PISCES
Progressive Information, Security, Computer, and Embedded System

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023

Peningkatan Keamanan Dokumen terhadap Serangan Trojan Berbasis Algoritma AES-192 (Advanced Encryption Standard)

[1]Irmayana Sunarti

[1]Universitas Negeri Makassar, Jl. A.P. Pettarani, Kota Makassar, Sulawesi Selatan, Indonesia

Email: irmayana1528@gmail.com[1]

Received : 22 Juli 2023
Accepted : 30 Agustus 2023
Published : 25 September 2023

ABSTRAK

Keamanan dokumen merupakan perlindungan informasi yang terkandung dalam dokumen dari ancaman dan risiko yang mungkin timbul, baik dari serangan fisik maupun serangan siber, salah satunya serangan trojan. Algoritma adalah salah satu solusi atau metode pengamanan dokumen yang tepat untuk menjaga kerahasiaan dan keaslian dokumen, serta dapat meningkatkan aspek keamanan suatu dokumen atau informasi. Algoritma yang digunakan dalam peningkatan keamanan dokumen untuk melakukan proses enkripsi dan dekripsi dokumen adalah algoritma AES-192 bit (*Advanced Encryption Standard*). Metode yang digunakan adalah metode waterfall yang terdiri dari studi literatur, analisis sistem, desain sistem, implementasi dan pengujian. Aplikasi yang dihasilkan adalah aplikasi enkripsi dan dekripsi AES menggunakan metode algoritma AES-192 berbasis web. Aplikasi ini ditujukan untuk mengamankan dokumen dengan format: .docx, .xls, .xlsx, .pdf dan .text. Hasil penelitian dapat disimpulkan bahwa peningkatan keamanan data menggunakan algoritma AES-192 berhasil. Proses enkripsi dilakukan untuk menghasilkan data yang tidak mudah dibaca dan tidak mudah diretas oleh orang lain kecuali mereka memiliki kunci untuk mendekripsi data tersebut. Kunci yang digunakan untuk mengenkripsi dan mendekripsi sama. Jika kunci yang digunakan sama maka data dapat digunakan, tetapi jika berbeda maka hasilnya tidak akan terbaca.

Kata Kunci: Keamanan Dokumen, AES-192, Enkripsi, Dekripsi, Trojan

ABSTRACT

Document security is the protection of information contained in documents from threats and risks that may arise, both from physical attacks and cyber attacks, one of which is a trojan attack. An algorithm is a solution or method of document security that is appropriate for maintaining the confidentiality and authenticity of documents, and can improve the security aspects of a document or information. The algorithm used in enhancing document security to encrypt and decrypt documents is the AES-192bit algorithm (Advanced Encryption Standard). The method used is the waterfall method which consists of literature studies, system analysis, system design, implementation and testing. The resulting application is an AES encryption and decryption application using the web-based AES-192 algorithm method. This application is intended to secure documents in the following formats: .docx, .xls, .xlsx, .pdf and .text. The results of the study can be concluded that increasing data security using the AES-192 algorithm is successful. The encryption process is carried out to produce data that is not easy to read and not easily hacked by others unless they have the key to decrypt the data. The key used to encrypt and decrypt is the same. If the key used is the same then the data can be used, but if it is different then the result will not be read.

Keywords: Document Security, AES-192, Encryption, Decryption, Trojan

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023

1. PENDAHULUAN

Seiring dengan perkembangan teknologi seperti sekarang ini, keamanan dokumen sangatlah penting dalam melindungi informasi dari serangan yang tidak diinginkan. Pengamanan dokumen dilakukan untuk menjaga kerahasiaan, keutuhan, keabsahan dan ketersediaan data. Teknik yang digunakan untuk mengamankan data dengan cara mengenkripsi data, membatasi akses terhadap data, dan menjaga integritas data agar tidak rusak atau terhapus. Bentuk dari enkripsi data yaitu dengan membuat data asli menjadi dimanipulasi sehingga data tersebut bisa menjadi data rahasia. Dan untuk mengembalikan atau mengubah data rahasia ke data asli dengan dilakukan dekripsi data (Ravida & Santoso, 2020).

Berbagai jenis ancaman terhadap keamanan data yang sering muncul salah satunya adalah serangan trojan yang dapat merusak, mencuri, atau memodifikasi data tanpa sepengetahuan pengguna (Gunawan, 2021). Trojan sebagai salah satu malware yang sangat berbahaya karena bisa menimbulkan banyak kerugian seperti dengan melakukan pencurian data dan melakukan pengubahan akses ke device pengguna. Trojan bisa masuk ke dalam data melalui berbagai cara, seperti email palsu, unduhan berbahaya, atau lewat celah keamanan pada sistem. Oleh karena itu, dibutuhkan suatu sistem yang dapat mencegah serangan Trojan dan menjaga keamanan data dari serangan tersebut.

Untuk meningkatkan keamanan data maka teknik atau cara yang dilakukan adalah melalui penggunaan algoritma AES (*Advanced Encryption Standard*) (Widodo & Purnomo, 2020). AES adalah algoritma enkripsi simetris yang memiliki tingkat keamanan yang tinggi dan sering digunakan dalam berbagai aplikasi untuk mengamankan data (Gunawan, 2021). Algoritma AES sebagai algoritma enkripsi yang aman untuk mengamankan data. Algoritma AES sebagai algoritma enkripsi yang aman untuk melindungi data dan informasi sensitif. Dirilis oleh NIST (*National Institute of Standards and Technology*) pada tahun 2001, AES digunakan untuk menggantikan algoritma DES, yang dianggap lebih tua dan lebih mudah untuk diretas (Pariddudin & Syauqi, 2020). Jumlah putaran yang dilakukan oleh AES tergantung pada ukuran kunci yang digunakan. Misalnya, jika ukuran kunci adalah 128, ukuran blok tetap 128 bit berarti 10 putaran, 192 bit berarti 12 putaran, dan 256 bit berarti 14 putaran. Algoritma AES-128 adalah jenis enkripsi simetris. Ini berarti menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi informasi. Selain itu, pengirim dan penerima data memerlukan salinan data untuk mendekripsinya (Ardian & Pramusinto, 2022).

Pada algoritma AES ini sebagai teknik penyembunyian data rahasia ke dalam sebuah wadah (media) sehingga data yang disembunyikan sulit untuk dikenali oleh indera manusia (Nahar Mardiyantoro & Listiani, 2021). Tidak seperti Rijndael yang block dan kuncinya dapat berukuran kelipatan 32 bit dengan ukuran minimum 128 bit dan maksimum 256 bit (Hartato et al., 2020). Berdasarkan ukuran block yang tetap, AES bekerja pada matriks berukuran 4x4 di mana tiap-tiap sel matriks terdiri atas 1 *byte* (8 bit) (Aria et al., 2023). Algoritma AES telah terbukti tangguh dan aman dalam melindungi data dari serangan trojan dan analisis kriptografi yang canggih. Dengan penggunaan AES untuk yang dapat mencegah dokumen dari serangan trojan yang dapat membahayakan kerahasiaan dan integritas data (Cristy & Riandari, 2021).

