Jurnal SimanteC
Vol. 11, No. 2 Juni 2023 P-ISSN : 2088-2130
E-ISSN : 2502-4884

# IMPLEMENTASI KRIPTOGRAFI PADA KEAMANAN DATA MENGGUNAKAN ALGORITMA *ADVANCE ENCRYPTION STANDARD* (AES)

# *CRYPTOGRAPHIC IMPLEMENTATION IN DATA SECURITY USING ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM*

**Brikitha Olivia Putri Irine Irawan[1)], Muhlis Tahir[2)] , Nimas Ayu Windrastuti[3)] , Delsa Yurina Cholili[4)] , Dina Mulaikah[5)] , Ahmad Batsul Mushofi Septian wachid[6)]**

[1,2,3,4,5,6]Prodi Pendidikan Informatika, Fakultas Ilmu Pendidikan, Universitas Trunojoyo
Jl. Raya Telang, PO BOX 2 Kamal, Bangkalan
E-mail : [1]brikitha.olivia13@gmail.com, [2]muhlis.tahir@trunojoyo.ac.id,
[3]nimasayuwindrastuti@gmail.com, [4]delsaflk@gmail.com, [5]dinamulaika@gmail.com,
[6]wd.musofi@gmail.com

**ABSTRAK**

Keamanan adalah bagian penting dari kerangka data, sudut pandang ini seringkali cukup menonjol untuk diperhatikan oleh pemilik dan administrator kerangka data. Dalam hal ini, tim kami mengembangkan sistem informasi yang menggunakan kriptografi untuk mengamankan dokumen. Enkripsi dan deskripsi adalah dua konsep penting dalam bidang kriptografi. Untuk menjaga agar data yang tersimpan diblokir untuk pihak yang tidak disetujui maka diperlukan pengamanan data. Untuk tidak menyadap atau mencuri dokumen yang berisi data penting untuk klien dan untuk menjaga kepercayaan ini, diperlukan perhitungan yang dapat melindungi catatan, yaitu Perhitungan Enkripsi Standar Tingkat Tinggi (AES). Tujuan dari penelitian ini adalah menggunakan algoritma AES untuk menjamin keamanan data pada dokumen. Hasil penelitian ini diperoleh bahwa file atau dokumen yang melalui proses enkripsi, maka isi dari file akan berubah menjadi simbol yang tidak dapat dibaca begitu saja. Kemudian, ketika hasil enkripsi melalui proses dekripsi dengan memasukkan kunci yang digunakan pada proses enkripsi, maka isi file akan kembali seperti semula.

***Kata kunci :*** *advanced standard encryption (AES); dokumen; keamanan; kriptografi*.

***ABSTRACT***

*Security is an important part of the data framework, this viewpoint is often prominent enough to be noticed by database owners and administrators. In this case, our team develops an information system that uses cryptography to secure documents. Encryption and description are two important concepts in the field of cryptography. To keep the stored data from being blocked for unauthorized parties, data security is needed. In order not to intercept or steal documents that contain important data for clients and to maintain this trust, calculations are needed that can protect records, namely High Level Standard Encryption Computation (AES). The purpose of this study is to use the AES algorithm to ensure data security. The results of this study obtained that files or documents that go through the encryption process, the contents of the file will turn into symbols that cannot be read just like that. Then, when the encryption results go through the decryption process by entering the key used in the encryption process, the contents of the file will return to normal.*

***Keywords:*** *advanced standard encryption (AES); document; security; cryptography*.

## PENDAHULUAN

Industri 4.0 adalah masa dimana terjadi perubahan dalam aspek teknologi dan informasi yang terjadi dengan sangat cepat [1]. Globalisasi dapat berdampak pada perkembangan tersebut karena teknologi terus berkembang, termasuk komputer, dari tahun ke tahun. Komputer adalah instrumen yang memungkinkan orang mengelola data sesuai dengan protokol yang telah ditetapkan. Siapa pun yang akrab dengan terobosan ini dapat memanfaatkan komputer, baik yang berusia muda maupun tua [2].

