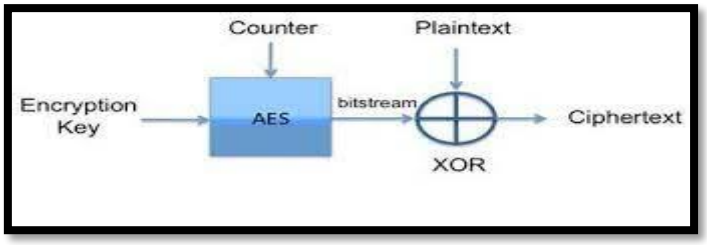
Kriptografi berasal dari kata Yunani yang menggabungkan dua kata: cryptocurrency dan graphene. Kryptos artinya tersembunyii atau *secret* dan *graphenee* artinya menulis. Kriptografi secara harfiah berarti menulis rahasia untuk mengirim pesan yang harus dirahasiakan. Arti lain dari kriptografi adalah mengenkripsi teks biasa (*plaintext*) secara acak dengan kunci penyandian, membuat plainteks sulit dibaca oleh pihak yang tidak memiliki kunci dekripsi (*ciphertext*). Ilmu kriptografi berkembang seiring dengan kemajuan teknologi. Secara kronologis, ilmu kriptografi dapat dibedakan menjadi dua pengertian, yaitu kriptografi klasik dan kriptografi modern. Kedua interpretasi tersebut didasarkan pada penggunaan alat analisis kriptografi dan generator pesan (Febriana & S, 2017). Kriptografi adalah ilmu kriptografi di mana "teks asli" (plaintext) dienkripsi dengan kunci sandi menjadi "skrip acak" (ciphertext) yang sulit diuraikan oleh seseorang yang tidak memiliki kunci dekripsi. Anda dapat mengembalikan data asli dengan mendekripsi dengan kunci dekripsi. Teknik enkripsi yang digunakan dalam kriptografi klasik adalah enkripsi simetris, dimana kunci dekripsi sama dengan kunci enkripsi. Kriptografi kunci publik membutuhkan kriptografi asimetris, dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi, dan pembangkitan kunci untuk skema enkripsi asimetris lebih intensif secara komputasi daripada enkripsi simetris. Ini karena enkripsi asimetris menggunakan angka yang sangat besar. (Muhammad Yasin, 2017).



Gambar 1. Konsep Kriptografi

3. Algoritma *Advanced Encryption Standard (AES)*

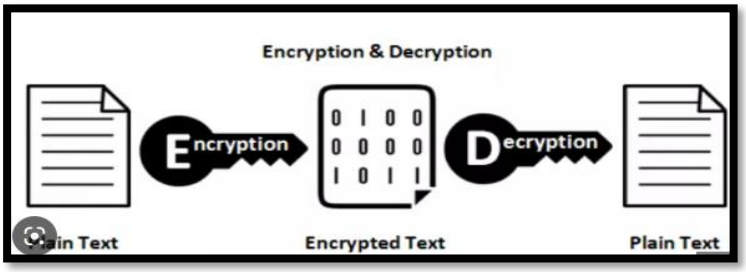
Advanced Encryption Standard (AES) adalah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris pada saat ini. Dalam algoritma kriptografi AES 128, 1blok plainteks berukuran 128 bit terlebih dahulu dikonversi menjadi matriks heksadesimal berukuran 4x4 yang disebut state. Setiap elemen *state* berukuran 1 *byte.* Proses enkripsi pada AES merupakan transformasi terhadap state secara berulang dalam 10 ronde. Setiap ronde AES membutuhkan satu kunci hasil dari generasi kunci yang menggunakan 2 transformasi yaitu subtitusi dan transformasi. Pada proses enkripsi AES mengunakan 4 transformasi dasar dengan urutan trasformasi *subbytes, shiftrows, mixcolumns,* dan *addroundkey.* Sedangkan pada proses dekripsi mengunakan invers semua transformasi dasar pada algoritma AES kecuali *addroundkey* dengan urutan transformasi *invshiftrows, invsubbytes, addroundkey,dan invmixcolumns.* Pada data teks, proses enkripsi diawali dengan mengkonversi teks menjadi kode ASCII dalam bilangan heksadesimal yang dibentuk menjadi matriks byte 4x4. Selanjutnya dilakukan beberapa trnsformasi dasar seperti *subbytes, shiftrows, mixcolumns,* dan *addroundkey.* Akan tetapi ketika melakukan trasformasi data yang diproses pada setiap trasformasi berupa data biner dari matriks heksadesimal. Kriptografi AES 128 bit memiliki ruang kunci 2 128 yang merupakan nilai yang sangat besar dan dianggap aman untuk digunakan sehingga terhindar dari *brute force attack* (Tulloh et al., 2016).



