Jurnal Pendidikan Sains dan Komputer

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1390

Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)

Muhammad Azhari[1)], Dadang Iskandar Mulyana[2)], Faizal Joko Perwitosari [3)], Firhan Ali [4)]
[1] Fisikom, Sistem Informasi, Stikom CKI, Jakarta, Indonesia
[1]1mazharii2004@gmail.com , [2]mahvin2012@gmail.com, [33]faizaljoko1@gmail.com ,
[4]firhanjazz46@gmail.com

open access

***Penulis Korespondensi**

Histori Artikel:
Submit: 2022-02-22
Diterima: 2022-03-11
Dipublikasikan: 2022-03-11

Kata Kunci:
Advanced Encryption Standard (AES), Dokumen, Dekripsi, Enkripsi,Kriptografi.

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

ABSTRAK

Ringkasan Seiring berjalannya waktu, kemajuan teknologi komputer dan telekomunikasi telah menjadi kebutuhan yang sangat berguna untuk melakukan banyak tugas dengan cepat, tepat, dan akurat. Namun, diyakini bahwa aspek keamanan data penting untuk informasi sensitif, karena juga memiliki efek negatif dari orang yang tidak berwenang menyadap data penting. Enkripsi adalah salah satu solusi atau metode keamanan data terbaik untuk menjaga kerahasiaan dan keandalan data Anda, serta dapat meningkatkan keamanan data atau informasi Anda. Kriptografi adalah bidang ilmiah yang mempelajari teknologi enkripsi data. Kriptografi dibagi menjadi dua jenis, klasik dan modern, dengan kunci simetris dan asimetris. Kunci simetris adalah Advanced Encryption Standard (AES) atau kadang disebut sebagai Rijndael. AES adalah algoritma enkripsi aman untuk melindungi data atau informasi sensitif menggunakan berbagai teknik enkripsi dan dekripsi panjang kunci seperti 128-bit, 192 bit, dan 256 bit. Pada tahun 2001, Pada proses enkripsi AES mengunakan 4 transformasi dasar dengan urutan trasformasisubbytes, shiftrows, mixcolumns, danaddroundkey. Sedangkan pada proses dekripsi mengunakan invers semua transformasi dasar pada algoritma AES kecuali addroundkey dengan urutan transformasi invshiftrows, invsubbytes, addroundkey,dan invmixcolumns. Proses enkripsi diawali dengan menentukan plaintext dan key nya. Selanjutnya dilakukan beberapa trnsformasi dasar seperti subbytes, shiftrows, mixcolumns, danaddroundkey. Akan tetapi ketika melakukan trasformasi data yang diproses pada setiap trasformasi berupa data biner dari heksadesimal. Kriptografi AES memiliki ruang kunci yang untuk digunakan sehingga terhindar dari pencurian data.

LATAR BELAKANG

Perkembangan teknologi terkini telah memungkinkan orang untuk berkomunikasi dan bertukar data dan informasi tanpa batasan jarak atau waktu. Dengan meningkatnya tuntutan keamanan atas kerahasiaan informasi yang dipertukarkan, maka tuntutan akan ketersediaan data dan sistem keamanan informasi yang lebih baik untuk melindungi data dari ancaman pencurian data. Oleh karena itu, pengembangan metode pembelajaran ilmiah.Untuk melindungi data merupakan dampak positif dari adanya sistem keamanan untuk melindungi data yang dikirimkan melalui jaringan komunikasi.

Desa Chipinan Kabupaten Majalengka, Provinsi Rajagal Permasalahannya adalah belum tersedianya sistem keamanan untuk membackup data. Oleh karena itu, masih relatif mungkin bagi

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

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1390

seseorang yang tidak memiliki wewenang untuk menyajikan presentasi untuk mengubah atau mengedit data penting. Termasuk tanggal seleksi peserta JAMKESMAS. Selama ini aparat desa hanya mengandalkan mirrored data backup system untuk data yang tersimpan di media penyimpanan, sehingga bisa terus melakukan verifikasi kehandalan data. Selain itu, orang yang tidak berwenang dapat memodifikasi file teks/dokumen penting yang tersimpan di komputer Anda.