Komputer ini memang memiliki kekurangan, salah satunya adalah kesulitan keamanan komputer, di samping kelebihannya. Keamanan komputer adalah komponen penting dari sistem data apa pun, namun sering kali keamanan komputer terganggu atau terkena bahaya yang, misalnya, menyebabkan kehilangan atau kerusakan pada data klien yang penting di komputer pelanggan itu sendiri [3]. Sejalan dengan kemudahan ini, diperlukan keamanan atas informasi dan data yang ditukarkan agar informasi dan data tidak jatuh kepada orang yang tidak berwenang. Oleh karena itu diperlukan sistem keamanan untuk menjaga informasi dan data yang ditukarkan.

Virus komputer yang dapat merusak data atau orang jahat yang sadar akan kecanggihan komputer dan dapat mencuri data dari komputer Anda hanyalah dua contoh dari sekian banyak cara yang dapat digunakan untuk menyerang keamanan komputer, seperti peretas. Penting untuk mengetahui berbagai risiko yang dapat muncul dari penggunaan internet, termasuk gangguan, penyadapan, manipulasi, dan fabrikasi [4]. Seorang programmer dapat mengambil informasi yang benar-benar dia inginkan. Tentu saja, ini memiliki efek negatif yang signifikan pada pengguna, terutama mereka yang mengandalkan komputer untuk membantu mereka dalam hal-hal yang melibatkan data perusahaan yang tersimpan di komputer. Kebocoran database Dirjen Pajak yang ditambahkan ke forum hacker menjadi salah satu kejadiannya. Ada 34 file PDF, RAR, CSV, dan ZIP dalam data yang diklaim. Kriptografi dapat menyelesaikan masalah terkait pengamanan data atau dokumen.

Teori matematika yang sering diterapkan dalam teknologi informasi adalah kriptografi. Data dapat disimpan dengan aman dengan menggunakan kriptografi untuk mencegah akses yang tidak sah ke informasi dan data. Tiga fungsi enkripsi, deskripsi, dan *key* membentuk dasar kriptografi modern [3]. Informasi dapat diubah melalui proses enkripsi agar tidak dapat dibaca. Di sisi lain, dekripsi adalah proses mengubah data yang dienkripsi kembali menjadi data yang dapat dibaca [5].

Karena dapat beroperasi dalam blok 128-bit atau 16-karakter, *Advance Encryption Standard* (AES) biasanya digunakan dalam proses enkripsi format teks dan format file dokumen di mana format teks dapat lebih dari 16 karakter. *Advence Encryption Standard* (AES) melakukan enkripsi simetris berdasarkan *block cipher* dengan panjang kunci 128 bit, 192 bit, dan 256 bit secara paralel untuk memfasilitasi pemrosesan file yang dienkripsi dan didekripsi, selain itu juga dapat digunakan untuk keamanan atau sebagai kunci suatu objek [6]. Dari pernyataan diatas, penulis mengkaji lebih dalam terkait "Implementasi Kriptografi Pada Keamanan Data Menggunakan Algoritma *Advence Encryption Standard* (AES)".

### *Kriptografi*

Kriptografi merupakan seni dan ilmu penyandian pesan sehingga tidak dapat lagi dipahami. Metode ini menjaga kerahasiaan pesan. Keamanan data adalah masalah kriptografi. Hal ini mencakup pembuatan proses berbasis algoritma matematika yang menyediakan sejumlah fungsi keamanan informasi utama [7]. *Enkripsi* dan dekripsi adalah dua proses dalam kriptografi. Plaintext adalah nama yang diberikan untuk pesan terenkripsi. disebut demikian karena siapapun dapat membaca dan memahami informasi ini. Perhitungan yang digunakan untuk mengacak dan mendekode plainteks meliputi penggunaan beberapa jenis kunci.