Penelitian ini akan membahas tentang bagaimana penggunaan algoritma AES dapat meningkatkan keamanan data terhadap serangan Trojan. Tujuan dari penelitian ini adalah untuk mengembangkan sistem keamanan yang dapat melindungi data dari serangan trojan dan menguji kinerja sistem tersebut dalam mengamankan data. Dengan algoritma AES dapat dilakukan sistem keamanan yang efektif untuk mencegah serangan Trojan.

2. STUDI LITERATUR

Pada algoritma AES ini sebagai teknik penyembunyian data rahasia ke dalam sebuah wadah (media) sehingga data yang disembunyikan sulit untuk dikenali oleh indera manusia (Nahar Mardiyantoro & Listiani, 2021). Tidak seperti Rijndael yang block dan kuncinya dapat berukuran kelipatan 32 bit dengan ukuran minimum 128 bit dan maksimum 256 bit (Hartato et al., 2020). Berdasarkan ukuran block yang tetap, AES bekerja pada matriks berukuran 4x4 di mana tiap-tiap sel matriks terdiri atas 1 byte (8 bit) (Aria et al., 2023). Algoritma AES telah terbukti tangguh dan aman dalam melindungi data dari serangan trojan dan analisis kriptografi yang canggih. Dengan penggunaan AES untuk yang dapat mencegah dokumen dari serangan trojan yang dapat membahayakan kerahasiaan dan integritas data (Cristy & Riandari, 2021).

Dalam pengamanan dokumen menggunakan algoritma AES ini memiliki beberapa tantangan terhadap penelitian sebelumnya tentang implementasi dalam pembuatan aplikasi algoritma AES. Dalam penelitian yang berjudul "*Advanced Encryption Standard* (AES) 128 Bit untuk Keamanan Data *Internet of Things* (IoT) Tanaman Hidroponik" dapat disimpulkan bahwa algoritma AES cocok untuk diterapkan dalam mengamankan data yang terdapat pada sistem/database (Ravida & Santoso, 2020). Proses enkripsi dilakukan untuk menghasilkan data yang

tidak mudah dibaca dan tidak mudah diretas oleh orang lain kecuali mereka memiliki kunci untuk mendekripsi data tersebut. AES telah terbukti efektif dalam melindungi data dari serangan dan pemecahan oleh pihak yang tidak berwenang. Terkait dengan algoritma AES dalam pengamanan dokumen telah dilakukan dengan menggunakan steganografi yang dikombinasikan dengan algoritma AES-128 menghasilkan efektif dalam pengiriman pesan file rahasia cukup baik dalam keamanan sistem informasi (Fatma et al., 2020). Algoritma AES-192 merupakan algoritma *Advanced Encryption Standard* (AES) yang sebagai literasi atau lanjutan dari algooritma AES-128 yang memiliki 12 round.

Dalam penelitian yang berjudul "Modifikasi Enkripsi dan Dekripsi AES dengan *Polybius Chiper* dalam Pengamanan Data" dapat disimpulkan bahwa performa waktu enkripsi dan dekripsi yang dimiliki untuk masingmasing AES modifikasi membutuhkan waktu yang relative lama dibandingkan AES standar dikarenakan komplekasitas algoritma yang digunakan mempengaruhi waktu komputasi. AES menggunakan teknik enkripsi simetris, di mana kunci yang sama digunakan untuk mengenkripsi dan mendekripsi data (Permatasari et al., 2020). Algoritma ini memiliki tiga variasi kunci, yaitu AES-128, AES-192, dan AES-256, yang masing-masing menggunakan kunci dengan panjang yang berbeda. Semakin panjang kunci yang digunakan, semakin tinggi tingkat keamanannya. Penggunaan algoritma AES dalam mengamankan data telah dilakukan berbagai bentuk seperti dengan berbasis android mmaupun berbasis website (Bimantoro & Sari, 2022).

Dalam penelitian yang berjudul "Penerapan Algoritma AES (*Advance Encryption Standart*) 128 untuk Enkripsi Dokumen di PT. Gunung Geulis Elok Abadi" dapat disimpulkan bahwa dengan adanya aplikasi enkripsi – dekripsi file menggunakan algoritme AES-128 dapat meningkatkan keamanan dokumen dari serangan pihak lain (Ignasius & Shaka Yudha Sakti, 2022). AES didesain berdasarkan dengan kunci yang digunakan pada proses enkripsi harus sama dalam melakukan proses dekripsi. Penggunaan kunci pada AES sangat berpengaruh dalam pengaman data (Fitriani & Utomo, 2020). Pada penelitian yang berjudul "Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES dari Serangan Brute Force" dapat disimpulkan bahwa pengamanan file data dengan metode algoritma AES dapat bekerja dan berproses secara optimal dalam melakukan pengamanan file data (Gunawan, 2021). AES-192 merupakan algoritma yang digunakan dalam enkripsi dan dekripsi dokumen menggunakan kunci dengan panjang 192 bit, yang lebih panjang dibandingkan dengan AES-128 namun lebih pendek dibandingkan dengan AES-256. Penelitian menunjukkan bahwa menggunakan kunci dengan panjang 192 bit meningkatkan kompleksitas algoritma enkripsi dan membuatnya lebih sulit untuk dipecahkan oleh serangan brute force atau serangan kriptanalisis lainnya (Sitorus et al., 2020). AES-192 memberikan tingkat perlindungan yang baik terhadap serangan yang umumnya digunakan oleh penyerang untuk mencoba mendapatkan akses tidak sah ke data yang dienkripsi.