Gambar 2. Alur Algoritma AES

4. Enkripsi Data

Secara umum Enkropsi merupakan teknik pengamanan informasi yang dilakukan dengan cara mengolah informasi awal (plaintext) dengan suatu kunci tertentu menggunakan suatu metode enkripsi tertentu sehingga menghasilkan informasi baru (ciphertext) yang tidak dapat dibaca seecara langsung. Ciphertext tersebut dapat dikembalikan menjadi informasi awal (plaintext) melalui proses deskripsi (Ismail, Syahrir, 2021). Enkripsi adalah proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal(Tahir, 2018). Enkripsi menggunakan algoritma yang kompleks yang disebut cipher dalam rangka untuk mengubah data normal (plaintext) menjadi serangkaian karakter acak (ciphertext) yang tidak dapat dibaca oleh orang-orang tanpa kunci khusus yang membuat data tersebut terdekripsi (Wiharto & Irawan, 2018)



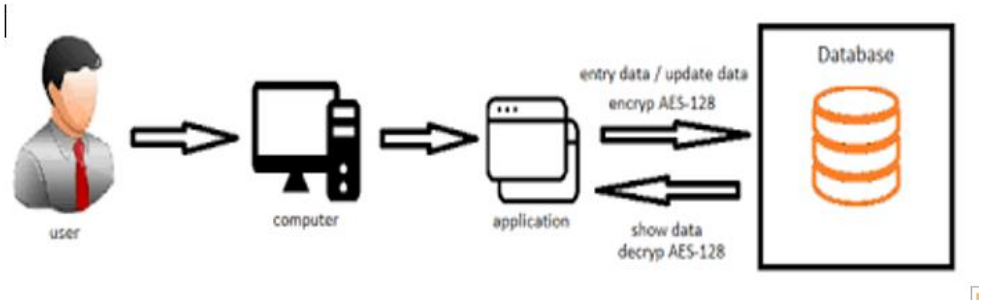
Gambar 3. Proses Enkripsi

Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI) p-ISSN: 2620 – 5327
Volume 7 Nomor 1, April 2024 e-ISSN: 2715 – 5501
DOI : 10.57093/jisti.v7i1.221

METODE PENELITIAN

1. Rancangan Sistem

Langkah-langkah yang diambil dalam merancang sistem ini membuat saran logis dan lainnya untuk pemecahan masalah. Berikut ini adalah diagram Implementasi Algoritma Advanced Encryption Standard Untuk Keamanan Data Customer Pegadaian Upc Pacongkang.



Gambar 4. Proses Pengamanan Data dengan Metode AES

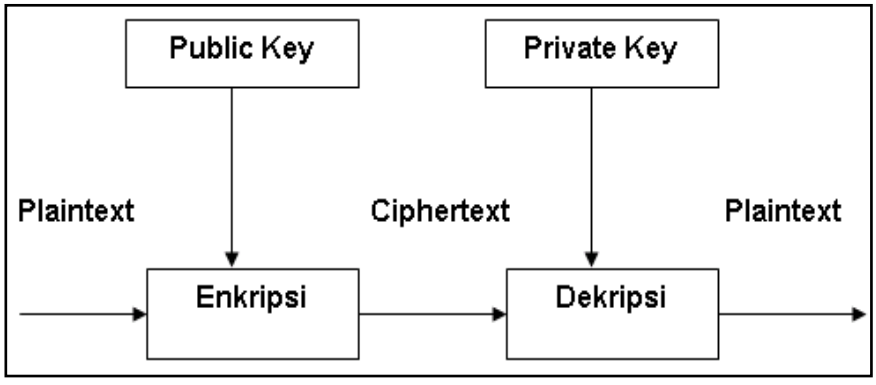
2. Metode Pengujian Sistem

Metode yang digunakan untuk menguji sistem yang diusulkan adalah metode black-box. Metode ini memungkinkan Anda untuk mengukur kompleksitas desain prosedural Anda dan menggunakannya sebagai panduan untuk menentukan Prosedur Fungsional Sistem:

HASIL DAN PEMBAHASAN

1. Implementasi Algoritma

Kriptografi bertujuan untuk mengamankan isi data atau menjaga kerahasiaan informasi dari orang yang tidak berhak untuk mengetahui isi data tersebut. Dengan teknik atau algoritma tertentu yang disebut proses enkripsi (encrypt), data diubah menjadi data sandi yang bentuknya berbeda dengan data aslinya. Berikut alur sistem Kriptografi yang digambarkan pada blok diagram:



Gambar 5. Cara Kerja Algoritma

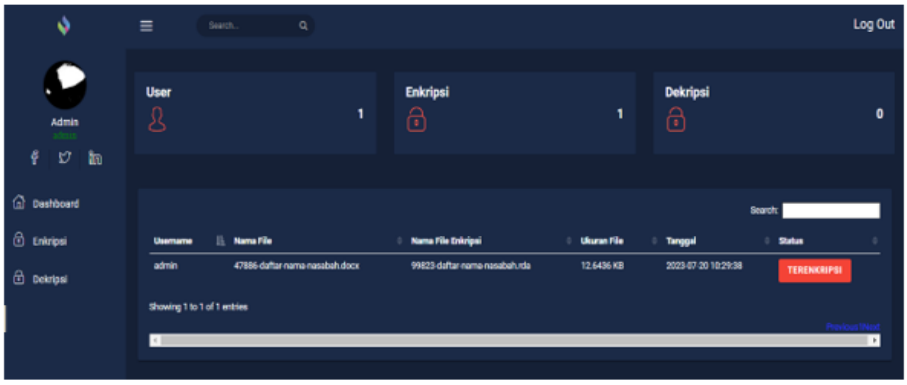
p-ISSN: 2620 – 5327
e-ISSN: 2715 – 5501

2. Implementasi Sistem

Pada tahapan ini dilakukan implementasi aplikasi dengan menggunakan bahasa pemrograma php. Berikut ini hasil implementasi aplikasi:

a. Halaman Utama

Berikut adalah gambar tampilan halaman utama aplikasi kriptografi keamanan file:

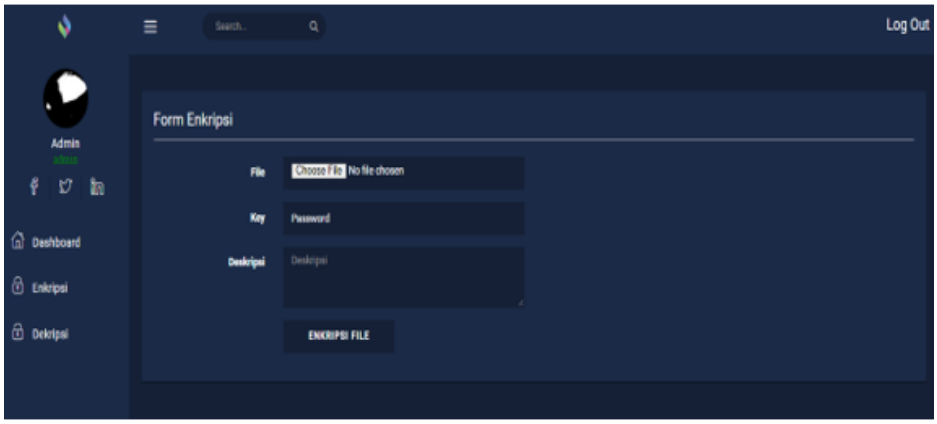


Gambar 6. Halaman Utama Aplikasi

Gambar diatas merupakan hasil implementasi halaman utama aplikasi. Halaman ini merupakan halaman yang pertama kali tampil pada saat aplikasi kriptografi dibuka.