*Cryptext* mengacu pada pesan eksplisit yang menyertakan *ciphertext* [8].

**Keamanan Data**

Data adalah deskripsi dari objek dan kejadian yang kita temui. Data bisnis adalah deskripsi objek (sumber daya) dan kejadian (transaksi) yang terjadi di dalam perusahaan [9]. Data dalam penelitian ini adalah segala bentuk fakta, data, dan segala bentuk informasi yang digali dari penelitian subjek [10]. Dari pengertian di atas dapat disimpulkan bahwa data adalah kumpulan fakta tentang suatu objek, peristiwa, atau kegiatan yang disimpan atau direkam. Dengan berkembangnya teknologi di bidang komunikasi dan perpesanan. Informasi tersebut harus aman dan rahasia. Karena informasi atau dokumen tersebut dapat mengandung informasi rahasia atau menjadi dokumen berharga yang perlu dirahasiakan. Salah satu cara yang dapat digunakan untuk mengamankan informasi atau dokumen adalah penggunaan sistem kriptografi.

**Algoritma *Advence Encryption Standard* (AES)**

*Advence Encryption Standard* (AES) memiliki panjang blok sebanyak 128 bit. Kunci *Advence Encryption Standard* (AES) dapat memiliki panjang kunci 128 bit, 192 bit, dan 256 bit. AES juga menggunakan lima ukuran data yaitu *bit*, *byte*, *word*, *blok*, dan *state*. *Bit* adalah unit terkecil dari data. yang merupakan nilai bilangan dalam sistem bilangan biner. Sementara *byte* adalah 8 *bit*, word memiliki ukuran 4 *byte* (32 *bit*), dan sebuah blok adalah 16 *byte* (128 *bit*), sedangkan *state* adalah *blok* yang disusun dalam *matriks* 4x4 *byte*. Fungsi yang tecakup dalam AES adalah operasi-operasi yang teridentifikasi dalam *finite field* GF($2^8$) berupa polinominal l irreducible pembangkit m(x) = x8 + x 4 + x3 + x + 1 [11].

Algoritma Algoritma *Advanced Encryption Standard* (AES) dipilih karena tingkat keamanannya yang tinggi dan pertukaran informasi yang sangat baik. Dalam penelitian ini, file dokumen uji digunakan untuk menentukan seberapa cepat dokumen dapat dienkripsi dan didekripsi [12].

Algoritma *Advence Encryption Standard* (AES) memiliki 3 parameter:

1. *Plain teks* merupakan array 16 *byte* yang berisi data input.
2. *Cipher teks* adalah array 16 byte yang berisi hasil enkripsi.
3. Kunci atau *key* merupakan sebuah array 16 byte yang berisi kunci cipher.

*SubBytes*, *ShiftRows*, *MixColumns*, *dan AddRoundKey* adalah empat tipe byte transformasi yang digunakan dalam proses enkripsi AES. Input yang telah masuk ke dalam state akan mengalami perubahan *AddRoundKey byte* demi *byte* pada awal proses enkripsi. SubBytes, *ShiftRows*, *MixColumns*, dan *AddRoundKey* kemudian akan berulang kali diubah dalam status Nr. Fungsi bulat adalah nama yang diberikan untuk proses ini dalam algoritma AES. Putaran terakhir agak tidak sama dengan putaran sebelumnya di mana pada putaran terakhir, keadaan tidak melalui perubahan *MixColumns* [6].