3. METODE

3.1 Alur Penelitian

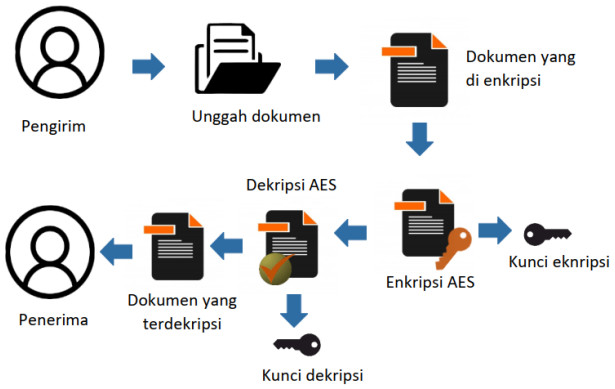
Alur penelitian yang digunakan dalam pengembangan algoritma AES-192 bit menggunakan metode waterfall. Adapun tahapan dari penelitian yang dilakukan yaitu studi literature dengan meelakukan pencarian literatur mengenai trojan dan algoritma AES untuk memahami konsep, prinsip, kelebihan, dan kekurangan masing-masing topik. Studi literatur ini sebagai landasan proses pembuatan sistem dari proses eknripsi dan dekripsi AES-192. Analisis sistem, melakukan analisis mengenai kebutuhan sistem keamanan dalam hal ini berkaitan dengan penggunaan algoritma AES untuk enkripsi dan deskripsi serta kebutuhan dalam perancangan seperti dari segi software dan hardware yang akan digunakan. Desain sistem, tahap ini dilaksanakan perancangan aplikasi sistem yang akan dibuat berdasarkan hasil analisis yang ada. Perancangan Aplikasi sistem ini meliputi desain menu utama yang terdiri dari enkripsi dekripsi file dan teks serta pemrograman. Implementasi, menerapkan sistem keamanan data yang dirancang berdasarkan desain sistem dan rancangan yang telah dibuat pada tahap sebelumnya dalam bentuk program. Pengujian, melakukan pengujian pada sistem keamanan data yang sudah diimplementasikan untuk menguji kinerja dan efektivitasnya terhadap serangan Trojan menggunakan Algoritma AES yang sudah dibuat.

3.2 Arsitektur Sistem

Sistem yang dibangun adalah sistem yang dapat melakukan proses enkripsi dan dekripsi terhadap file dokumen. Hal ini dilakukan untuk meningkatkan keamanan dokumen terhadap serangan trojan dan akses oleh orang tidak dikenal. Pada proses ini setiap file yang dilakukan enkripsi dengan algoritma AES-192 akan tidak dapat dibaca oleh pembuka biasa. Adapun bentuk proses dari arsitektur sistem yang akan dibuat dapat dilihat pada gambar 1.

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023



Gambar 1. Arsitektur Sistem

Penjelasan dari gambar 1 yaitu data yang ingin dikirimkan oleh pengirim kemudian dilakukan unggah data dari data yang sudah dikirim. Lalu proses enkripsi data menggunakan algoritma AES dengan kunci yang sama pada pengirim dan penerima data. Algoritma AES akan mengenkripsi data menggunakan kunci yang yang sudah ditentukan. Setelah data dienkripsi, hanya pengguna yang memiliki kunci yang tepat yang dapat membuka dan membaca data. Setelah data berhasil dikirim ke tujuan akhir, algoritma AES akan digunakan lagi untuk mendekripsi data tersebut menggunakan kunci yang tepat. Proses dekripsi data menggunakan algoritma AES dengan kunci yang sama pada pengirim dan penerima data. Data yang telah didekripsi dan tiba di tujuan. Setelah data berhasil didekripsi, data tersebut dapat dibaca dan diproses oleh penerima yang sah.

3.3 Algoritma AES-192

a. Proses Enkripsi

Proses Enkripsi dimulai dari *AddRoundKey*. *AddRoundKey* yaitu mengkobinasikan sebuah chiperkey dan plaintext dengan menggunakan operator XOR. Kemudian *SubBytes* adalah menukar isi matriks dengan baris dan kolom pada tabel S-Box. Yang ke tiga *ShiftRows* adalah sebuah proses melakukan pergeseran pada setiap elemen blok/tabel yang dilakukan per barisnya. Baris pertama tidak dilakukan pergeseran, baris kedua dilakukan pergeseran 1 *byte*, baris ketiga dilakukan pergeseran 2 *byte* dan baris ke-empat dilakukan pergeseran 3 *byte*. Setelah itu, M*ixColumns* adalah mengalikan tiap elemen dari Blok Chiper dengan matriks yang sudah ditentukan. Pengalian dilakukan seperti perkalian matriks biasa yaitu menggunakan Dot Product lalu perkalian keduanya dimasukkan ke dalam sebuah Blok Chiper baru. Bila sudah dikalikan semua dengan matriks yang sudah ditentukan. Maka terbentuk hasil *Polynomial* dengan bentuk biner dan hasil itu di gabungkan dengan rumus perkalian *MixColumns* pada setiap tahap perkalian matriks. Dan yang terakhir *AddRoundKey* adalah mengkombinasikan Chiperteks yang sudah ada dengan Chiperkey dihubungkan pada operator XOR sehingga terbentuk ciphertext.

b. Proses Dekripsi

Proses Dekripsi dimulai dari *InvMixColumns* yaitu setiap kolom dalam state dikalikan dengan matrik yang sudah ditentukan pada perkalian dalam AES-192, berikutnya *InvShiftRows* adalah transformasi byte yang berkebalikan dengan transformasi *ShiftRows*. Pada transformasi *InvShiftRows*, dilakukan pergeseran bit ke kanan sedangkan pada *ShiftRows* dilakukan pergeseran bit ke kiri. Yang ketiga *InvSubBytes* juga merupakan transformasi *byte* yang berkebalikan dengan transformasi *SubBytes*. Pada *InvSubBytes*, tiap elemen pada state dipetakan dengan menggunakan tabel *Inverse* S-Box dan yang terakhir *AddRoundKey* adalah mengkombinasikan chiperteks yang sudah ada dengan chiperkey dihubungkan pada operator XOR sehingga menjadi plainteks.

c. Ekpansi Kunci AES

Proses AES secara garis besar dibagi menjadi dua proses utama yaitu *Key Expansion* dan *Round Transformation*. *Key Expansion* merupakan proses dimana kunci enkripsi dibentuk kedalam blok -blok kunci putaran yang akan digunakan pada proses enkripsi dan dekripsi menggunakan *Round Transformation*. *Round Transformation* merupakan proses transformasi yang terdiri dari n-putaran. Round Transformation merupakan proses transformasi yang terdiri dari n-putaran (Haris et al., 2023).