Adapun tujuan dari penelitian ini yaitu mengetahui konsep kriptografi untuk pengamanan data berbasis text dengan menggunakan algoritma AES. Algoritma AES dipilih karena kemampuannya dalam mengenkripsi dan mendekripsikan data dengan panjang kunci yang bervariasi yaitu 128 bit, 192 bit, dan 256 bit dan perbedaan panjang kunci ini yang nantinya mempengaruhi jumlah putaran pada algoritma AES [1] Pengamanan file dengan menggunakan teknik kriptografi telah banyak dilakukan dalam berbagai penelitian. Tampaknya implementasi yang hanya menggunakan algoritma kriptografi telah ditinggalkan dan beralih menggunakan kombinasi asimetri dan simetri. Dalam penelitian ini, Anda akan membuat aplikasi untuk mengenkripsi dokumen dan pesan teks menggunakan algoritma Advanced Encryption Standard (AES).

AES adalah algoritma simetris yang digunakan sebagai algoritma enkripsi dan dekripsi dokumen. Implementasi algoritma AES juga dilakukan untuk mengenkripsi dan mendekripsi proses enkripsi email. Penyelidikan telah menunjukkan bahwa pesan email dapat diambil oleh pengguna lain, tetapi lebih aman saat mengirim dan menerima email. Teks yang ditampilkan berbentuk heksadesimal dalam format karakter dan muncul sebagai simbol yang tidak jelas saat digunakan sebagai string dan belum terbaca [2]. Algoritma AES digunakan dalam penelitian ini karena memiliki kecepatan enkripsi dan dekripsi, analisis statistik, dan perhitungan error. Selain itu, algoritma AES tidak memiliki analisis histogram dan analisis statistik menyerang menggunakan koefisien korelasi [3].Berdasarkan uraian diatas,maka penulis mengkaji secara mendalam terkait "**Implementasi Pengamanan Data Pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)**".

STUDI LITERATUR

Kriptografi.

Kriptografi adalah ilmu menjaga kerahasiaan pesan dengan cara menyandikannya dalam bentuk yang tidak dapat dipahami lagi. Dalam kriptografi terdapat dua proses yaitu enkripsi dan dekripsi. Pesan terenkripsi disebut plaintext. Disebut demikian karena informasi ini dapat dengan mudah dibaca dan dipahami oleh siapa saja. Algoritma yang digunakan untuk mengenkripsi dan mendekripsi plaintext melibatkan penggunaan beberapa bentuk kunci. Pesan eksplisit dengan ciphertext disebut ciphertext. Dalam pengkodean, kita sering menemukan istilah yang berbeda. Beberapa istilah yang perlu diketahui adalah:berbeda. Beberapa istilah yang perlu diketahui adalah:

1. Message, plaintext dan ciphertext Pesan adalah data atau informasi yang dapat dibaca dan dipahami dengan sendirinya. Nama lain dari pesan tersebut adalah (clear text) atau teks yang jelas (clear text).

2. Pengirim dan penerima Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim adalah entitas yang mengirimkan pesan ke entitas lain. Penerima adalah entitas yang menerima pesan.

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

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1390

3. Enkripsi dan Dekripsi Proses penyandian plainteks menjadi cipherteks dikenal dengan istilah enkripsi (enkripsi) atau enkripsi (nama standar ISO 74982). Sementara prosedur mengembalikan ciphertext ke plaintext, awalnya disebut dekripsi atau dekripsi (nama standar menurut ISO 74982).

4. Kriptografi dan Kunci Algoritme kriptografi disebut juga dengan kriptografi, yaitu aturan-aturan untuk enkripsi, dekripsi, dan atau fungsi matematis antara keduanya yang digunakan untuk enkripsi dan dekripsi. Beberapa cipher memerlukan algoritma yang berbeda untuk enkripsi dan dekripsi. Konsep matematika dasar dari algoritma kriptografi adalah hubungan antara dua himpunan yang berisi elemen plaintext dan himpunan yang berisi sandi. Enkripsi dan dekripsi adalah fungsi yang memetakan item antara dua set. [4]

Sejarah Kriptografi

Sejarah kriptografi sebagian besarmerupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (transposition cipher) dan algoritma substitusi (substitution cipher). Ciphertransposisi mengubah susunan huruf-huruf di dalam pesan, sedangkan ciphersubstitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain.[4]