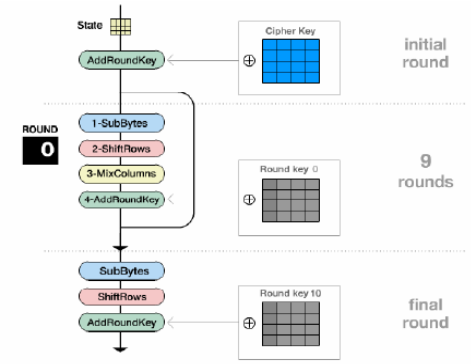
**Cara Kerja Algoritma *Advence Encryption Standard* (AES)**

Algoritma *Advanced Encryption Standard* (AES) mengikuti skema global berikut:

1) *AddRoundKey* adalah siklus XOR antara teks biasa dan kunci kode. Tahap ini juga disebut babak awal.
2) Putar hingga seratus kali. Prosedur setiap putaran mencakup hal-hal berikut: Untuk memulai, *subbyte*, khususnya cara *subbing byte* yang paling umum menggunakan *S-box* atau tabel pengganti. *SubBytes* adalah transformasi *byte* di mana tabel substitusi S-*Box* digunakan untuk memetakan setiap komponen state [13]. Kedua, Shiftrows adalah

proses yang mengeksekusi pergeseran komponen blok/tabel yang harus dilakukan per baris; baris pertama tidak perlu digeser 2 byte, dan baris keempat hanya perlu digeser 3 *byte* setelahnya [13]. *Shiftrows* menggunakan pembungkus untuk memindahkan baris dalam status array. Ketiga, *mixcolumns*, atau prosedur penempatan data secara acak ke setiap kolom *array state*. Perhitungan *mixcolumns* akan menambahkan satu baris matriks default ke satu *byte* kolom pertama [14]. Keempat, addroundkey yaitu Untuk menemukan lokasi *addroundkey*, proses *xor byte state keyschedule* dengan *mixcolumns* [14]. Operasi XOR antara keadaan saat ini dan kunci bulat dilakukan oleh kunci tambahan. *Cipherteks* yang diperoleh pada putaran pertama akan digunakan sebagai input pada putaran kedua, dan *cipherteks* yang diperoleh pada putaran kedua akan digunakan sebagai input pada putaran ketiga. Hingga putaran kesepuluh, prosedur ini terus berlanjut [15].

3) Putaran terakhir, untuk lebih spesifik siklus putaran terakhir termasuk *SubBytes, ShiftRows, dan AddRoundKey*.




**Gambar 1.** Diagram Proses *Enkripsi*

## METODE

Terdapat metode penelitian untuk memastikan penelitian sesuai dengan rencana dan prosedur, sehingga mendapatkan hasil yang diharapkan. Metode yang digunakan dalam penelitian adalah sebagai berikut :

### Studi Literatur

Pada tahap ini, review jurnal, artikel, dan penelitian sebelumnya dapat dijadikan referensi. Hal tersebut dibutuhkan untuk mendapatkan informasi terkait algoritma AES dan bahasa pemrograman PHP sebagai acuan penelitian ini.

### Desain Perancangan dan Analisis

Prosedur ini memungkinkan untuk menerapkan data dari hasil literatur. Analisis dan implementasikan dengan salah satu algoritma AES menggunakan metode desain SDLC, sehingga ini bisa menjadi sistem yang aman, terutama keamanan algoritma AES.

### Implementasi

Pada tahap ini, algoritma AES juga dapat digunakan untuk membuat sistem keamanan. Dengan menggunakan bahasa pemrograman PHP dan menggunakan database MySQL.

### Pengujian

Prosedur pengujian ini menguji apakah algoritma AES bekerja dengan baik dan tidak terjadi kesalahan Eksekusi Bahasa Pemrograman PHP dan perbaikan jika ditemukan error atau kesalahan pada sistem.