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES
Progressive Information, Security, Computer, and Embedded System

PISCES Volume 01 Nomor 02 September 2023

Proses enkripsi algoritma AES 192 terdiri dari 4 jenis transformasi bytes, awal proses enkripsi, input yang telah disalin ke dalam state akan mengalami transformasi byte *AddRoundKey*. Setelah itu, state akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut dengan round function. Round terakhir agak berbeda dengan round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi *MixColumns* (Kurniawan & Pradana, 2022). Tahap *SubBytes* menggantikan setiap byte dalam blok dengan byte yang sesuai dari tabel substitusi. Kemudian, tahap *ShiftRows* menggeser setiap baris dalam blok ke kiri. Tahap *MixColumns* melibatkan operasi matematika pada setiap kolom dalam blok. Terakhir, tahap *AddRoundKey* melibatkan penggabungan blok dengan kunci enkripsi yang telah dijadwalkan sebelumnya. Proses dekripsi AES melibatkan langkah-langkah yang berlawanan dengan proses enkripsi. Setiap blok data yang dienkripsi akan diproses menggunakan tahap-tahap yang berlawanan dengan tahap enkripsi, yaitu InvSubBytes, InvShiftRows, InvMixColumns, dan InvAddRoundKey. Tahap-tahap ini mengembalikan blok data ke bentuk aslinya sebelum dienkripsi (Tahir et al., 2020).

Ekspansi kunci menghasilkan total Nb(Nr+1) *word*. Algoritma ini membutuhkan set awal *key* yang terdiri dari Nb *word*, dan setiap round Nr membutuhkan data kunci sebanyak Nb *word*. Hasil *key* schedule terdiri dari array 4 byte *word linear* yang dinotasikan dengan [wi]. SubWord adalah fungsi yang mengambil 4 byte *word input* dan mengaplikasikan S-Box ke tiap-tiap data 4 byte untuk menghasilkan *word output*. Fungsi RotWord mengambil *word* [a0, a1, a2, a3] sebagai input, melakukan permutasi siklik, dan mengembalikan word [a1, a2, a3, a0]. Rcon[i] terdiri dari nilai-nilai yang diberikan oleh [xi-1, {00}, {00}, {00}], dengan xi-1 sebagai pangkat dari x (x dinotasikan sebagai {02}). Pseudocode dari proses ekspansi kunci dapat dilihat dalam gambar 2.

```
AES
Nb = 4
Nk = number of doublewords in the chiper key (1, 6, 9 for AES-128, AES-192 AES-256, resp.)
Nr= number of round in the chiper (Nr = 10, 12, 14 for AES-128, AES-192 AES-256, resp.)

The keyExpantion routine
KeyExpansion (byte key[4*Nk], word[Nb*(Nr+1)], Nk)
begin
      word temp
i= 0

while (i < Nk)
      w[i] = word(key[4*i], key[4*i+2], key[4*i+3])
i = i + 1
end while

i = Nk

while (i < Nb * (Nr+1))
      temp = w[i-1]
      if (i mod Nk = 0)
            temp SubWord(RotWord(temp) xor Rcon[i/Nk])
      else if (Nk > 6 and i mod Nk = 4)
            temp = SubWord(temp)
      end if
      w[i] = w[i-Nk] xor temp
      i = i +1
      end while
end
```

Gambar 2. *Pseudocode* Ekpansi Kunci Algoritma AES

Pada gambar 2 merupakan *word* ke Nk pertama pada ekspansi kunci berisi kunci cipher. Setiap *word* berikutnya, w[i], sama dengan XOR dari *word* sebelumnya, w[i-1] dan *word* Nk yang ada pada posisi sebelumnya, w[i-Nk]. Untuk *word* pada posisi yang merupakan kelipatan Nk, sebuah transformasi diaplikasikan pada w[i-1] sebelum XOR, lalu dilanjutkan oleh XOR dengan konstanta round, Rcon[i]. Transformasi ini terdiri dari pergeseran siklik dari byte data dalam suatu *word RotWord*, lalu diikuti aplikasi dari lookup tabel untuk semua 4 byte data dari *word SubWord*.

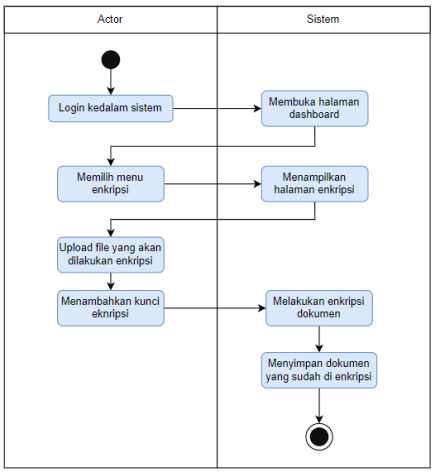
3.4 Perancangan Sistem

Pada perancangan sistem akan dibuat dengan menggunakan activity diagram. Dari diagram tersebut permodelan interaksi dari keseluruhan alur kerja sistem dapat digambarkan dengan baik. Proses pertama adalah proses enkripsi yang dimulai dengan memilih lokasi file yang akan di enkripsi, setelah itu dilanjutkan dengan memasukkan dan mengkonfirmasi kunci enkripsi. Proses kedua adalah dekripsi, pada proses ini file

E-ISSN: 2986-7258
P-ISSN : 2986-724X

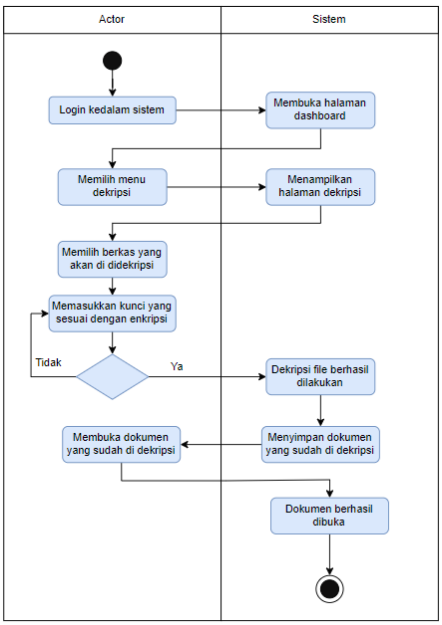
PISCES Volume 01 Nomor 02 September 2023

yang sebelumnya sudah melalui proses enkripsi dimasukkan lagi sebagai file inputan yang kemudian ditambahkan dengan kunci yang sama, hal ini diperlukan karena peran kunci adalah validasi untuk dapat melanjutkan proses dekripsi. Output dari proses ini adalah file dokumen yang telah terdekripsi. Adapun prosesnya dapat dilihat pada gambar 2 untuk proses enkripsi dan pada gambar 3 untuk proses dekripsi.



Gambar 3. Activity Diagram Enkripsi

Pada gambar 3 menjelaskan aktivitas diagram proses enkripsi berkas pada aplikasi yang akan dibuat. Dimulai oleh admin yang melakukan login kepada aplikasi, lalu admin akan melakukan upload berkas ke dalam sistem dan menambahkan kata sandi sebagai key encryption. Lalu sistem akan merubah berkas kedalam bentuk enkripsi dengan algoritma AES 192 Bit dan merubah ekstensi berkas menjadi .rda.