***Advanced Encryption Standard* (AES)**

Pada tahun 1997 kontes pemilihan suatu standar algoritma kriptografi baru pengganti DES dimulai dan diikuti oleh 21 peserta dari seluruh dunia. Setelah melewati tahap seleksi yang ketat, pada tahun 1999 hanya tinggal 5 calon yaitu algoritma Serpent (Ross Anderson-University of Cambridge, Eli Biham-Technion, Lars Knudsen-University of California San Diego), MARS (IBM Amerika), Twofish (Bruce Schneier, John Kelsey, dan Niels Ferguson-Counterpane Internet Security Inc, Doug Whiting-Hi/fn Inc, David Wagner-University of California Berkeley, Chris Hall-Princeton University), Rijndael (Dr. Vincent Rijmen-Katholieke Universiteit Leuvendan Dr. Joan Daemen-Proton World International), dan RC6 (RSA Amerika). Setahun kemudian pada tahun 2000, algoritma Rijndael terpilih sebagai algoritma kriptografi yang selain aman juga efisien dalam implementasinya dan dinobatkan sebagai AES. Nama Rijndael sendiri berasal dari gabungan nama penemunya.[4]

Keamanan

Masalah keamanan merupakan salah satu aspek yang penting dari sebuah sistem informasi. Masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila menggangu performansi dari sistem,seringkali keamanan dikurangi atau ditiadakan (Dowd & McHenry, 1998: 24-28) yang dikutip oleh Rahardjo. Pengelolaan terhadap keamanan dapat di lihat dari sisi pengelolaan resiko (*risk management*). Lawrie Brown dalam (Lee, 2000) yang dikutip oleh Rahardjo menyarankan menggunakan "*Risk Management Model*" untuk menghadapi ancaman (*managing threats*). Ada tiga komponen yang memberikan kontribusi kepada *Risk*, yaitu *Asset, Vulnerabilities, dan Threats*.[5]

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

Jurnal Pendidikan Sains dan Komputer

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1390

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. Awal nya ukuran kunci sandi DES yaitu 56 bit sudah cukup pada saat algoritma ini dibuat, namun,dengan meningkatnya kemampuan komputasi serangan brutal telah mungkin terjadi.[6]

METODE

Metode Pengumpulan Data

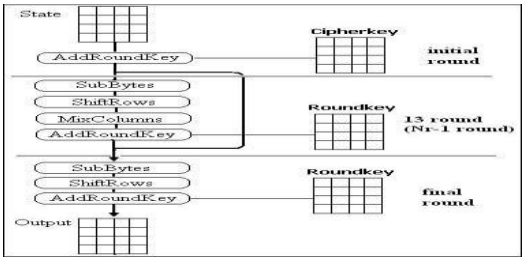
Penelitian ini menggunakan metode penelitian terapan, dimana jenis penelitian bertujuan untuk memberikan solusi praktis terhadap permasalahan tertentu. Penelitian ini tidak menitikberatkan pada pengembangan ide, teori atau ide apapun tetapi pada penerapan penelitian dalam kehidupan sehari-hari, dimana ciri utama penelitian ini adalah tingkat abstraksinya rendah, dan manfaat atau efeknya dapat dirasakan secara langsung.didasarkan pada asumsi dasar bahwa AES merupakan kelanjutan dari algoritma enkripsi Data Encryption Standard (DES) yang masa berlakunya dianggap telah habis karena faktor keamanan, apalagi kriteria pemilihan AES didasarkan pada 3 kriteria utama yaitu keamanan , harga dan karakteristik algoritma serta implementasinya [7].

Rancangan Aplikasi

Dalam penelitian ini penulis menggunakan gambaran berupa proses enskripsi AES dapat digambarkan seperti Gambar 1 [8]. Berdasarkan anggapan dasar tersebut, maka penulis dapat menyimpulkan hipotesis bahwa jika implementasi enkripsi dan dekripsi AES diterapkan maka keamanan data informasi peserta seleksi jamkesmas yang ada akan lebih maksimal dan lebih aman. Karena AES menggunakan kunci internal yang berbeda-beda, maka proses perputaran enkripsi dan dekripsi AES-128 akan dikerjakan sebanyak 10 kali, sedangkan pada proses enkripsi dan dekripsi AES-192 proses putaran akan dikerjakan 12 kali, dan untuk AES-256 proses putaran akan dikerjakan 14 kali[9]. .