b. Halaman Enkripsi File

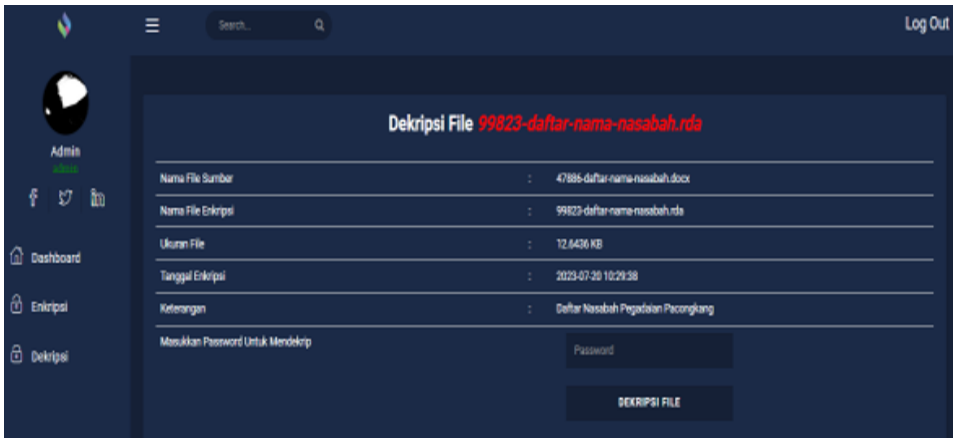
Tampilan implementasi halaman enkripsi file pada aplikasi kriptografi keamanan file. Halaman ini bertujuan untuk memproses file data nasabah menjadi pesan rahasia yang beda dengan file aslinya. Berikut adalah gambar tampilan halaman enkripsi file kriptografi keamanan file data nasabah pegadaian UPC Pacongkang :



Gambar 7. Halaman Enkripsi File

c. Halaman Dekripsi File

Tampilan implementasi halaman dekripsi file pada aplikasi kriptografi keamanan file data nasabah. Halaman ini bertujuan untuk memproses file yang telah dienkripsi dengan mengembalikan file aslinya. Berikut adalah gambar tampilan halaman Dekripsi file Kriptografi keamanan file data nasabah pegadaian UPC Pacongkang :



Gambar 8. Halaman Ekstrak File

SIMPULAN

Berdasarkan hasil Implementasi Algoritma Advanced Encryption Standard Untuk Keamanan Data Customer Pegadaian Upc Pacongkang, maka dapat ditarik kesimpulan sebagai berikut:

1. Hasil analisis data menggunakan teknik Spiral sistem yang digunakan pada proses pengamanan file belum memiliki keamanan yang tinggui sehingga mudah dimanipulasi oleh orang lain.
2. Berdasarkan hasil perancangan sistem yang dibuat dengan menggunakan konsep perancangan terstruktur menggunakan Dokumen Flowchart telah berjalan sesuai dengan yang diinginkan sehingga memudahkan dalam pembuatan sistem keamanan file berbasis kriptografi EAS.
3. Dengan diimplementasikan Implementasi Kriptografi Superenkripsi Menggunakan Metode *Advanced Encrytion Standard* Pada Pengamatan Data *Customer* Pegadaian UPC Pacongkang. File data nasabah Pegadaian UPC Paconggkang menjadi aman dan tidak mudah dimanipulasi oleh orang lain karena pesan asli sudah diubah menjadi file acak yang tidak bisa dimengerti.

SARAN

Setelah melaukukan penelitian ini, maka penulis menyarankan agar pada peneltian berikutnya diharapkan menggunakan metode yang lain untuk membuat sistem keamanan file agar ada pembanding metode

DAFTAR PUSTAKA

Arman, A. (2017). Sistem Informasi Pengolahan Data Penduduk Nagari Tanjung Lolo, Kecamatan Tanjung Gadang, Kabupaten Sijunjung Berbasis Web. *Edik Informatika*, *2*(2), 163–170. https://doi.org/10.22202/ei.2016.v2i2.1459

Budiman, Q., Mouton, S., Veenhoff, L., & Boersma, A. (2021). ANALISIS PENGENDALIAN MUTU DI BIDANG INDUSTRI MAKANAN (Studi Kasus: UMKM Mochi Kaswari Lampion Kota Sukabumi). *Jurnal Inovasi Penelitian*, *1*(0.1101/2021.02.25.432866), 1–15.

Destiningrum, M., & Adrian, Q. J. (2017). Sistem Informasi Penjadwalan Dokter Berbassis Web Dengan Menggunakan Framework Codeigniter (Studi Kasus: Rumah Sakit Yukum Medical Centre). *Jurnal Teknoinfo*, *11*(2), 30. https://doi.org/10.33365/jti.v11i2.24

Febriana, I., & S, G. A. (2017). Penerapan Teknik Kriptografi Pada Keamanan Smsandroid. *JOEICT (Jurnal of Education and Information Communication Technology)*, *1*(1), 29–36.