Gambar 4. Activity Diagram Dekripsi

Pada gambar 4 menjelaskan aktivitas diagram proses Deskripsi dokumen pada aplikasi yang akan dibuat. Dimulai oleh admin ataupun user yang melakukan login kepada aplikasi, lalu admin ataupun user memilih berkas yang akan di deskripsi dan memasukkan kata sandi yang sesuai. Jika kata sandi salah maka sistem akan menampilkan pesan kesalahan, jika kata sandi benar, maka sistem akan melakukan proses deskripsi pada

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023

berkas dan merubah ekstensi .rda ke dalam ekstensi yang sebenarnya. Setelah berkas berhasil di deskripsi, maka admin dapat membuka dokumen dari sistem dan menyimpannya pada komputer lokal.

4. HASIL DAN PEMBAHASAN

Aplikasi yang dirancang adalah sebuah aplikasi enkripsi dan dekripsi menggunakan metode *Advanced Encryption Standard* (AES-192) berbasis web. Pada aplikasi yang di rancang tersebut akan melakukan proses enkripsi dan dekripsi dokumen yang menggunakan kunci yang sama. Proses enkripsi dapat mengubah teks atau data (plaintext) menjadi teks rahasia (ciphertext), kemudian sebaliknya proses deskripsi yang dapat mengembalikan teks rahasia (ciphertext) menjadi teks atau data (plaintext) (Nuari & Ratama, 2020). Proses enkripsi dan dekripsi AES dengan panjang kunci 192 bit melibatkan lebih banyak putaran untuk meningkatkan tingkat keamanan. Namun, prinsip dasar dari algoritma AES tetap sama, yaitu membagi data menjadi blok-blok, menerapkan tahap-tahap yang sesuai, dan menggunakan kunci enkripsi yang valid (Sarah et al., 2022). Implementasi dari sistem yang dibuat akan menghasilkan dokumen yang tidak bisa dibaca oleh pihak lain karena pada prosesnya akan memiliki sebuah password yang hanya diketahui oleh orang yang berwenang sehingga dokumen yang dikirim akan aman. Dari tahap implementasi ini akan dilakukan uji coba terhadap dokumen yang akan dilakukan proses enkripsi dan dekripsi dengan menggunakan algoritma AES-192 bit.

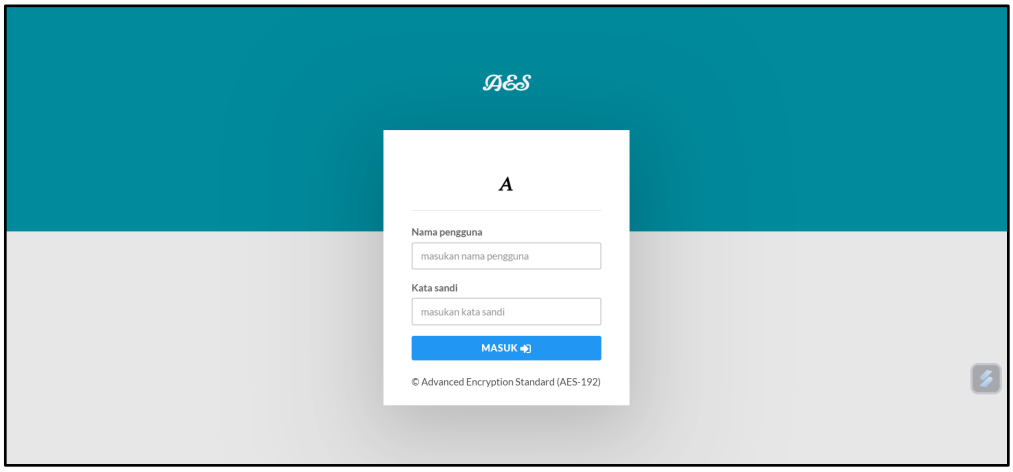
Pada tahap implementasi, maka dapat dilakukan dengan memasang aplikasi pada komputer karena hanya menggunakan web. Dalam aplikasi ini pengguna bisa melakukan enkripsi dan dekripsi file, dimana apabila user lain ingin mengambil file dokumen yang sudah terdekripsi bisa melakukan login di aplikasi sebagai user dan untuk pengambilan file menggunakan password sehingga tidak bisa diambil oleh pengguna lain yang tidak berhak. Pengujian proses enkripsi dan dekripsi dilakukan menggunakan dokumen dengan ekstensi docx, doc, xls, ppt dan pdf dengan ukuran file maksimal 3 MB. Pengujian dilakukan dengan aplikasi enkripsi dan dekripsi AES-192 melibatkan serangkaian langkah untuk memastikan bahwa implementasi algoritma AES-192 berfungsi dengan benar dan dapat melindungi data secara efektif.

4.1 Tampilan Aplikasi

Jika terdapat penomoran pada sub judul, maka gunakan huruf kecil dan abjad seperti berikut:

a. Tampilan awal aplikasi

Pada tampilan awal akan terdapat halaman login, user diminta untuk menginputkan username dan password supaya bisa menggunakan aplikasi dapat dilihat pada gambar 5.

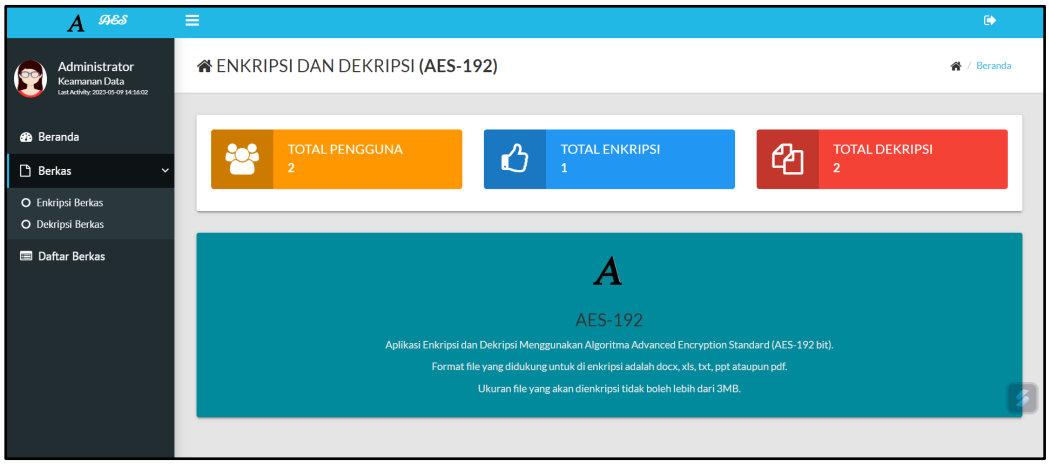


Gambar 5. Tampilan Awal

Pada gambar 5 merupakan tampilan awal dari aplikasi enkripsi dekripsi AES 192. Pada tampilan awal akan terdapat halaman login baik untuk admin maupun user. Untuk dapat menggunakan aplikasi maka admin maupun user dapat menginputkan nama pengguna dan password sehingga dapat menggunakan aplikasi.

b. Tampilan Dashboard

Pada tampilan dashboard akan terdapat menu untuk proses enkripsi, dekripsi dan daftar berkas yang dapat dilihat pada gambar 6.