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

Jurnal Pendidikan Sains dan Komputer
Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1390



Gambar 1. Proses enkripsi AES

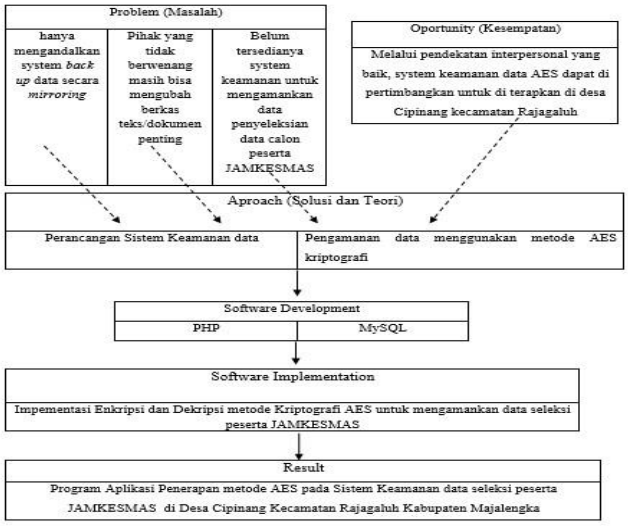
Kerangka berfikir penelitian

Berdasarkan gambar 2, penulis coba untuk menganalisis beberapa temuan yang di peroleh pada lokasi penelitian yaitu di Desa Cipinang Kecamatan Rajagaluh Kabupaten Majalengka. Setelah dilakukan studi pendahuluan melalui observasi dan wawancara dengan bagian arsip, serta manganalisis sumber data yang di peroleh pada lokasi penelitian, maka di temukan beberapa permasalahan yaitu:

1. Permasalahan yang terdapat pada desa yaitu hanya mengandalkan system *back up* data secara *mirroring*. Sehingga kesempatan atau peluang penyalahgunaan data atau edit data penting masih tergolong tinggi.

2. Permasalahan selanjutnya yaitu pihak yang berwenang masih bisa dengan bebas mengubah berkas teks / dokumen penting yang terdapat di desa.

3. Belum tersedianya system keamanan data untuk mengamankan data penyeleksian calon peserta JAMKESMAS.



Gambar 2. Kerangka berfikir penelitian

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

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1390

HASIL

No	Pengujian	Keterangan
1	Form login	Valid
2	Form enkripsi data	Valid
3	Form dekripsi	Valid
4	Form rekam jejak	Valid

PEMBAHASAN

Rancangan Aplikasi

. Tampilan form login



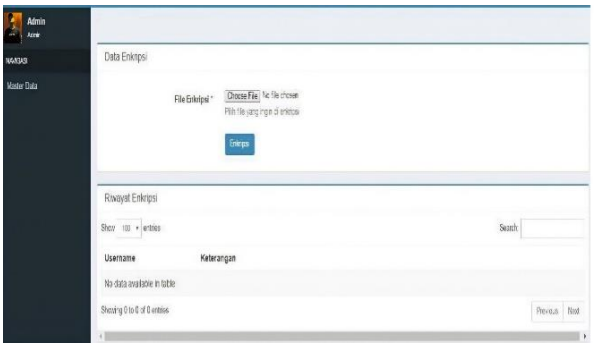
Gambar 1 Form login.

Karna data yang ingin di enkripsi atau di dekripsi masih berbentuk database. Maka pertama yang dilakukan yaitu men-export dahulu data dari database yaitu dengan cara masuk terlebih dahulu ke dalam PhpMyAdmin lalu pilih database mana yang ingin di export. Selanjutnya untuk dapat melakukan enkripsi dan dekripsi data, admin/user harus masuk terlebih dahulu kedalam aplikasi AES dengan mengisikan username dan password yang telah tervalidasi.

Tampilan Form enkripsi

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

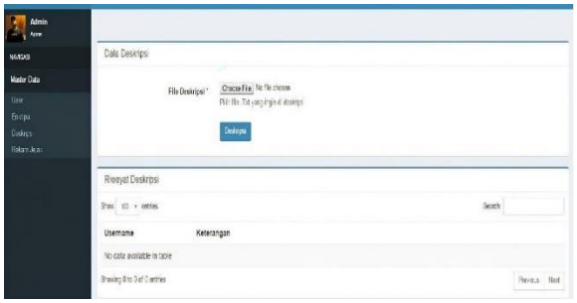
Jurnal Pendidikan Sains dan Komputer
Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1390



Gambar 2. Form enkripsi

untuk proses enkripsi ini terdapat pada Gambar 2. Choose file digunakan untuk pemilihan data yang akan dienkripsi

Tampilan Form dekripsi



Gambar 3. Form dekripsi

Sedangkan implementasi untuk proses dekripsi ini terdapat pada Gambar 3. Choose file digunakan untuk pemilihan data yang akan didekripsi.