## HASIL DAN PEMBAHASAN

### *Designer* Sistem

Algoritma *Advanced Encryption Standard* (AES) digunakan oleh sistem aplikasi untuk keamanan dokumen. Eksekusi program ditampilkan pada Gambar 2. Gambar tersebut menjelaskan proses enkripsi secara garis besar yang diterapkan di dalam program.

```
function encrypt($input){
        # memecah inputan/data ke dalam bentuk string
        $data = str_split($input);

        $state = array();
        $count  = 0;
        $this->pos_w = 0;

        for($i=0; $i<4; $i++){
                for($j=0; $j<4; $j++) {
                        if ($count < count($data)){
                                $this->state[$i][$j] = ord($data[$count]);
                        } else{
                                $this->state[$i][$j] = 0;
                        }
                        $count++;
                }
        }
        // AddRoundKey #1
        for($i=0; $i<4; $i++){

                for($j=0; $j < $this->Nb; $j++) {
                        $this->state[$i][$j] = $this->state[$i][$j] ^ $this->w[$i][$this->pos_w + $j];
                }
        }
        $this->pos_w = $this->pos_w + $this->Nb;

        for ($i=0; $i<$this->Nr-1; $i++) {
                $this->state = $this->SubByte($this->state);
                $this->state = $this->ShiftRow($this->state);
                $this->state = $this->MixColumns($this->state);
                $this->state = $this->AddRoundKey($this->state);
                $this->pos_w = $this->pos_w + $this->Nb;

        }
        $this->state = $this->SubByte($this->state);
        $this->state = $this->ShiftRow($this->state);
        $this->state = $this->AddRoundKey($this->state);
        $cipher = "";
        foreach($this->state as $state){
                foreach($state as $data) {
                        $cipher .= chr($data);
                }
        }
        return $cipher;
}
```

**Gambar 2.** Kode fungsi utama

## Implementasi Antarmuka

Suatu program yang didasarkan pada hasil sistem yang dirancang dalam implementasi antarmuka. Implementasi antarmuka dapat dilihat di bawah ini:

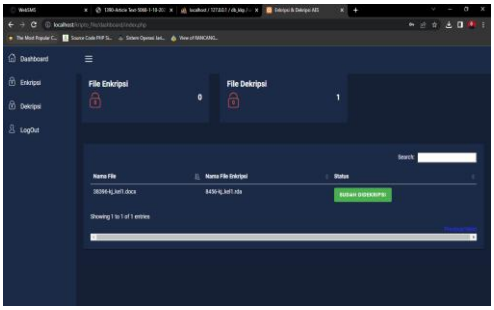
a) Halaman *Login*

Halaman login digunakan untuk masuk terlebih dahulu ke dalam aplikasi AES dengan menginputkan username dan *password* yang telah terdaftar di dalam *database*. Untuk membatasi penggunaan enkripsi data dalam aplikasi AES ini yang ditunjukkan pada Gambar 3 untuk pengguna terdaftar.


**Gambar 3.** Halaman login

b) Halaman *Dashboard*

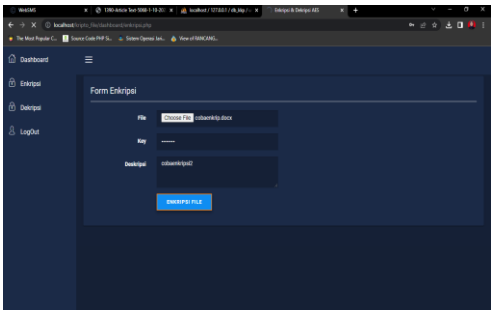
Pada halaman ini menampilkan jumlah file yang dienkripsi dan didekripsi. Selain itu terdapat tabel yang menampilkan nama file yang *diexport*, nama *file* hasil *enkripsi*, dan status file tersebut sudah dienkripsi atau belum. Pada halaman ini juga menampilkan menu yang berisi *navigasi dashboard*, *enkripsi*, dekripsi, dan *logout* ditampilkan pada Gambar 4.