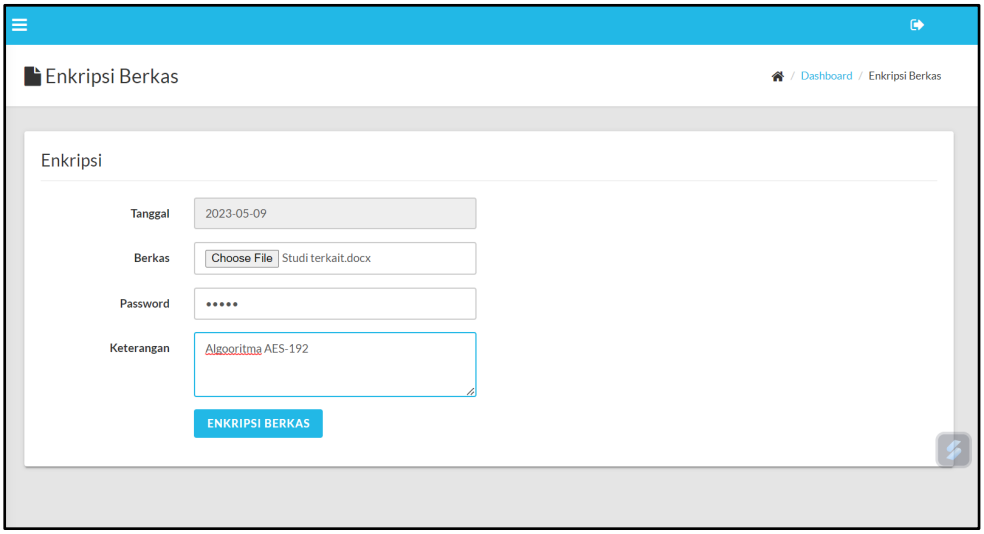


Gambar 6. Tampilan Dashboard

Pada gambar 6 merupakan tampilan dashboard dari aplikasi enkripsi dekripsi AES 192. Pada tampilan dashboard terdapat menu enkripsi berkas, dekripsi berkas, daftar berkas, total pengguna, total enkripsi dan total dekripsi. Selain itu, juga pada tampilan ini akan memberikan keterangan mengenai algoritma yang digunakan, format file yang didukung dan maksimal ukuran file yang bisa dilakukan proses enkripsi dan dekripsi.

4.2 Enkripsi Dokumen

Proses enkripsi file dokumen dapat dilakukan dengan mengupload file pada menu enkripsi yang dilakukan dengan cara pada menu enkripsi terdapat inputan file maupun password kosong maka akan muncul notifikasi untuk upload file dan password. Untuk uji coba dapat dilakukan dengan menginputkan file document dapat dilihat pada gambar 7.



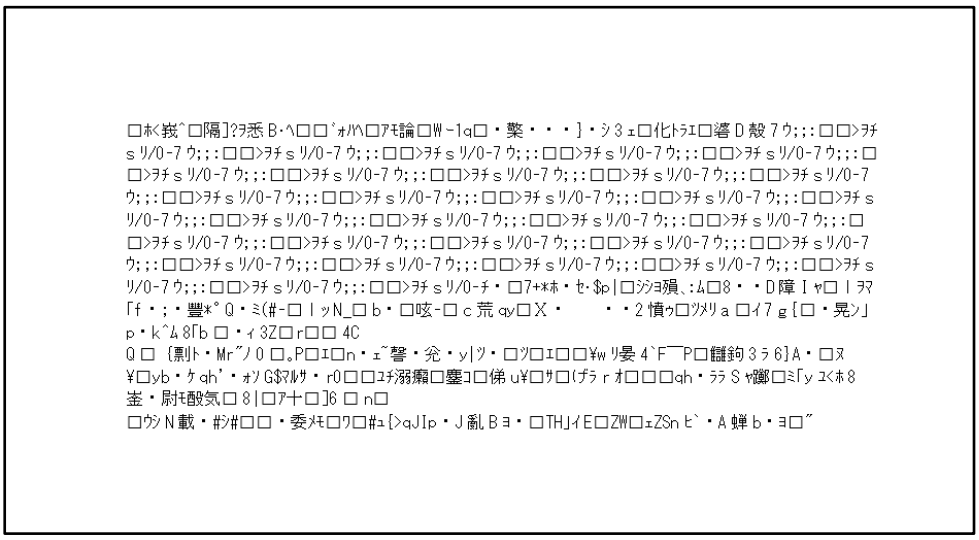
Gambar 7. Tampilan Proses Enkripsi

Pada gambar 7 merupakan tampilan proses enkripsi. Pada tampilan proses enkripsi tersebut user memasukkan file yang akan dienkripsi kemudian memasukkan password dan keterangan. Setelah itu

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023

dilakukan enkripsi berkas. Apabaila berhasil maka muncul notifikasi enkripsi berhasil dan hasilnya akan berbentuk file dengan eksitensi .rda yang dapat dilihat pada folder di komputer secara langsung. Setelah dilakukan proses enkripsi, lalu kemudian file dibuka maka hasilnya yang dapat dilihat pada gambar 8.

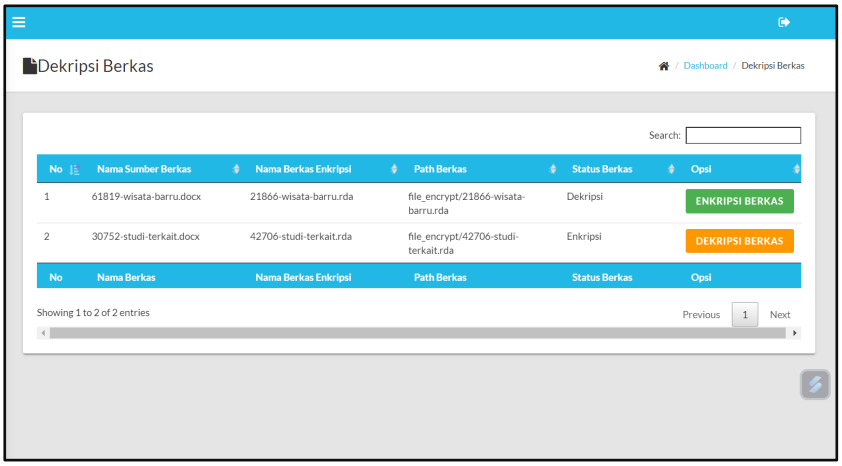


Gambar 8. Tampilan Hasil Enkripsi

Pada gambar 8 merupakan tampilan hasil enkripsi. Pada hasil enkripsi tersebut file yang dienkripsi dibuka maka hasil prosesnya isi dari file tersebut tidak bisa dibaca. Hasil proses enkripsi menghasilkan sebuah kode-kode yang tidak bisa dibaca.