Han, E. S., & goleman, daniel; boyatzis, Richard; Mckee, A. (2019). Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah. *Journal of Chemical Information and Modeling*, *53*(9), 2.

Hasibuan, A. M. (2017). *Rancang Bangun Aplikasi Keamanan Data Menggunakan Metode AES Pada Smartphone*. *2*(1), 29–35.

Hulu, D., Nadeak, B., & Aripin, S. (2020). Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan. *KOMIK (Konferensi …*, *4*, 78–86. https://doi.org/10.30865/komik.v4i1.2590

Ismail, Syahrir, M. (2021). Sistem keamanan pesan email menggunakan algoritma kriptografi klasik. *Jurnal Ilmiah Sistem Informasi Dan Teknik Informatika "JISTI," 4*(1), 47–57.

Karman, J., Nurhasan, A., Studi, P., Informasi, S., & Insan, U. B. (2019). *PERANCANGAN SISTEM KEAMANAN DATA INVENTORY BARANG DI TOKO NANDA BERBASIS WEB MENGGUNAKAN METODE KRIPTOGRAFI VIGENERE CIPHER*. *11*(01), 29–36.

Lestari, A., Coyanda, J. R., & Dasrial, 2015. (2015). Sistem Infomasi Pelelangan Barang Secara Online Pada PT . Pegadaian (Persero) Unit Pelayanan Cabang Pasar 26 ILIR Palembang. *Jurnal Informatika Global*, *6*(1), 8–12.

Nawassyarif, M. Julkarnain, & Rizki Ananda, K. (2020). Sistem Informasi Pengolahan Data Ternak Unit Pelaksana Teknis Produksi Dan Kesehatan Hewan Berbasis Web. *Jurnal Informatika, Teknologi Dan Sains*, *2*(1), 32–39. https://doi.org/10.51401/jinteks.v2i1.556

Nursakti. (2019). Penerapan Aplikasi Mobile Android Sebagai Media Promosi Dan Layanan Pelanggan Pada Usaha. *Jurnal Ilmiah Sistem Informasi Dan Teknik Informatika*, *2*(2), 27–33.

Rahmat, I. (2018). Manajemen Sumber Daya Manusia Islam: Sejarah, Nilai Dan Benturan. *Jurnal Ilmiah Syi'ar*, *18*(1), 23. https://doi.org/10.29300/syr.v18i1.1568

Siregar, H. F., & Melani, M. (2019). Perancangan Aplikasi Komik Hadist Berbasis Multimedia. *Jurnal Teknologi Informasi*, *2*(2), 113. https://doi.org/10.36294/jurti.v2i2.425

Sitinjak Daniel Dido Jantce TJ, M., & Suwita, J. (2020). Analisa Dan Perancangan Sistem Informasi Administrasi Kursus Bahasa Inggris Pada Intensive English Course Di Ciledug Tangerang. *Ipsikom*, *8*(1), 1–19.

Solikhin, I., Sobri, M., & Saputra, R. (2018). Sistem Informasi Pendataan Pengunjung Perpustakaan (Studi kasus : SMKN 1 Palembang). *Jurnal Ilmiah Betrik*, *9*(03), 140–151. https://doi.org/10.36050/betrik.v9i03.40

Sun, Y. Sen, Qiu, B., & Li, Q. S. (2013). The research of negative ion test method for fabric. *Advanced Materials Research*, *756–759*(1), 138–140. https://doi.org/10.4028/www.scientific.net/AMR.756-759.138

Tahir, M. A. (2018). Implementasi Ajax Pada Aplikasi Index Artikel Berbasis Web. *Jurnal Ilmiah Sistem Informasi Dan Teknik Informatika*, *1*(2), 60–68.

Tulloh, A. R., Permanasari, Y., Harahap, E., Matematika, P., Matematika, F., Ilmu, D., & Alam, P. (2016). Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen Cryptography Advanced Encryption Standard (AES) for File Document Encryption. *Prosiding Matematika*, *Vol 2*(1), 1–8.

Wiharto, Y., & Irawan, A. (2018). Enkripsi Data Menggunakan Advanced Encryption Standart 256. *Kilat*, *7*(2), 91–99. https://doi.org/10.33322/kilat.v7i2.352