**Gambar 4.** Halaman *dashboard*

c) Halaman *File Enkripsi*

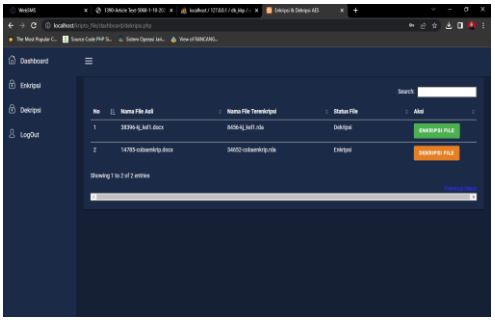
Halaman *enkripsi* dimana pada halaman ini *user* diminta untuk memasukkan *file* yang akan dienkripsi, kemudian masukkan *key* untuk diproses pada AES, dan deskripsi untuk file yang akan dienkripsi. Jika sudah memasukkan semua yang diminta pada form, maka klik tombol enkripsi *file* untuk memproses *file* ke dalam *file* enkripsi ditampilkan pada Gambar 5.




**Gambar 5.** Halaman File *Enkripsi*

d) Halaman *File Deskripsi*

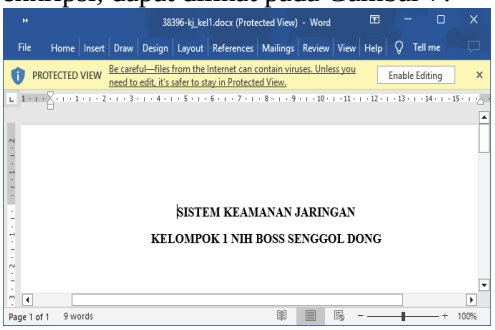
Halaman *file deskripsi* menampilkan detail info mengenai file yang dienkripsi sebelumnya, mulai dari nama *file* asli, nama file enkripsi, ukuran *file*, tanggal, dan keterangan. Ketika ingin melakukan dekripsi pada *file* maka kita perlu memasukkan *password* yang sebelumnya telah kita masukkan sebelum mengenkripsi *file*. Jika sudah, maka klik tombol dekripsi *file* untuk melakukan proses dekripsi. Hasil dari proses enkripsi maupun dekripsi dapat dilihat pada file yang ada dalam folder *project* aplikasi.ditampilkan pada Gambar 6.



**Gambar 6.** Halaman *file* dekripsi

e) Hasil *Dekripsi*

Hasil dekripsi merupakan dokumen kj_kel1.docx yang akan di enkripsi, dapat dilihat pada Gambar 7.




**Gambar 6.** Dokumen deskripsi

f) Hasil *Enkripsi*

Hasil *enkripsi* merupakan hasil dari dokumen kj_kel1.docx, dapat dilihat pada Gambar 8.

**Gambar 7.** Hasil enkripsi

## SIMPULAN

Perhitungan AES dapat digunakan sebagai pengamanan data dengan menyembunyikan informasi melalui enkripsi dan dekripsi. Algoritma AES yang diterapkan dalam program untuk keamanan data menghasilkan sebuah *file* atau dokumen yang berisi tulisan abstrak atau tidak dapat dibaca begitu saja setelah melewati proses enkripsi dengan mengatur kunci. *File* atau dokumen tersebut dapat kembali seperti semula ketika melewati proses dekripsi, namun harus memasukkan kunci yang sama dengan yang dimasukkan ketika proses enkripsi.

## SARAN

Penelitian ini dibuat untuk menunjukkan manfaat penerapan algoritma AES dalam keamanan data. Namun, hasil penelitian ini memang belum sempurna dan perlu pengkajian teori yang lebih dalam agar dapat menciptakan inovasi dan teknologi yang lebih baik. Maka penulis berharap penelitian ini dapat ditinjau dan dikembangkan kembali oleh penulis lainnya sehingga dapat menciptakan teknologi keamanan data yang lebih baik lagi.

## DAFTAR PUSTAKA

[1] H. Prasetyo and W. Sutopo, "Industri 4.0: Telaah Klasifikasi Aspek Dan Arah Perkembangan Riset," *J@ti Undip J. Tek. Ind.*, vol. 13, no. 1, p. 17, 2018, doi: 10.14710/jati.13.1.17-26.