4.3 Dekripsi Dokumen

Proses dekripsi file dokumen dapat dilakukan dengan masuk ke menu dekripsi, lalu klik enkripsi file, masukkan password yang sama saat melakukan proses dekripsi. Maka akan muncul gambar 9.

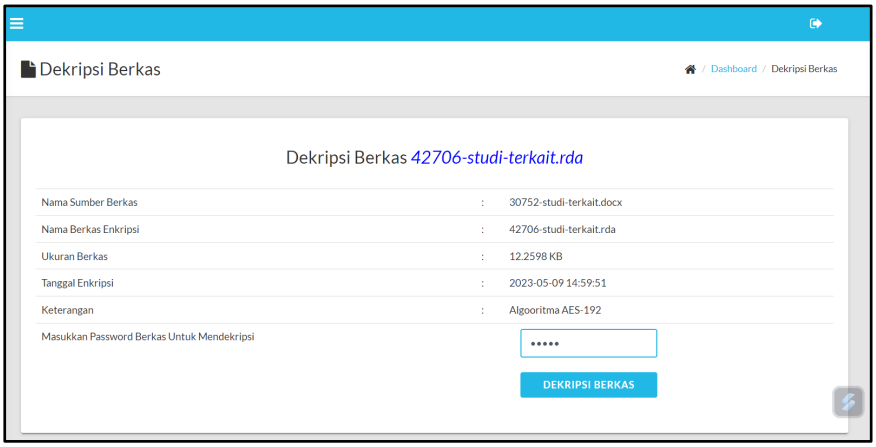


Gambar 9. Melakukan Proses Dekripsi

Pada gambar 9 merupakan tampilan melakukan proses dekripsi. Pada tampilan tersebut akan muncul file yang akan dilakukan dekripsi. Maka pada keterangan opsi pilih file yang akan didekripsi eksitensi .docx dapat dilihat pada gambar 10.

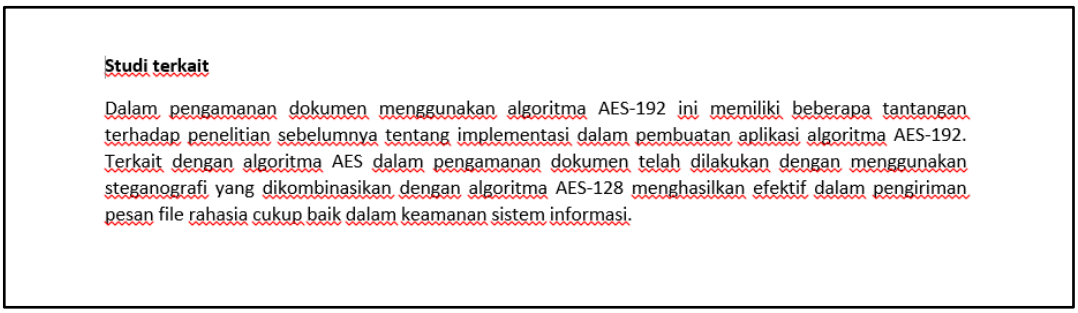
E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 01 Nomor 02 September 2023



Gambar 10. Tampilan Proses Dekripsi

Pada gambar 9 merupakan tampilan proses dekripsi. Pada tampilan dekripsi tersebut akan muncul nama file yang akan didekripsi. Untuk melakukan dekripsinya maka harus diketahui password yang digunakan. Apabila password sudah dimasukkan dan berhasil maka akan muncul notifikasi berhasil didekripsi. Setelah dilakukan proses dekripsi, lalu kemudian file dibuka maka hasilnya yang dapat dilihat pada gambar 17.



Gambar 10. Tampilan Hasil Dekripsi

Pada gambar 10 merupakan tampilan hasil dekripsi. Pada hasil dekripsi tersebut file yang didekripsi dibuka maka hasil prosesnya isi dari file tersebut dapat dibaca. Dimana pada proses dekripsi ini file hanya bisa didekripsi oleh user yang mengetahui password yang digunakan saat proses enkripsi sehingga file akan aman.

4.4 File Uji Coba Enkripsi dan Dekripsi AES-192

Untuk melakukan pengujian waktu maka akan terdapat 5 file yang akan diuji coba dengan ukuran file dan eksitensi yang berbeda. Adapun file yang akan di uji dapat dlihat pada tabel 1.

Tabel 1. File Uji Coba Enkripsi dan Dekripsi

No	Nama File	Size	Tipe File	Eksitensi
1	Perkenalan.txt	1 KB	Text Document	.txt
2	Studi terkait.docx	13 KB	DOCX Document	.docx
3	wisata barru.pdf	188 KB	Text Document	.pdf
4	Uji coba algoritma AES-192.pptx	39 KB	PPTX Presentation	.pptx
5	Tugas statistik.xlsx	11 KB	XLSX Worksheet	.xlsx

5. KESIMPULAN DAN SARAN

a. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan terkait peningkatan keamanan dokumen menggunakan aplikasi Enkripsi Dekripsi AES maka proses implementasi berhasil menggunakan algoritma Advance Encryption Standard (AES) 192 dalam proses enkripsi dan dekripsi dokumen dengan format doc, docx, xls, xlsx, pdf dan txt. Proses enkripsi dilakukan untuk menghasilkan data yang tidak mudah dibaca dan tidak mudah diretas oleh orang lain kecuali mereka memiliki kunci untuk mendekripsi data tersebut. Kunci yang digunakan untuk mengenkripsi dan mendekripsi sama. Jika kunci yang digunakan sama maka data dapat digunakan, tetapi jika berbeda maka hasilnya tidak akan terbaca. Untuk proses dekripsi digunakan kunci untuk mengembalikan dokumen ke bentuk semula sehingga dapat dibaca. Dengan adanya aplikasi pengamanan dokumen menggunakan algoritma AES-192 bit ini dapat mengamankan dokumen atau file sehingga dapat terjaga kerahasiaan data dari orang yang tidak bertanggung jawab.

b. Saran

Adapun saran dalam yang ingin disampaikan yaitu diharapkan kedepannya apluikasi Enkripsi dan Dekripsi AES-192 ini bisa dikembangkan lagi berbasis android. Penelitian selanjutnya dapat memperluas peninjauan terhadap algoritma kriptografi lainnya yang dapat meningkatkan keamanan dokumen. Dalam upaya meningkatkan keamanan dokumen, penting untuk mempertimbangkan penggunaan algoritma kriptografi yang lebih kuat dan canggih daripada AES-192. Algoritma seperti AES-256, *Twofish*, atau *Serpent* dapat memberikan tingkat keamanan yang lebih tinggi.