Tampilan Form rekam jejak



Gambar 4. Form rekam jejak

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

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1390

Karena data seleksi peserta JAMKESMAS ini termasuk kedalam data yang penting, maka peneliti menambahkan menu rekam jejak untuk melihat rincian aktivitas user yang telah melakukan enkripsi maupun dekripsi data.

KESIMPULAN

Pada kesimpulan mengenai penulisan yang berjudul "**Implementasi Pengamanan Data Pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)**", Berdasarkan hasil peneltian tersebut dapat dismpulkan keamanan pada data atau dokumen hasil seleksi para peserta JAMKESMAS sehingga dapat lebih maksimal karena data yang di simpan telah terenkrpsi dan hanya bisa dilihat keaslian file tersebut jika file tersbut telah di deskripsi.selain file yang sudah di enkripsi maka akan berubah ekstensi menjadi "AES" dan file yang sudah di dekripsi akan kembali menjadi ekstensi seperti semula tanpa mengubah file keaslian data tersebut. Diharapkan dengan dibuatnya system keamanan data ini dapat menyelesaikan permasalahan yang ada sehingga membantu pihak desa dalam mengamankan datadata penting contohnya yaitu data seleksi peserta JAMKESMAS.

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

[1] Bhaudhayana, G.W., Widiartha, I.M., 2015, Implementasi Algoritma Kriptografi AES 256 dan Metode Stganografi LSB Pada Gambar Bitmap, Jurnal Ilmiah Ilmu Komputer Universitas Udayana,Vol.8 No.2 September, pp. 15-25, [online] Available : https://ojs.unud.ac.id/index.php/jik/article/view/18360/11888

[2] Rosyadi, Ahmad., 2012, Implementasi Algoritma Kriptografi AES Untuk Enkripsi Dan Dekripsi Email, Jurnal Transient, Volume 1 No 3, pp.63-67, [online] Available : https://ejournal3.undip.ac.id/index.php/transient/article/view/19/1807

[3] Wahyu, M.A., 2018, Perbandingan Enkripsi Citra Digital Dengan Menggunakan Algoritma AES, RSA, dan Chaos, Skripsi, Program Studi Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta

[4] F. Nandar Pabokory, I. Fitri Astuti, and A. Harsa Kridalaksana, "IMPLEMENTASI KRIPTOGRAFI PENGAMANAN DATA PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD," 2015.

[5] D. I. Mulyana, S. Tinggi, I. Komputer, and C. Karya Informatika, "KAJIAN PENERAPAN ENCODE DATA DENGAN BASE64 PADA PEMROGRAMAN PHP," Jurnal CKI On SPOT, vol. 9, no. 1, 2016.

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

Jurnal Pendidikan Sains dan Komputer
Volume 2, Number 1, February 2022
e-ISSN: 2809-476X
https://doi.org/10.47709/jpsk.v2i1.1390

[6] E. D. Saragih, N. A. Hasibuan, and ..., "Implementasi Algoritma Triple Des Dan Algoritma Advanced Encryption Standard Dalam Penyandian File Teks," *Inf. dan …*, vol. 6, pp. 29–35, 2019, [Online]. Available: https://www.ejurnal.stmik-budidarma.ac.id/index.php/inti/article/view/1015.

[7] I. R. M. Adi Akbar, Ilhamsyah, "Jurnal Coding Sistem Komputer Untan," *J. Coding Sist. Komput. Untan*, vol. 04, no. 2, pp. 184–194, 2016. Guritno, Suryo., Sudaryono., Untung. Rahardja., 2011, Theory and Application Of IT Research : Metodologi Penelitian Teknologi Informasi, Andi : Yogyakarta

[8] Sadikin, Rifki., 2010, Kriptografi untuk Keamanan Jaringan dan Implementasinya Dalam Bahasa Java, Andi : Yogyakarta 108.

[9] Udayana, I.PA.E.D., Sastra, N.P., 2016, Perbandingan Performansi Pengamanan File Backup LPSE Menggunakan Algoritma DES dan AES, Jurnal Teknologi Elektro, volume 15 Nomor 01 Januari, pp.111-117, [online]Available:https://ojs.unud.ac.id/index.php/JTE/article/view/20966/14139

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