[2] M. B. Firdaus, E. Budiman, Haviluddin, M. Wati, H. J. Setyadi, and H. S. Pakpahan, "An openness of government website content using text analysis method," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 5, pp. 1461–1466, 2019, doi: 10.35940/ijeat.E1214.0585C19.

[3] M. S. Rahmawati and R. Soekarta, "Teori Grup Pada Algoritma DES Dan Transformasi Wavelet Diskrit Dalam Program Aplikasi Keamanan Citra Digital," *Insect (Informatics Secur. J. Tek. Inform.*, vol. 4, no. 1, p. 1, 2019, doi: 10.33506/insect.v4i1.281.

[4] D. Novianto and Y. Setiawan, "Aplikasi Pengamanan Informasi Menggunakan Metode Least

Significant Bit (Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Ilm. Inform. Glob.*, vol. 9, no. 2, pp. 83–89, 2019, doi: 10.36982/jig.v9i2.561.

[5] Ferdiansyah, A. Id Hadiana, and F. Rakhmat Umbara, "Penggunaan QR Code Berbasis Kriptografi Algoritma AES (Advanced Encryption Standard) Untuk Administrasi Rekam Medis," *J. Inf. Technol.*, vol. 3, no. 2, pp. 20–27, 2021, doi: 10.47292/joint.v3i2.64.

[6] A. Eka Putri, A. Kartikadewi, and L. A. Abdul Rosyid, "Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang," *Appl. Inf. Syst. Manag.*, vol. 3, no. 2, pp. 69–78, 2021, doi: 10.15408/aism.v3i2.14722.

[7] Y. J. El Anwar, R. Habibi, and N. Riza, "Penerapan Metode Kriptografi Aes Untuk Mengamankan File Dokumen," *J. Tekno Insentif*, vol. 16, no. 2, pp. 92–104, 2022, doi: 10.36787/jti.v16i2.852.

[8] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[9] A. Ignasius and D. V. Shaka Yudha Sakti, "Penerapan Algoritma Aes (Advance Encryption Standart) 128 Untuk Enkripsi Dokumen Di Pt. Gunung Geulis Elok Abadi," *Skanika*, vol. 5, no. 1, pp. 1–10, 2022, doi: 10.36080/skanika.v5i1.2118.

[10] I. A. R. Simbolon, I. Gunawan, I. O. Kirana, R. Dewi, and S. Solikhun, "Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar," *J. Comput. Syst. Informatics*, vol. 1, no. 2, pp. 54–60, 2020.

[11] A. Pariddudin and F. Syauqi, "Penerapan Algoritma AES pada QR CODE untuk Keamanan Verifikasi Tiket," *Teknois J. Ilm. Teknol. Inf. dan Sains*, vol. 10, no. 2, pp. 43–52, 2020, doi: 10.36350/jbs.v10i2.87.

[12] B. Wicaksana and M. Setiawan, "Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Pengamanan Berkas Soal Ujian," *Teknois J. Ilm. Teknol. Inf. dan Sains*, vol. 10, no. 1, pp. 25–34, 2020, doi: 10.36350/jbs.v10i1.74.

[13] E. S. Marsiani, I. Setiadi, and A. Cahyo, "Implementasi Sistem Keamanan AES 256-Bit GCM Guna Mengamankan Data Pribadi," *JRKT (Jurnal Rekayasa Komputasi Ter.*, vol. 1, no. 02, pp. 108–114, 2021, doi: 10.30998/jrkt.v1i02.4096.

[14] S. Widyastuti, W. Ariandi, and V. Sulistiono, "Implementasi Kriptografi AES Dalam Pengamanan Data Seleksi Peserta JAMKESMAS," *J. Ilm. Intech Inf. Technol. J. UMUS*, vol. 1, no. 02,

pp. 13–22, 2019, doi: 10.46772/intech.v1i02.66.

[15] D. Widyawan and I. Imelda, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite Nasional Keselamatan Transportasi," *Skanika*, vol. 4, no. 1, pp. 15–22, 2021, doi: 10.36080/skanika.v4i1.2216.