REFERENSI

Ardian, M. T., & Pramusinto, W. (2022). *Pengamanan Database Perpustakaan Dengan Algoritma Aes-128 Pada Sma Waskito Library Database Security With Aes-128 Algorithm on*. *September*, 248–257.

Aria, M., Widodo, A., Thasandra, M., Sutra, S. O., Nasution, A. B., Ikhwan, A., Negeri, U. I., Utara, S., William, J., Ps, I. V, Estate, M., Percut, K., Tuan, S., & Serdang, D. (2023). Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi pada E-Voting di Kota Medan dengan Menggunakan Algoritma AES. *Journal on Education*, *05*(03), 6780–6787.

Bimantoro, Y., & Sari, R. T. K. (2022). Enkripsi Data Menggunkan RSA & AES pada Aplikasi Instant Messaging Berbasis Mobile. *Jurnal Teknik Informatika*, *14*(2), 135–144. https://journal.uinjkt.ac.id/index.php/ti/article/view/23469/pdf%0A

Cristy, N., & Riandari, F. (2021). Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan. *JIKOMSI [Jurnal Ilmu Komputer Dan Sistem Informasi]*, *4*(2), 75–85. https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181%0A

Fatma, Y., Hafid, A., & Dani, H. O. (2020). Peningkatan Keamanan Pengiriman Pesan Teks: Kombinasi Advanced Encryption Standard (AES) 128 dan Least Significant Bit (LSB). *JUSIFO (Jurnal Sistem Informasi)*, *6*(2), 111–120. https://doi.org/10.19109/jusifo.v6i2.6746

Fitriani, I., & Utomo, A. B. (2020). Implementasi Algoritma Advanced Encryption Standard (AES) pada Layanan SMS Desa. *JISKA (Jurnal Informatika Sunan Kalijaga)*, *5*(3), 153–163. https://doi.org/10.14421/jiska.2020.53-03

Gunawan, I. (2021). Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force. *TECHSI - Jurnal Teknik Informatika*, *13*(1), 14. https://doi.org/10.29103/techsi.v13i1.2395

Haris, M., Lydia, M. S., & Sutarman, S. (2023). Pengamanan Pada Citra Digital dengan Menggunakan Modifikasi Blok Data Algoritma AES-Rijndael. *Jurnal Media Informatika Budidarma*, *7*(1), 444–453. https://doi.org/10.30865/mib.v7i1.5458

Hartato, E., Gunawan, I., Parlina, I., Solikhun, S., & Wanto, A. (2020). Analisis Algoritma Aes Dalam Mengamankan Data Pada Kantor Walikota Pematangsiantar. *Jurnal Ilmiah Informatika*, *8*(01), 18.

Ignasius, A., & Shaka Yudha Sakti, D. V. (2022). Penerapan Algoritma Aes (Advance Encryption Standart) 128 Untuk Enkripsi Dokumen Di Pt. Gunung Geulis Elok Abadi. *Skanika*, *5*(1), 1–10.

https://doi.org/10.36080/skanika.v5i1.2118

Kurniawan, A., & Pradana, R. (2022). *IMPLEMENTASI ALGORITMA AES DAN RC4 UNTUK IMPLEMENTATION OF AES AND RC4 ALGORITHM FOR SECURING NEW INSTALLATION CUSTOMER DATA FILES. september*, 360–367.

Nahar Mardiyantoro, & Listiani, M. (2021). Implementasi Algoritma AES Pada QR-Code Sebagai Parameter Keaslian Data Dalam Pembuatan KTA. *SATESI: Jurnal Sains Teknologi Dan Sistem Informasi*, *1*(1), 26–31. https://doi.org/10.54259/satesi.v1i1.5

Nuari, R., & Ratama, N. (2020). Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping. *Journal Of Artificial Intelligence And Innovative Applications*, *1*(2), 2716–1501. http://openjournal.unpam.ac.id/index.php/JOAIIA

Pariddudin, A., & Syauqi, F. (2020). Penerapan Algoritma AES pada QR CODE untuk Keamanan Verifikasi Tiket. *Teknois : Jurnal Ilmiah Teknologi Informasi Dan Sains*, *10*(2), 43–52. https://doi.org/10.36350/jbs.v10i2.87

Permatasari, S., Aminudin, A., & Arifianto, S. (2020). Modifikasi Enkripsi dan Dekripsi AES dengan Polybius Chiper dalam Pengamanan Data. *JRST (Jurnal Riset Sains Dan Teknologi)*, *4*(1), 41. https://doi.org/10.30595/jrst.v4i1.6208

Ravida, R., & Santoso, H. A. (2020). Advanced Encryption Standard (AES) 128 Bit untuk Keamanan Data Internet of Things (IoT) Tanaman Hidroponik. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *4*(6), 1157–1164. https://doi.org/10.29207/resti.v4i6.2478

Sarah, N. M., Nugroho, N. B., & Ristamaya, W. (2022). Implementasi Kriptografi Untuk Pengamanan Data Aset Perusahaan Pada PT. PLN (Persero) Dengan Menggunakan Metode Algoritma AES 192. *Jurnal Cyber Tech*, *x*. https://ojs.trigunadharma.ac.id/index.php/jct/article/view/1909

Sitorus, F. A., Nugroho, N. B., & Pane, U. F. S. S. (2020). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit untuk Keamanan Data Transaksi Penjualan Pada PT. Mitsubishi Electric Indonesia. *Jurnal CyberTech*, *x*, 1–15. https://ojs.trigunadharma.ac.id/

Tahir, T. Bin, Hadi Sirad, M. A., & Rais, M. (2020). Sistem Informasi Encrypt Dan Decrypt Dengan Algoritma AES Menggunakan Framework Laravel. *Patria Artha Technological Journal*, *4*(1), 41–46. https://doi.org/10.33857/patj.v4i1.326

Widodo, B. E., & Purnomo, A. S. (2020). Implementasi Advanced Encryption Standard Pada Enkripsi Dan the Implementation of Advanced Encryption Standard on the Encryption and Decryption of the Confidential Documents At. *Jurnal Teknik Informatika (Jutif)*, *1*(2), 69–77.